Dispel IEC 62443 Remote Access Framework Mapping

Cybersecurity Frameworks
IEC 62443:2019
Sept. 2022 Update

DISPEL

Dispel's Alignment With IEC 62443

Introduction

Industrial automation and control system ("IACS") organizations increasingly use commercial off-the-shelf ("COTS") networked devices that are inexpensive, efficient, and highly automated. Control systems are also increasingly interconnected with non-IACS networks for valid business reasons. These devices, open networking technologies, and increased connectivity elevate the theoretical cyber risk of control system hardware and software. This, in turn, has raised concerns over Health, Safety and Environmental ("HSE"), financial, and/or reputational consequences from cyberattacks on deployed control systems.

IEC 62443 is not a proscriptive guide. The goal of the IEC 62443 series is to provide a flexible framework that *facilitates* addressing current and future vulnerabilities in IACSs and applying necessary mitigations in a systematic, defensible manner through an IACS Security Program (an "IACS SP"). For those readers working in Corporate, the reports you receive on Security Program efficacy are based off of Security Program Ratings ("SPRs") – quantified assessments of the SP efficacy.

IEC 62443 in Context

Much like the interrelationship between the National Institute of Standards and Technology ("NIST") Cyber Security Framework (the "CSF") Version 1.1 and the NIST Special Publications (the "NIST SP"s), IEC 62443 is structured as a series of interleaving modular documents. These documents are categorized into four series, with the designation structure of IEC 62443-[series]-[sub document number].

The **IEC 62443-1** series exists to define the terms and frameworks off of which the rest of the documents and recommendations contained in IEC 62443 rely.

The **IEC 62443-2** series is used to define the roles, responsibilities, requirements, and audit mechanisms for the organizational structure and management of the IACS SP. As such, the IEC 62443-2 series is the one that you are most likely to encounter first if coming over from Corporate or serving in an advisory capacity to a firm that follows IEC 62443. However, with the exception

of IEC 62443-2-4, the rest of IEC 62443-2 is not the series of direct relevance to assessing products or services going into an IACS.

As a point of clarification, while new readers of the IEC 62443-2 series will notice that it generally references the IEC 62443-3 series when discussing product capabilities, they will also notice that some sections, such as §8.4 of IEC 62443-2-1, have documentation requirements which implicitly require any productized solution to have a set of underlying features. While true, with the exception of IEC 62443-2-4, sections throughout the rest of the series, including §8.4 of IEC 62443-2-1, are still cross-referenced over to IEC 62443-3.

IEC 62443-2-4 serves as a guide for third parties interacting with an IACS on what to request at an organizational and procedural level from the IACS owner. IEC 62443-2-4 is the exception to the rest of the IEC 62443-2 series in that, regrettably, it does not provide a cross referencing structure as of the time of this document's printing.

The **IEC 62443-3** series is most usefully perceived as the mapping series within the broader IEC 62443 structure from objectives to practical implementation at a technological level. Here, Framework Requirements ("FR"s) are aligned with System Requirements ("SR") for control systems.

The **IEC 62443-4** series serves as a guide for suppliers of systems that form, or form a part of, a control system. As with IEC 62443-3, Framework Requirements ("FR"s) are aligned with System Requirements ("SR") for control systems. **IEC 62443-4-1** is primarily focused on applying a standardized process to the development, deployment, and sustainment of product. **IEC 62443-4-2** is primarily focused on defining the security attributes and capabilities that should be present within a control system, or a supporting component thereto.

Based upon the above summary, the remainder of this document is focused on Dispel's coverage with respect to IEC 62443-3 and IEC 624430-4.

Contents

Mapping For IEC 62443-3-3: System Security Requirements and Security Levels

This part of the IEC 62443 series provides detailed technical control system requirements ("SR"s) associated with the seven foundational requirements ("FR"s) described in IEC 62443-1-1 including defining the requirements for control system capability security levels, (Security Level Capability, or "SL-C"). These requirements would be used by various members of the industrial automation and control system (IACS) community along with the defined zones and conduits for the System under Consideration (SuC) while developing the appropriate security level for the target control system, (Security Level Target, or "SL-T"),

As defined in IEC 62443-1-1 there are a total of seven FRs:

FR 1 - Identification and authentication control (IAC),
FR 2 - Use control (UC),
FR 3 - System integrity (SI),
FR 4 - Data confidentiality (DC),
FR 5 - Restricted data flow (RDF),
FR 6 - Timely response to events (TRE), and
FR 7 - Resource availability (RA).

These seven requirements are the foundation for control system capability SLs, SL-C (control system). Defining security capability at the control system level is the goal and objective of this standard as opposed to target SLs, SL-T, or achieved SLs, SL-A, which are out of scope.

See IEC 62443-2-1 for an equivalent set of non-technical, program-related, capability SRs necessary for fully achieving a control system target SL.

IEC 62443-3-3 FR 1 – Identification and Authentication Control

Part	Title	Requirement	Dispel Product/Feature	
SR 1.1	**Human user identification and authentication**	The control system shall provide the capability to identify and authenticate all human users. This capability shall enforce such identification and authentication on all interfaces which provide human user access to the control system to support segregation of duties and least privilege in accordance with applicable security policies and procedures.	Each human user must log in using a minimum of a unique username and complex password to access Dispel. Roles and access controls are assigned to each user account. Pursuant to §5.3.2, paragraph 2, control rooms or critical operations rooms may set up role-based users so a team of human users can connect under the same username and password associated with the control room to the access portal. Dispel strongly advises against this practice except under very unique conditions. Please see SR 2.1 for permissions enforcement. Each human user is uniquely identified when using Dispel by their login username and password except where, pursuant to §5.3.2, paragraph 2, role-based or group-based access identification is chosen as the preferred route in control room or critical operations rooms.	Yes

SR 1.1 RE 1	Unique identification and authentication	The control system shall provide the capability to uniquely identify and authenticate all human users.	Each human user is uniquely identified when using Dispel by their login username and password except where, pursuant to §5.3.2, paragraph 2, role-based or group-based access identification is chosen as the preferred route in control room or critical operations rooms.	Yes
SR 1.1 RE 2	Multifactor authentication for untrusted networks	The control system shall provide the capability to employ multifactor authentication for human user access to the control system via an untrusted network (see 5.15, SR 1.13 – Access via untrusted networks).	Dispel supports TOTP authentication tools (QR code style) such as Google Authenticator, Microsoft Authenticator, 1Password, Authy, etc. Dispel also supports FIDO U2F hardware tokens such as Yubikeys, RSA SecurID tokens, and Common Access Cards.Dispel integrates with Active Directory, LDAP, Okta, and native OS biometric authentication systems including Apple Touch ID and Windows Hello in apps. Admins may enforce MFA be used by all Dispel all users.	Yes

SR 1.1 RE 3	Multifactor authentication for all networks	The control system shall provide the capability to employ multifactor authentication for all human user access to the control system.	Dispel supports TOTP authentication tools (QR code style) such as Google Authenticator, Microsoft Authenticator, 1Password, Authy, etc. Dispel also supports FIDO U2F hardware tokens such as Yubikeys, and RSA SecurID tokens. Dispel integrates with Active Directory, LDAP, Okta, and native OS biometric authentication systems including Apple Touch ID and Windows Hello in apps. Admins may enforce MFA be used by all Dispel all users.	Yes
SR 1.2	**Software process and device identification and authentication**	The control system shall provide the capability to identify and authenticate all software processes and devices. This capability shall enforce such identification and authentication on all interfaces which provide access to the control system to support least privilege in accordance with applicable security policies and procedures.	"Dispel can restrict what protocols may be used when accessing a control system. Using a Dispel Virtual Desktop ("VDI") as part of the remote access deployment, the types of software available to the User can be pre-defined, and software pro-cesses being run can be tracked"	Yes

SR 1.2 RE 1	Unique identification and authentication	The control system shall provide the capability to uniquely identify and authenticate all software processes and devices.	While Dispel is able to proactively identify and authenticate all software processes being run on a Dispel Virtual Desktop and all devices connected to a Dispel remote access network, because of the mention of "devices", we believe SR 1.2 RE 1 was intended to be in reference to the control system itself and the layers below it, rather than the remote access layer above it. We, therefore, do not consider this section to be applicable.	Not Applicable
SR 1.3	**Account management**	The control system shall provide the capability to support the management of all accounts by authorized users, including adding, activating, modifying, disabling and removing accounts.	Dispel includes a user account management system; providing tools for adding, updating, removing, and permissioning users. Dispel also integrates with commonly used user management tools such as Microsoft Active Directory, LDAP, and Okta.	Yes
SR 1.3 RE 1	Unified account management	The control system shall provide the capability to support unified account management.	Dispel supports unified account management tools such as Microsoft Active Directory, LDAP, and Okta. When a customer chooses to use one of these tools, their account relies on the UAM for all users.	Yes

SR 1.4	**Identifier management**	The control system shall provide the capability to support the management of identifiers by user, group, role or control system interface.	Dispel supports identifier based management for users and groups.The system allows restrictions on how a user is allowed to access control systems (via a VDI, or through a VPN application) and then what ports, IPs, and protocols they may use in that control environment.While it is strongly discouraged, Dispel does support access by general accounts (e.g., a "Control Room" master user account). However, a human user or machine account is supposed to be tied to a unique identifier.	Yes
SR 1.5	**Authenticator management**	The control system shall provide the capability to: a) initialize authenticator content; b) change all default authenticators upon control system installation; c) change/refresh all authenticators; and d) protect all authenticators from unauthorized disclosure and modification when stored and transmitted.	Dispel supports authenticator's for proving identity. A user account has a salted and hashed password associated with their login. User accounts do not have default passwords. Passwords and tokens are always transmitted under strong encryption (e.g., AES-256 with 4096-bit keys). During login, the service generates and grants a user a session. User sessions automatically expire after a set period of time.	Yes

SR 1.5 RE 1	Hardware security for software process identity credential	For software process and device users, the control system shall provide the capability to protect the relevant authenticators via hardware mechanisms.	For standard deployments, User passwords are salted and hashed before being stored in the Dispel database. This database is then encrypted by EBS encryption via the AWS Key Management Service. At no time are passwords stored in the Dispel database in plaintext. While the data on NVMe instance store volumes is encrypted using an XTS-AES-256 cipher implemented on a hardware module on the instance, there is no guarantee AWS uses NVMe for the Dispel database. User session authenticators are not saved to devices that touch control systems. Sessions are stored in system memory. Note that system memory does not utilize hardware modules such as Apple T2 Security Chips or Microsoft TPM.For deployments requiring Hardware Security Modules (HSMs), key management is instead performed through a single-tenanted FIPS 140-2 Level 3 validated HSM or a client-provided FIPS 140-2 Level 4 validated HSM. While this option exists, we wish to stress that it is not typically used due to the costs associated with it.	Yes

SR 1.6	**Wireless access management**	The control system shall provide the capability to identify and authenticate all users (humans, software processes or devices) engaged in wireless communication.	All remote access to a control system that runs through Dispel traverses a piece of hardware called a Wicket External Systems integrator. The customer can specify what backhaul is used (wired, LTE, satellite, etc.) by the Wicket ESI during its configuration. This specification, in turn, can be documented within either the description section of the Wicket ESI on the management console, or in the name itself of the Wicket ESI (recommended), allowing for the ready identification of whether the communications accessing the control system are coming in wirelessly or not. For the Wicket ESI to function, it must successfully authenticate against the Dispel system. This action is necessarily a unique authentication action.	Yes

SR 1.6 RE 1	Unique identification and authentication	The control system shall provide the capability to uniquely identify and authenticate all users (humans, software processes or devices) engaged in wireless communication.	All remote access to a control system that runs through Dispel traverses a piece of hardware called a Wicket External Systems integrator. The customer can specify what backhaul is used (wired, LTE, satellite, etc.) by the Wicket ESI during its configuration. This specification, in turn, can be documented within either the description section of the Wicket ESI on the management console, or in the name itself of the Wicket ESI (recommended), allowing for the ready identification of whether the communications accessing the control system are coming in wirelessly or not. For the Wicket ESI to function, it must successfully authenticate against the Dispel system. This action is necessarily a unique authentication action.	Yes
SR 1.7	**Strength of password-based authentication**	For control systems utilizing password-based authentication, the control system shall provide the capability to enforce configurable password strength based on minimum length and variety of character types.	Dispel passwords enforce password strength based on a minimum length, and combination of uppercase characters, special characters, and numbers.	Yes

SR 1.7 RE 1	Password generation and lifetime restrictions for human users	The control system shall provide the capability to prevent any given human user account from reusing a password for a configurable number of generations. In addition, the control system shall provide the capability to enforce password minimum and maximum lifetime restrictions for human users. These capabilities shall conform with commonly accepted security industry practices.	Dispel prevents the re-use of old passwords, and enforces lifetime restrictions for passwords.	Yes
SR 1.7 RE 2	Password lifetime restrictions for all users	The control system shall provide the capability to enforce password minimum and maximum lifetime restrictions for all users.	Dispel does enforces lifetime restrictions for passwords.	Yes
SR 1.8	**Public key infrastructure (PKI) certificates**	Where PKI is utilized, the control system shall provide the capability to operate a PKI according to commonly accepted best practices or obtain public key certificates from an existing PKI.	Dispel uses industry-standard PKI methods for key management including VPN sessions and TLS certificates.	Yes

SR 1.9	**Strength of public key authentication**	For control systems utilizing public key authentication, the control system shall provide the capability to: a) validate certificates by checking the validity of the signature of a given certificate; b) validate certificates by constructing a certification path to an accepted CA or in the case of self-signed certificates by deploying leaf certificates to all hosts which communicate with the subject to which the certificate is issued; c) validate certificates by checking a given certificate's revocation status; d) establish user (human, software process or device) control of the corresponding private key; and e) map the authenticated identity to a user (human, software process or device)	Dispel PKI is used to identify Dispel's identity to users in circumstances such as TLS. Users are not authenticated using PKI. In this context, Dispel complies with the steps listed here.	Yes
SR 1.9 RE 1	Hardware security for public key authentication	The control system shall provide the capability to protect the relevant private keys via hardware mechanisms according to commonly accepted security industry practices and recommendations.	Dispel uses PKI for TLS, not user authentication. In the TLS context, hardware mechanisms are used to protect private keys.	Yes

SR 1.10	**Authenticator feedback**	The control system shall provide the capability to obscure feedback of authentication information during the authentication process.	Dispel provides general feedback to users to obscure what information may be accurate during authentication. For example, if an invalid username or password is used during authentication the system replies that an invalid username/password was used. Or, when a password reset is made the system replies "If that account exists, it will receive an email shortly."	Yes
SR 1.11	**Unsuccessful login attempts**	The control system shall provide the capability to enforce a limit of a configurable number of consecutive invalid access attempts by any user (human, software process or device) during a configurable time period. The control system shall provide the capability to deny access for a specified period of time or until unlocked by an administrator when this limit has been exceeded.	Dispel locks a user account after a set number of failed consecutive logins. Locked out accounts must be manually re-enabled. Idling is prevented through the use of virtual desktops with Administrator defined maximum lifespans.	Yes
SR 1.12	**System use notification**	The control system shall provide the capability to display a system use notification message before authenticating. The system use notification message shall be configurable by authorized personnel.	For customers seeking to meet this requirement (along with many others within the IEC 62443 framework, for that matter), Dispel requires the use of a virtual desktop - on which a system use notification may be placed. In addition, a system use notification can be presented to the User as part of form-based access request procedures (where implemented).	Yes

SR 1.13	**Access via untrusted networks**	The control system shall provide the capability to monitor and control all methods of access to the control system via untrusted networks.	Dispel strictly controls all access to control systems from untrusted networks through the use of single-use virtual desktops tied to a moving target defense SD-WAN. Monitoring is provided via syslogging and session recording on VDIs.	Yes
SR 1.13 RE 1	Explicit access request approval	The control system shall provide the capability to deny access requests via untrusted networks unless approved by an assigned role.	Dispel denies access by default. Users must authenticate with proper credentials and multifactor authentication functions; be granted permission to access control systems; and have user based access permissions for the IP addresses, ports, and protocols of the control systems they wish to access.	Yes

IEC 62443-3-3 FR 2 - Use Control

Part	Title	Requirement	Dispel Product/Feature	
SR 2.1	**Authorization enforcement**	On all interfaces, the control system shall provide the capability to enforce authorizations assigned to all human users for controlling use of the control system to support segregation of duties and least privilege.	Dispel provides device, protocol, process, and session-level access control which, by definition, leads to an identical degree of authorization mapping. This capability is enforced at multiple levels within the Dispel product. For human users, single-use virtual desktops ensure session-level segmentation and excel at protocol and process segmentation against determined adversaries. The network infrastructure spanning the distance from the user to the Wicket ESI located at the Control System can be set to self-destruct after each session is concluded, providing a safeguard that task segregation is achieved temporally. At the Wicket ESI, user-session-specific whitelisting of underlying equipment serves as a failsafe for human users connecting through a virtual desktop interface.	Yes

SR 2.1 RE 1	Authorization enforcement for all users	On all interfaces, the control system shall provide the capability to enforce authorizations assigned to all users (humans, software processes and devices) for controlling use of the control system to support segregation of duties and least privilege.	Dispel provides device, protocol, process, and session-level access control which, by definition, leads to an identical degree of authorization mapping. This capability is enforced at multiple levels within the Dispel product. For human users, single-use virtual desktops ensure session-level segmentation and excel at protocol and process segmentation against determined adversaries. For machine users, this responsibility necessarily falls instead to the network infrastructure and Wicket ESI, which both hold roles as bastion components. The network infrastructure spanning the distance from the user to the Wicket ESI located at the Control System can be set to self-destruct after each session is concluded, providing a safeguard that task segregation is achieved temporally. At the Wicket ESI, user-session-specific whitelisting of underlying equipment serves as a failsafe for human users connecting through a virtual desktop interface, and as the primary mechanism for providing such protection in the case of machine users.	Yes

SR 2.1 RE 2	Permission mapping to roles	The control system shall provide the capability for an authorized user or role to define and modify the mapping of permissions to roles for all human users.	Dispel addresses this problem with two converging procedures. First, authorized users are allowed to define or modify the mapping of permissions to a human user through the management console. Second, if the customer so chooses, Dispel's remote access system can be set to require a form be completed by the person requesting access or a change to their access permissions. In this second situation, two humans – the user and administrator – are able to define precisely what it is that a person is going to be given access too. This technique serves to reduce the risk of an administrator assigned a permission set that is broader than needed by the user.	Yes

SR 2.1 RE 3	Supervisor override	The control system shall support supervisor manual override of the current human user authorizations for a configurable time or event sequence.	First, authorized users are allowed to define or modify the mapping of permissions to a human user through the management console at any time. Virtual desktops are set with time-to-live conditions, allowing an administrator to cleanly configure the time during which an authorization set are held open. Wicket ESIs control equipment whitelisting and can be reconfigured at any time as well. The stated requirement of SR 2.1 RE 3, however, is clarified in the "Note" section to be in reference to emergency situations; the goal being to allow a supervisor to expand a permission set without forcing the operator to log out and log in again to obtain access to the broadened capabilities. In practice, not all permissions can be overridden without a new session being created – the reason being that different equipment sets require different applications to run them, and Dispel virtual desktops are not launched with applications irrelevant to the equipment to which a user is granted access. For this reason, we have assigned this section a Partial Coverage rating.	Yes
SR 2.1 RE 4	Dual approval	The control system shall support dual approval where an action can result in serious impact on the industrial process.	An administrator can specify that dual approval is required to access a specific part of the control system.	Yes

SR 2.2	**Wireless use control**	The control system shall provide the capability to authorize, monitor and enforce usage restrictions for wireless connectivity to the control system according to commonly accepted security industry practices.	Dispel provides remote access to control systems via a Wicket ESI – a virtual or hardware appliance. In either case, the backhaul from the Wicket ESI is a known quantity, which means all connections to the control system are uniform in their use of a particular backhaul. All traffic attempting to reach the Control System must undergo the same rigorous authorization requirements, and may be monitored, as well as recorded, per the Dispel customer's specifications.	Yes
SR 2.2 RE 1	Identify and report unauthorized wireless devices	The control system shall provide the capability to identify and report unauthorized wireless devices transmitting within the control system physical environment.	Not applicable.	Not Applicable
SR 2.3	**Use control for portable and mobile devices**	The control system shall provide the capability to automatically enforce configurable usage restrictions that include: A) Preventing the use of portable and mobile devices; B) Requiring context specific authorization; and C) Restricting code and data transfer to/from portable and mobile devices.	Any connection reaching the Control System through Dispel necessarily traverses a disposable intermediate component – typically, a virtual desktop. This intermediate component serves the purpose of creating a protocol break between the mobile/portable device and the Control System and controlling data transfer. Context specific authorization is available if an access request form process has been activated by the customer.	Yes
SR 2.3 RE 1	Enforcement of security status of portable and mobile devices	The control system shall provide the capability to verify that portable or mobile devices attempting to connect to a zone comply with the security requirements of that zone.	Not applicable.	Not Applicable

SR 2.4	**Mobile code**	The control system shall provide the capability to enforce usage restrictions for mobile code technologies based on the potential to cause damage to the control system that include: a) preventing the execution of mobile code; b) requiring proper authentication and authorization for origin of the code; c) restricting mobile code transfer to/from the control system; and d) monitoring the use of mobile code.	For those reading this document without a copy of IEC 62443-3-3 in front of them, "mobile code" is defined to include such things as Java, JavaScript, ActiveX, and Portable Document Format (PDF), to name a few. To meet SR 2.4, Dispel typically does not permit the upload of files to the single-use virtual desktop that forms a part of the remote access system (in other words, a heavy emphasis on restriction c in order to meet restriction a. However, there are times when customers want to push mobile code up to virtual desktops. In these situations, certificate checks can be required, and virus scans can be performed. All activities, including those involving mobile code, are monitored in Dispel deployments when the appropriate logging and recording packages are included by the customer.	Yes
SR 2.4 RE 1	Mobile code integrity check	The control system shall provide the capability to verify integrity of the mobile code before allowing code execution.	For those reading this document without a copy of IEC 62443-3-3 in front of them, "mobile code" is defined to include such things as Java, JavaScript, ActiveX, and Portable Document Format (PDF), to name a few. To meet SR 2.4 RE 1, Dispel embeds a virus scanner onto its virtual desktops.	Yes

SR 2.5	**Session Lock**	The control system shall provide the capability to prevent further access by initiating a session lock after a configurable time period of inactivity or by manual initiation. The session lock shall remain in effect until the human user who owns the session or another authorized human user re-establishes access using appropriate identification and authentication procedures.	Dispel accomplishes this task by assigning time-to-live restrictions on its virtual desktops. Virtual desktops may also be manually destroyed prior to their pre-specified time to live by an administrator at any time.	Yes
SR 2.6	**Remote session termination**	The control system shall provide the capability to terminate a remote session either automatically after a configurable time period of inactivity or manually by the user who initiated the session.	Regardless of whether the user is a human or machine, the virtual infrastructure out of which a Dispel remote access system is composed can be destroyed in accordance with a pre-specified schedule. The remote session may be terminated at any time by the user who initiated the session.	Yes
SR 2.7	**Concurrent session control**	The control system shall provide the capability to limit the number of concurrent sessions per interface for any given user (human, software process or device) to a configurable number of sessions.	Dispel permits this configuration in the management console.	Yes

SR 2.8	**Auditable events**	The control system shall provide the capability to generate audit records relevant to security for the following categories: access control, request errors, operating system events, control system events, backup and restore events, configuration changes, potential reconnaissance activity and audit log events. Individual audit records shall include the timestamp, source (originating device, software process or human user account), category, type, event ID and event result.	Dispel renders these services, to the extent they are visible to Dispel components, through its logging and screen recording systems. Please note that Dispel's alignment with SR 2.8 is not a replacement for logging inside of the control system itself.	Yes
SR 2.8 RE 1	Centrally managed, system-wide audit trail	The control system shall provide the capability to centrally manage audit events and to compile audit records from multiple components throughout the control system into a systemwide (logical or physical), time-correlated audit trail. The control system shall provide the capability to export these audit records in industry standard formats for analysis by standard commercial log analysis tools, for example, security information and event management (SIEM).	Not applicable. However, Dispel is able to interface its systems directly to the analytics packages envisioned by SR 2.8 RE 1. Aggregation, in short, is not completed by Dispel.	Yes
SR 2.9	**Audit storage capacity**	The control system shall allocate sufficient audit record storage capacity according to commonly recognized recommendations for log management and system configuration. The control system shall provide auditing mechanisms to reduce the likelihood of such capacity being exceeded.	Dispel offers logging storage capacity in hot, cold, and LTO forms to whatever specifications are provided by the client.	Yes

SR 2.9 RE 1	Warn when audit record storage capacity threshold reached	The control system shall provide the capability to issue a warning when the allocated audit record storage volume reaches a configurable percentage of maximum audit record storage capacity.	Dispel's storage system provides a warning when capacity is being reached.	Yes
SR 2.10	**Response to audit processing failures**	The control system shall provide the capability to alert personnel and prevent the loss of essential services and functions in the event of an audit processing failure. The control system shall provide the capability to support appropriate actions in response to an audit processing failure according to commonly accepted industry practices and recommendations.	Dispel's logging and audit systems sit in a segmented area from those systems responsible for performing essential services and functions. An alert is provided when a log server experiences a failure.	Yes
SR 2.11	**Timestamps**	The control system shall provide timestamps for use in audit record generation.	All logged activities are time stamped.	Yes
SR 2.11 RE 1	Internal time synchronization	The control system shall provide the capability to synchronize internal system clocks at a configurable frequency.	All Dispel components sit on virtualized platforms which only time sync to Coordinated Universal Time per the Network Time Protocol. The frequency with which synchronizations occur cannot be specified by the customer at this time.	Partial

SR 2.11 RE 2	Protection of time source integrity	The time source shall be protected from unauthorized alteration and shall cause an audit event upon alteration.	The time source for all Dispel components are the publicly referenced atomic clocks whose defences - and cross referenceable structure - serve to prevent malicious alteration. Reference is made to these Stratum 0 clocks via Stratum 1 NTP servers supplied and maintained by the cloud(s) upon which the Dispel system is deployed (for example, Amazon Time Sync Service).	Yes
SR 2.12	**Non-repudiation**	The control system shall provide the capability to determine whether a given human user took a particular action.	Dispel can provide session recordings of all activities performed by a user through a virtual desktop. Session recording is rendered as an optional service.	Yes
SR 2.12 RE 1	Non-repudiation for all users	The control system shall provide the capability to determine whether a given user (human, software process or device) took a particular action.	Human and machine users are both assigned whitelisted device, protocol, session level access. If logging is activated by the customer, this level of granularity should provide insight into whether a particular user was responsible for a given action. We would stress that action and effect are different. A simplistic example being an adversary reversing the wires on a servo so that, in spite of the logs reporting that a person's action was to close a valve, the effect was the valve being opened.	Yes

IEC 62443-3-3 FR 3 - System Integrity

Part	Title	Requirement	Dispel Product/Feature	
SR 3.1	**Communication integrity**	The control system shall provide the capability to protect the integrity of transmitted information.	Data sent over Dispel's remote access system traverses a colorless core, moving target defense software defined wide area network built over any of 7 major commercial public cloud provider or, depending upon the customer, private or government clouds. Except if specified by the customer, Dispel encrypts all transmission within the network such that they exceed CNSA Suite guidelines – specifically, by using AES-256 with independent 4096-bit keys used for the initial key exchange. SR 3.1 goes further in the supplemental guidance section, however, in calling for hardening of hardware components to meet relevant environmental risks to signal integrity. Dispel provides ruggedized form-factor Wicket ESIs to the specifications of the customer. While case-by-case, typical ruggedized Wicket ESI form factors are tested to align with IEC 60068-2-64 and IEC 60068-2-27.	Yes
SR 3.1 RE 1	Cryptographic integrity protection	The control system shall provide the capability to employ cryptographic mechanisms to recognize changes to information during communication.	Except where specified by the customer to the contrary, all data sent over a Dispel remote access network is twice encrypted using AES-256 with independent 4096-bit keys used for the initial key exchange. Alternative options include Curve25519 and certain post-quantum prototypes.	Yes

SR 3.2	**Malicious code protection**	The control system shall provide the capability to employ protection mechanisms to prevent, detect, report and mitigate the effects of malicious code or unauthorized software. The control system shall provide the capability to update the protection mechanisms.	Dispel deploys anti-virus software, process whitelisting, and protocol whitelisting on a disposable virtual desktop – coupled with logging and tieback to the Control System's SIEM to prevent, detect, and report on malicious code or unauthorized software injection attempts. As a mitigation measure, attention should be drawn to the disposability of the virtual desktops – the solution to concern around an infection on the virtual desktop to simply destroy and replace the virtual desktop with another provisioned on a distinct hypervisor. Virtual desktops are built with the latest patches and, therefore, protection mechanisms, each time they are launched.	Yes

SR 3.2 RE 1	Malicious code protection on entry and exit points	The control system shall provide the capability to employ malicious code protection mechanisms at all entry and exit points.	Dispel serves as the remote access point for control systems. In that role, Dispel deploys anti-virus software, process whitelisting, and protocol whitelisting on a disposable virtual desktop – coupled with logging and tieback to the Control System's SIEM to prevent, detect, and report on malicious code or unauthorized software injection attempts. As a mitigation measure, attention should be drawn to the disposability of the virtual desktops – the solution to concern around an infection on the virtual desktop to simply destroy and replace the virtual desktop with another provisioned on a distinct hypervisor. Virtual desktops are built with the latest patches and, therefore, protection mechanisms, each time they are launched.	Yes
SR 3.2 RE 2	Central management and reporting for malicious code protection	The control system shall provide the capability to manage malicious code protection mechanisms.	As provided in the notes section of SR 3.2 RE 2, this mechanism was expected by the authors of IEC 62443-3-3 to be delivered through an integration with either a SIEM, endpoint infrastructure management systems, or a combination thereof. Dispel provides management over code protection tools within the remote access system (antivirus software on virtual desktops), but also ties into the customer's SIEM to support unified oversight.	Yes

SR 3.3	**Security functionality verification**	The control system shall provide the capability to support verification of the intended operation of security functions and report when anomalies are discovered during FAT, SAT and scheduled maintenance. These security functions shall include all those necessary to support the security requirements specified in this standard.	When testing of the nature described in SR 3.3 and its supplemental guidance section arise, Dispel not only provides the customer with the ability to have testers assess the live system, but also provides the customer with a replica environment the testers can run initial verifications against without potentially destabilizing operations. Tests may be scripted/automated or manual in nature and may be run during normal or offline operations.	Yes
SR 3.3 RE 1	Automated mechanisms for security functionality verification	The control system shall provide the capability to employ automated mechanisms to support management of security verification during FAT, SAT and scheduled maintenance.	When testing of the nature described in SR 3.3 and its supplemental guidance section arise, Dispel not only provides the customer with the ability to have testers assess the live system, but also provides the customer with a replica environment the testers can run initial verifications against without potentially destabilizing operations. Tests may be scripted/automated or manual in nature and may be run during normal or offline operations.	Yes

SR 3.3 RE 2	Security functionality verification during normal operation	The control system shall provide the capability to support verification of the intended operation of security functions during normal operations.	When testing of the nature described in SR 3.3 and its supplemental guidance section arise, Dispel not only provides the customer with the ability to have testers assess the live system, but also provides the customer with a replica environment the testers can run initial verifications against without potentially destabilizing operations. Tests may be scripted/automated or manual in nature and may be run during normal or offline operations.	Yes
SR 3.4	**Software and information integrity**	The control system shall provide the capability to detect, record, report and protect against unauthorized changes to software and information at rest.	Due to the description provided in the supplemental guidance section of SR 3.4, we strongly believe the focus of the Author's of IEC 62443-3-3 was on changes made to endpoints, rather than remote infrastructure. For this reason, we have labeled this section and SR 3.4 RE 1 Not Applicable. Further, since Dispel serves as the remote access conduit, rather than the Control System, and the Dispel infrastructure is ephemeral, no data is ever at rest within the Dispel infrastructure except in audit storage segments. For audit related alarms and storage, if Dispel is in control of that storage (ie, it is not being piped to an on-prem storage array at the customer), Dispel has audit records stored on WORM data tapes in secured, geographically dispersed facilities supplied and maintained by Partners (for example, Amazon Web Services' S3 Glacier Deep Archive).	Not Applicable

SR 3.4 RE 1	Automated notification about integrity violations	The control system shall provide the capability to use automated tools that provide notification to a configurable set of recipients upon discovering discrepancies during integrity verification.	Due to the description provided in the supplemental guidance section of SR 3.4, we strongly believe the focus of the Author's of IEC 62443-3-3 was on changes made to endpoints, rather than remote infrastructure. For this reason, we have labeled this section SR 3.4 Not Applicable. Further, since Dispel serves as the remote access conduit, rather than the Control System, and the Dispel infrastructure is ephemeral, no data is ever at rest within the Dispel infrastructure.	Not Applicable
SR 3.5	**Input validation**	The control system shall validate the syntax and content of any input which is used as an industrial process control input or input that directly impacts the action of the control system.	Dispel serves as the remote access conduit to HMIs that would have input validation mechanisms on them. It is not, itself, the input mechanism.	Not Applicable
SR 3.6	**Deterministic output**	The control system shall provide the capability to set outputs to a predetermined state if normal operation cannot be maintained as a result of an attack.	Please note that Dispel serves only as the remote access conduit for the control system and, therefore, its adherence to 3.6 should not be misconstrued as providing internal safeguards to the control system from an attack launched on premises. Dispel's hardware Wicket ESIs can be configured to fail-to-closed if an attack is detected inside the perimeter. This requires an additional piece of hardware and configuration with the customer's SIEM or master alarm system.	Yes

SR 3.7	**Error handling**	The control system shall identify and handle error conditions in a manner such that effective remediation can occur. This shall be done in a manner which does not provide information that could be exploited by adversaries to attack the IACS unless revealing this information is necessary for the timely troubleshooting of problems.	Dispel supplies verbose error messages when systems have experienced failures that, if reviewed by a Dispel employee or trained third party with appropriate access credentials, can permit troubleshooting to take place efficiently. These error messages do not reveal information that would aid an attacker in damaging the Dispel system further.	Yes
SR 3.8	**Session integrity**	The control system shall provide the capability to protect the integrity of sessions. The control system shall reject any usage of invalid session IDs.	Users are only able to reach a virtual desktop supplied by Dispel using Microsoft Remote Desktop Protocol which, in turn, relies upon a uniquely generated session ID to maintain the connection.	Yes
SR 3.8 RE 1	Invalidation of session IDs after session termination	The control system shall provide the capability to invalidate session IDs upon user logout or other session termination (including browser sessions).	When a session is terminated, the associated virtual desktop is destroyed. This achieves the same outcome as invalidating the session ID, as there is nothing to which the session ID can associate any longer.	Yes
SR 3.8 RE 2	Unique session ID generation	The control system shall provide the capability to generate a unique session ID for each session and treat all unexpected session IDs as invalid.	To initiate a connection to a remote access conduit supplied by Dispel, a user must access a virtual desktop using RDP. RDP, in turn, generates a unique session ID for each session and treats all unexpected session IDs as invalid.	Yes

SR 3.8 RE 3	Randomness of session IDs	The control system shall provide the capability to generate unique session IDs with commonly accepted sources of randomness.	To initiate a connection to a remote access conduit supplied by Dispel, a user must access a virtual desktop using RDP. RDP, in turn, generates a unique session ID for each session and treats all unexpected session IDs as invalid. However, there is no reason to believe that these session IDs are created with an acceptable degree of randomness. To overcome this, Dispel relies upon a combination of IP Whitelisting at the virtual desktop level, and the randomly generated locations of these virtual desktops, to prevent the hijacking for which SR 3.8 RE 3 was written.	Yes
SR 3.9	**Protection of audit information**	The control system shall protect audit information and audit tools (if present) from unauthorized access, modification and deletion.	Where Dispel is in control of the storage of audit information rather than the customer, Dispel has audit records stored on WORM data tapes stored in secured, geographically dispersed facilities supplied and maintained by Partners (for example, Amazon Web Services' S3 Glacier Deep Archive).	Yes

SR 3.9 RE 1	Audit records on write-once media	The control system shall provide the capability to produce audit records on hardware-enforced write-once media.	Dispel offers, and strongly encourages its customers to use, Write-Once Ready Many Linear Tape Open recording systems for audit records kept on-premises. For customers who prefer to rely upon Dispel to manage the storage and retention of data, Dispel has audit records placed on WORM tape in geographically dispersed secured facilities supplied and maintained by Partners (for example, Amazon Web Services' S3 Glacier Deep Archive service).	Yes

IEC 62443-3-3 FR 4 - Data Confidentiality

Part	Title	Requirement	Dispel Product/Feature	
SR 4.1	**Information confidentiality**	The control system shall provide the capability to protect the confidentiality of information for which explicit read authorization is supported, whether at rest or in transit.	Dispel's networks are colorless core, meaning all data, irrespective of its confidentiality tier or external factors such as zone traversal, is encrypted to the same level. The standard encryption treatment employed by Dispel in 2022 is to encrypt data with AES 256 using 4096-bit keys for the initial key exchange. All audit data stored at rest is also encrypted using AES 256.	Yes
SR 4.1 RE 1	Protection of confidentiality at rest or in transit via untrusted networks	The control system shall provide the capability to protect the confidentiality of information at rest and remote access sessions traversing an untrusted network.	Dispel's networks are colorless core, meaning all data, irrespective of its confidentiality tier or external factors such as zone traversal, is encrypted to the same level. The standard encryption treatment employed by Dispel in 2022 is to encrypt data with AES 256 using 4096-bit keys for the initial key exchange. All audit data stored at rest is also encrypted using AES 256.	Yes
SR 4.1 RE 2	Protection of confidentiality across zone boundaries	The control system shall provide the capability to protect the confidentiality of information traversing any zone boundary.	Dispel's networks are colorless core, meaning all data, irrespective of its confidentiality tier or external factors such as zone traversal, is encrypted to the same level. The standard encryption treatment employed by Dispel in 2022 is to encrypt data with AES 256 using 4096-bit keys for the initial key exchange. All audit data stored at rest is also encrypted using AES 256.	Yes

SR 4.2	**Information persistence**	The control system shall provide the capability to purge all information for which explicit read authorization is supported from components to be released from active service and/or decommissioned.	Dispel purges all information from components before releasing them from active service and/or decommissioning them.	Yes
SR 4.2 RE 1	Purging of shared memory resources	The control system shall provide the capability to prevent unauthorized and unintended information transfer via volatile shared memory resources.	Dispel purges all information from components, including RAM, before releasing them from active service and/or decommissioning them.	Yes
SR 4.3	**Use of cryptography**	If cryptography is required, the control system shall use cryptographic algorithms, key sizes and mechanisms for key establishment and management according to commonly accepted security industry practices and recommendations.	Dispel exceeds CNSA Suite guidelines, employing AES 256 with 4096-bit keys. Dispel can, upon request, switch to Curve25519 or certain prototype post-quantum algorithms of the customer's choosing.	Yes

IEC 62443-3-3 FR 5 - Restricted Data Flow

Part	Title	Requirement	Dispel Product/Feature	
SR 5.1	**Network segmentation**	The control system shall provide the capability to logically segment control system networks from non-control system networks and to logically segment critical control system networks from other control system networks.	By default, Dispel provides Layer 3 logical network segmentation to critical control systems from external connection. In circumstances requiring physical medium breaks, Dispel support data diodes.	Yes
SR 5.1 RE 1	Physical network segmentation	The control system shall provide the capability to physically segment control system networks from non-control system networks and to physically segment critical control system networks from non-critical control system networks.	Dispel provides Layer 3 network segmentation and data diodes for physical breaks.	Yes – with note
SR 5.1 RE 2	Independence from non-control system networks	The control system shall have the capability to provide network services to control system networks, critical or otherwise, without a connection to non-control system networks.	Dispel links directly from the control system network to the Enclave SD-WAN. It does not require a connection to non-control system networks. In environments where all hardline routable networks cross non-critical networks, a cellular backhaul may be used from the Wicket ESI to the Enclave.	Yes
SR 5.1 RE 3	Logical and physical isolation of critical networks	The control system shall provide the capability to logically and physically isolate critical control system networks from non-critical control system networks.	Dispel's network routing isolates critical control systems from other network traffic. In the OSI model, Dispel cannot interfere with other physical hardware connections installed in the control system. But if all external traffic connections to critical control systems route through Dispel, then isolation may be enforced.	Yes – with note

SR 5.2	**Zone boundary protection**	The control system shall provide the capability to monitor and control communications at zone boundaries to enforce the compartmentalization defined in the risk-based zones and conduits model.	Dispel's SD-WAN provides several defense-in-depth zone boundaries; including firewalls, encrypted tunnels, and monitoring. Network traffic routing through Dispel may be logged. The SD-WAN Enclave enforces compartmentalization of zones connected to the Dispel environment.	Yes
SR 5.2 RE 1	Deny by default, allow by exception	The control system shall provide the capability to deny network traffic by default and allow network traffic by exception (also termed deny all, permit by exception).	Dispel's firewall rules deny all network traffic except explicitly authorized connections by default.	Yes
SR 5.2 RE 2	Island mode	The control system shall provide the capability to prevent any communication through the control system boundary (also termed island mode).	This is accomplished by disabling the Enclave. The Wicket ESI provides the uplink from the local control network to the remote access Enclave. If no Enclave exists, the Wicket ESI cannot route traffic.	Yes
SR 5.2 RE 3	Fail close	The control system shall provide the capability to prevent any communication through the control system boundary when there is an operational failure of the boundary protection mechanisms (also termed fail close). This 'fail close' functionality shall be designed such that it does not interfere with the operation of a SIS or other safety-related functions.	If the Enclave boundary mechanism fails, the Wicket ESI will lose the ability to route traffic through from the control network to the external Internet. Unless the control system depends on outside connections to function--which it should not--this fail close method will not affect the underlying control system.	Yes

SR 5.3	**General purpose person-to-person communication restrictions**	The control system shall provide the capability to prevent general purpose person-to-person messages from being received from users or systems external to the control system.	All Enclaves come equipped with firewall rules, including blocked sites and services. Admins can choose to block person-to-person communication tools (like Twitter, Facebook, etc as referenced in IEC 62443). File uploads can also be disabled for operators, preventing malware from getting to the control system.	Yes
SR 5.3 RE 1	Prohibit all general purpose person-to-person communications	The control system shall provide the capability to prevent both transmission and receipt of general purpose person-to-person messages.	When connected to a control system via Dispel, all external Internet connections are blocked. Dispel's SD-WAN does not allow split tunneling.	Yes
SR 5.4	**Application partitioning**	The control system shall provide the capability to support partitioning of data, applications and services based on criticality to facilitate implementing a zoning model.	Each part of Dispel's architecture lives on single tenant virtual machines. By default, systems are partitioned for security and redundancy.	Yes

IEC 62443-3-3 FR 6 – Timely Response To Events

Part	Title	Requirement	Dispel Product/Feature	
SR 6.1	**Audit log accessibility**	The control system shall provide the capability for authorized humans and/or tools to access audit logs on a read-only basis.	Dispel provides audit logs of who did what and when. Fully configurable by clients, Dispel's audit system includes monitoring, audit logging, IP filtering, and third-party security integrations. User roles and responsibilities are customizable, so (for example) your IT/ops team can monitor logs without being able to modify data.	Yes
SR 6.1 RE 1	Programmatic access to audit logs	The control system shall provide programmatic access to audit records using an application programming interface (API).	Dispel's logging service includes a JSON-based REST API.	Yes
SR 6.2	Continuous monitoring	The control system shall provide the capability to continuously monitor all security mechanism performance using commonly accepted security industry practices and recommendations to detect, characterize and report security breaches in a timely manner.	Dispel provides data visualization and monitoring for continous monitoring by security teams. Our syslogging audit system also includes unsupervised machine learning to help find patterns in data for anomaly and outlier detection.	Yes

IEC 62443-3-3 FR 7 – Resource Availability

Part	Title	Requirement	Dispel Product/Feature	
SR 7.1	**Denial of service protection**	The control system shall provide the capability to operate in a degraded mode during a DoS event.	Dispel will continue to operate at lower bandwidths experienced as a result of a DoS event.	Yes
SR 7.1 RE 1	Manage communication loads	The control system shall provide the capability to manage communication loads (such as using rate limiting) to mitigate the effects of information flooding types of DoS events.	Dispel manages communication loads by employing IP whitelisting between network components, being outbound-only at the Wicket ESI for establishing a connection to the first point in a remote access network, and for being unresponsive to inbound communications on all components once a connection is established (other than from that one IP address, of course). These actions have the effect of mitigating the risk of at DoS event taking place.	Yes
SR 7.1 RE 2	Limit DoS effects to other systems or networks	The control system shall provide the capability to restrict the ability of all users (humans, software processes and devices) to cause DoS events which affect other control systems or networks.	Dispel can throttle the amount of bandwidth consumed by any given user, be they human or machine.	Yes
SR 7.2	Resource management	The control system shall provide the capability to limit the use of resources by security functions to prevent resource exhaustion.	Dispel's components are positioned in virtualized environments which allow their resource consumption rates to be capped without relying upon any other part of the Dispel system functioning properly.	Yes

SR 7.3	**Control system backup**	The identity and location of critical files and the ability to conduct backups of user-level and system-level information (including system state information) shall be supported by the control system without affecting normal plant operations.	All backup data on Dispel's system is run from resource pools that are independent of those used to support plant operations.	Yes
SR 7.3 RE 1	Backup verification	The control system shall provide the capability to verify the reliability of backup mechanisms.	Backup mechanisms relevant to Dispel can be checked through the Dispel management console.	Yes
SR 7.3 RE 2	Backup automation	The control system shall provide the capability to automate the backup function based on a configurable frequency.	Dispel allows automated backup cycling of Dispel components to be set according to whatever schedule the customer desires.	Yes
SR 7.4	**Control system recovery and reconstitution**	The control system shall provide the capability to recover and reconstitute to a known secure state after a disruption or failure.	Dispel's components recover and reconstitute from "golden images" which, if tested to determine their security state, serve to meet the requirements of SR 7.4.	Yes
SR 7.5	**Emergency power**	The control system shall provide the capability to switch to and from an emergency power supply without affecting the existing security state or a documented degraded mode.	Dispel's components sit in datacenters which operate with Uninterrupted Power Supplies (UPS). Likewise, Dispel Wicket ESIs positioned on premises can be outfitted with a UPS.	Yes
SR 7.6	**Network and security configuration settings**	The control system shall provide the capability to be configured according to recommended network and security configurations as described in guidelines provided by the control system supplier. The control system shall provide an interface to the currently deployed network and security configuration settings.	Dispel's network topology is completely configurable.	Yes

SR 7.6 RE 1	Machine-readable reporting of current security settings	The control system shall provide the capability to generate a report listing the currently deployed security settings in a machine-readable format.	Dispel's system provides a readout of security settings within a deployment.	Yes
SR 7.7	**Least functionality**	The control system shall provide the capability to specifically prohibit and/or restrict the use of unnecessary functions, ports, protocols and/or services.	Dispel's system uses a whitelisted approach to ports and protocols. The virtual desktop component of Dispel deployments serves to prevent and/or restrict function and application accessibility.	Yes
SR 7.8	**Control system component inventory**	The control system shall provide the capability to report the current list of installed components and their associated properties.	All Dispel components are listed along with their specifications in the Dispel management console.	Yes

Mapping For IEC 62443-4-1: Secure Product Development Lifecycle Requirements

This part of IEC 62443 specifies process requirements for the secure development of products used in industrial automation and control systems. It defines a secure development life-cycle (SDL) for the purpose of developing and maintaining secure products. This life-cycle includes security requirements definition, secure design, secure implementation (including coding guidelines), verification and validation, defect management, patch management and product end-of-life. These requirements can be applied to new or existing processes for developing, maintaining and retiring hardware, software or firmware for new or existing products. These requirements apply to the developer and maintainer of the product, but not to the integrator or user of the product.

IEC 62443-4-1 Practice 1 – Security Management

Part	Title	Requirement	Dispel Product/Feature	
SM-1	**Development process**	A general product development/maintenance/support process shall be documented and enforced that is consistent and integrated with commonly accepted product development processes that include, but are not limited to: A) Configuration management with change controls and audit logging; B) Product description and requirements definition with requirements traceability; C) Software or hardware design and implementation practices, such as modular design; D) Repeatable testing verification and validation process; E) Review and approval of all development process records; and F) Life-cycle support.	Dispel's A.14.1 Secure Development Policy governs secure development and maintenance; and security vulnerability assessments for our organization. The secure development and maintenance policy addresses areas including risk assessment for the development process, securing the development environment, secure engineering principles, security requirements for new information systems, public networks, checking and testing implementation of security requirements, code versioning and repository control, change control, and protection of test data. The A.12.2 Change Management Policy governs testing and maintenance for code.	Yes

SM-2	**Identification of responsibilities**	A process shall be employed that identifies the organizational roles and personnel responsible for each of the processes required by this document.	Security roles and responsibilities for the processes required by this document are laid out within the ISMS scope defined in Dispel's 03.1 ISMS Scope Document. Various roles and responsibilities are governed by individual policies. For example, the 04.2 Personal Data Protection Policy addresses Data Privacy Officers, while A.12.2 Change Management Policy establishes the Head of QA/QC.	Yes
SM-3	**Identification of applicability**	A process shall be employed for identifying products (or parts of products) to which this document applies.	The 03.1 ISMS Scope Document defines the boundaries within Dispel's physical and digital environments governed by security policies.	Yes
SM-4	**Security expertise**	A process shall be employed for identifying and providing security training and assessment programs to ensure that personnel assigned to the organizational roles and duties specified in 5.4, have demonstrated security expertise appropriate for those processes.	The 12.1 Training and Awareness Plan establishes the standard procedures for training all employees to inform and orient them to Dispel's security practices, as well as raise awareness around cyber and operational security. Dispel provides all employees with security training and briefings commensurate with their involvement with sensitive information. This training covers topics such as general security awareness, device security, insider threat awareness, reporting requirements, and data protection.	Yes

SM-5	**Process scoping**	A process, that includes justification by documented security analysis, shall be employed to identify the parts of this document that are applicable to a selected product development project. Justification for scoping the level of compliance of a project to this document shall be subject to review and approval by personnel with the appropriate security expertise (see 5.6).	Dispel does not have a process for specific security analysis documentation for the purpose of scoping IEC 62443 implementation. Security reviews are conducted during the architecting, development, testing, and deployment phases. Feedback is received from clients and integrated into ongoing product improvement cycles.	Yes
SM-6	**File integrity**	A process shall be employed to provide an integrity verification mechanism for all scripts, executables and other important files included in a product.	File integrity for Dispel code placed into production environments is protected by code signing and MD5 hashes. For Dispel macOS, iOS, and Windows applications, code is signed by controlled developer certificates accepted by Apple and Microsoft. Version control generates an MD5 hash for stored server production code.	Yes
SM-7	**Development environment security**	A process that includes procedural and technical controls shall be employed for protecting the product during development, production and delivery. This includes protecting the product or product update (patch) during design, implementation, testing and release.	The A.14.1 Secure Development Policy addresses development environment security. The A.8.2 IT Security Policy covers the security for the physical devices used for software development. A.15 Supplier Security Policy addresses third-party safety, especially with regards to data privacy (including GDPR and CCPA). In situations when employees may use their own devices, the A.6.1 Bring Your Own Device BYOD Policy applies.	Yes

SM-8	**Controls for private keys**	The supplier shall have procedural and technical controls in place to protect private keys used for code signing from unauthorized access or modification.	The A.9.2 Password Policy includes procedures for handling private keys used for code signing. This includes user obligations, approved storage systems, and sharing guidelines.	Yes
SM-9	**Security requirements for externally provided components**	A process shall be employed to identify and manage the security risks of all externally provided components used within the product.	The 07.1 Risk Assessment and Risk Treatment Methodology defines the methodology for assessment and treatment of information risks at Dispel, and to define the acceptable level of risk according to the ISO/IEC 27001 standard.	Yes
SM-10	**Custom developed components from third-party suppliers**	A process shall be employed to ensure that product development life-cycle processes for components from a third-party supplier conform to the requirements used in this document when they meet the following criteria: A) The components are developed specifically for a single supplier for a specific purpose; and B) The components can have an impact on security.	Dispel does not outsource software development to third-party suppliers for components developed specifically for Dispel.	Yes

SM-11	**Assessing and addressing security-related issues**	A process shall be employed for verifying that a product or a patch is not released until its security-related issues have been addressed and tracked to closure (see 10.5). This includes issues associated with: A) Requirements (see Clause 6); B) Secure by design (see Clause 7); C) Implementation (see Clause 8); D) Verification/validation (see Clause 9); and, E) Defect management (see Clause 10).	The A.14.1 Secure Development Policy Change Control section addresses security-related issues. When code moves from a feature branch to staging to production, it is subject to a code review when the pull request is made to merge the branch into staging. This code review includes closing security-related issues.	Yes
SM-12	**Process verification**	A process shall be employed for verifying that, prior to product release, all applicable security-related processes required by this specification (see 5.7) have been completed with records documenting the completion of each process.	Within A.14.1 Secure Development Policy, there is a defined role responsible to define the methodology, responsibilities and the timing of checking whether all the security requirements from the Security Requirements Specification of A.14.1 have been met, and whether the system is acceptable for production.	Yes
SM-13	**Continuous improvement**	A process shall be employed for continuously improving the SDL. This process shall include the analysis of security defects in component/subsystem/system technologies that escape to the field.	Dispel's Secure Development Policy must be reviewed and, in necessary, updated at least once per year.	Yes

IEC 62443-4-1 Practice 2 – Specification of Security Requirements

Part	Title	Requirement	Dispel Product/Feature	
SR-1	**Product security context**	A process shall be employed to ensure that the intended product security context is documented.	Product feature development includes considering security implications. Typically this is a discussion between design and development, with input from operations and sales.	Yes

SR-2	**Threat model**	A process shall be employed to ensure that all products shall have a threat model specific to the current development scope of the product with the following characteristics (where applicable): A) Correct flow of categorized information throughout the system; B) Trust boundaries; C) Processes; D) Data stores; E) Interacting external entities; F) Internal and external communication protocols implemented in the product; G) Externally accessible physical ports including debug ports; H) Circuit board connections such as Joint Test Action Group (JTAG) connections or debug headers which might be used to attack the hardware; I) Potential attack vectors including attacks on the hardware, if applicable; J) Potential threats and their severity as defined by a vulnerability scoring system (for example, CVSS); K) Mitigations and/or dispositions for each threat; L) Security-related issues identified; and, M) External dependencies in the form of drivers or third-party applications (code that is not developed by the supplier) that are linked into the application. The threat model shall be reviewed and verified by the development team to ensure that it is correct and understood. The threat model shall be reviewed periodically (at least once a year) for released products and updated if required in response to the emergence of new threats to the product even if the design does not change. Any issues identified in the threat model shall be addressed as defined in 10.4 and 10.5.	Dispel does not have processes covering all of these categories. During development, Dispel looks specifically at (a) information flow, (b) boundaries, (c) processes, (d) data stores, (e) interacting external entities, (f) protocols, and (l) dependencies. Some threats and possible mitigations are considered (k); for example, types of threat actors, their intent, and attack routes are considered during development. Dispel also hardware supply requirements of the U.S. National Defense Authorization Act §889(a)(1)(B). Threat models are discussed, but not fully documented by the development team for all features.	Partial

SR-3	**Product security requirements**	A process shall be employed for ensuring that security requirements are documented for the product/feature under development including requirements for security capabilities related to installation, operation, maintenance and decommissioning.	Dispel's Secure Development Policy outlines documentation for security requirements for product/features under development. This includes third-party conformance assessments.	Yes
SR-4	**Product security requirements content**	A process shall be employed for ensuring that security requirements include the following information: A) The scope and boundaries of the component or system, in general terms in both a physical and a logical way; and B) The required capability security level (SL-C) of the product.	Network system architecture includes scope and boundaries of Dispel components and systems. These may include security requirements, when tied to business use-case specifications.	Yes
SR-5	**Security requirements review**	A process shall be employed to ensure that security requirements are reviewed, updated as necessary and approved to ensure clarity, validity, alignment with the threat model (discussed in 6.3), and their ability to be verified. Each of the following representative disciplines shall participate in this process. Personnel may be assigned to more than one discipline except for testers, who shall remain independent: A) Architects/developers (those who will implement the requirements); B) Testers (those who will validate that the requirements have been met); C) Customer advocate (such as sales, marketing, product management or customer support); and, D) Security advisor.	During the development process, architects/developers document their code which may include security requirements. Requirements are derived from input from customer advocates, testers, engineering, and management. At times, security advisors--including legal counsel and penetration testers--will also be consulted. Specific threat models are not often detailed during requirement documentation.	Yes

IEC 62443-4-1 Practice 3 – Secure by Design

Part	Title	Requirement	Dispel Product/Feature	
SD-1	**Secure design principles**	A process shall be employed for developing and documenting a secure design that identifies and characterizes each interface of the product, including physical and logical interfaces, to include: A) An indication of whether the interface is externally accessible (by other products), or internally accessible (by other components of the product), or both; B) Security implications of the product security context (see Clause 6) on the external interface; C) Potential users of the interface and the assets that can be accessed through it (directly or indirectly); D) A determination of whether access to the interface crosses a trust boundary; E) Security considerations, assumptions and/or constraints associated with the use of the interface within the product security context, including applicable threats; F) The security roles, privileges/rights and access control permissions needed to use the interface and to access the assets defined in c) above; G) The security capabilities and/or compensating mechanisms used to safeguard the interface and the assets defined in c) above, including input validation as well as output and error handling; H) The use of third-party products to implement the interface and their security capabilities; I) Documentation that describes how to use the interface if it is externally accessible; and, J) Description of how the design mitigates the threats identified in the threat model.	During the design and development phase, Dispel considers (A) Externally and internally accessible interfaces; (B) Security context of external interfaces; (C) Users of the interfaces; (D) Whether access crosses a trust boundary; (E) Security considerations; (F) Security roles and rights; (G) Safeguards; and, (H) Third-party products. Dispel uses CSA CAIQ risk assessments to review third-party products and their potential impact on the platform. Dispel also employs independent firms to review our code for security.	Yes

SD-2	**Defense in depth design**	A process shall be employed to implement multiple layers of defense using a risk based approach based on the threat model. This process shall be employed for assigning responsibilities to each layer of defense. NOTE 1 Each layer provides additional defense mechanisms. NOTE 2 It is possible for any layer to be compromised; therefore, secure design principles (see 7.2) are applied to each layer. NOTE 3 The objective is to reduce the attack surface of the subsequent layers.	Dispel considers and implements multiple layers of defense in depth in its design. Designs also incorporate varying safeguards for use when the security context changes--for example, the level of sensitivity of the facility Dispel is installed in may dictate additional mandatory product features are active. Dispel's design covers Notes 1, 2, and 3.	Yes
SD-3	**Security design review**	A process shall be employed for conducting design reviews to identify, characterize and track to closure security-related issues associated with each significant revision of the secure design including but not limited to: A) Security requirements (see Clause 6) that were not adequately addressed by the design; NOTE 1 Requirements allocation, including security requirements, is part of typical design processes. B) Threats and their ability to exploit product interfaces, trust boundaries, and assets (see 7.2); and, C) Identification of secure design practices (see 7.5) that were not followed (for example, failure to apply principle of least privilege). NOTE 2 Characterizing threats and their ability to exploit interfaces is often referred to as threat modelling.	Dispel conducts design reviews when promoting an architecture to development status. These reviews range from formal to informal, and may include security-related discussions. Dispel uses a developer-first method for secure software development. We engage GitHub Advanced Security for continuous independent static application security testing (SAST) and dependency vulnerability checking. Our products undergo independent penetration testing at least annually. Our internal security is assessed by independent auditors.	Yes

SD-4	**Secure design best practices**	A process shall be employed to ensure that secure design best practices are documented and applied to the design process. These practices shall be periodically reviewed and updated. Secure design practices include but are not limited to: A) Least privilege (granting only the privileges to users/software necessary to perform intended operations); B) Using proven secure components/designs where possible; C) Economy of mechanism (striving for simple designs); D) Using secure design patterns; E) Attack surface reduction; F) Documenting all trust boundaries as part of the design; and, G) Removing debug ports, headers and traces from circuit boards used during development from production hardware or documenting their presence and the need to protect them from unauthorized access.	Dispel's A.14.1 Secure Development Policy governs secure development and maintenance; and security vulnerability assessments for our organization. These policies incorporate many of the practices listed here in SD-4 and others.	Yes

IEC 62443-4-1 Practice 4 – Secure Implementation

Part	Title	Requirement	Dispel Product/Feature	
SI-1	**Security implementation review**	A process shall be employed to ensure that implementation reviews are performed for identifying, characterizing and tracking to closure security-related issues associated with the implementation of the secure design including: A) Identification of security requirements (see Clause 6) that were not adequately addressed by the implementation; NOTE Requirements allocation, including security requirements, is part of typical design processes. B) Identification of secure coding standards (see 8.4) that were not followed (for example, use of banned functions or failure to apply principle of least privilege); C) Static Code Analysis (SCA) for source code to determine security coding errors such as buffer overflows, null pointer dereferencing, etc. using the secure coding standard for the supported programming language. SCA shall be done using a tool if one is available for the language used. In addition, static code analysis shall be done on all source code changes including new source code. D) Review of the implementation and its traceability to the security capabilities defined to support the security design (see Clause 7); and, E) Examination of threats and their ability to exploit implementation interfaces, trust boundaries and assets (see 7.2 and 7.3).	Dispel uses a developer-first method for secure software development. We engage GitHub Advanced Security for continuous independent static application security testing (SAST) and dependency vulnerability checking. GitHub uses CodeQL, a semantic code analysis engine, to perform SAST on all code generated by the Dispel team when it is committed to repositories. Security issues are flagged and must be handled in pull requests as part of Dispel's code review process. We use the 2,000-plus CodeQL queries written and open sourced by the GitHub Security Lab and leading security researchers to find potential vulnerabilities in our code. Flagged security issues must be reviewed and closed before they code can be implemented in production.	Yes

SI-2	**Secure coding standards**	The implementation processes shall incorporate security coding standards that are periodically reviewed and updated and include at a minimum: A) Avoidance of potentially exploitable implementation constructs – implementation design patterns that are known to have security weaknesses; B) Avoidance of banned functions and coding constructs/design patterns – software functions and design patterns that should not be used because they have known security weaknesses; c) Automated tool use and settings (for example, for static analysis tools); D) Secure coding practices; E) Validation of all inputs that cross trust boundary. F) Error handling.	Dispel's secure coding policies include multiple standard practices, including those listed here.	Yes

IEC 62443-4-1 Practice 5 – Security Verification and Validation Testing

Part	Title	Requirement	Dispel Product/Feature	
SVV-1	**Security requirements testing**	A process shall be employed for verifying that the product security functions meet the security requirements and that the product handles error scenarios and invalid input correctly. Types of testing shall include: A) Functional testing of security requirements; B) Performance and scalability testing; and C) Boundary/edge condition, stress and malformed or unexpected input tests not specifically targeted at security.	Dispel code includes tests, error handling, and input validation. Tests include performance checks and edge conditions. Security tests are included.	Yes
SVV-2	**Threat mitigation test**	A process shall be employed for testing the effectiveness of the mitigation for the threats identified and validated in the threat model. Activities shall include: A) Creating and executing plans to ensure that each mitigation implemented to address a specific threat has been adequately tested to ensure that the mitigation works as designed; and B) Creating and executing plans for attempting to thwart each mitigation.	Dispel threat model mitigation is limited to architectural design reviews, client feedback, and penetration testing. Mitigation threat testing is performed by our third-party independent penetration testers.	Yes

SVV-3	**Vulnerability testing**	A process shall be employed for performing tests that focus on identifying and characterizing potential security vulnerabilities in the product. Known vulnerability testing shall be based upon, at a minimum, recent contents of an established, industry-recognized, public source for known vulnerabilities. Testing shall include: A) Abuse case or malformed or unexpected input testing focused on uncovering security issues. This shall include manual or automated abuse case testing and specialized types of abuse case testing on all external interfaces and protocols for which tools exist. Examples include fuzz testing and network traffic load testing and capacity testing; B) Attack surface analysis to determine all avenues of ingress and egress to and from the system, common vulnerabilities including but not limited to weak ACLs, exposed ports and services running with elevated privileges; C) Black box known vulnerability scanning focused on detecting known vulnerabilities in the product hardware, host or software components. For example, this could be a network based known vulnerability scan; D) For compiled software, software composition analysis on all binary executable files, including embedded firmware, delivered by the supplier to be installed for a product. This analysis shall detect the following types of problems at a minimum: 1) Known vulnerabilities in the product software components; 2) Linking to vulnerable libraries; 3) Security rule violations; and 4) Compiler settings that can lead to vulnerabilities; e) Dynamic runtime resource management testing that detects flaws not visible under static code analysis, including but not limited to denial of service conditions due to failing to release runtime handles, memory leaks and accesses made to shared memory without authentication. This testing shall be applied if such tools are available.	Dispel's secure development and maintenance program (Secure Development Policy) covers risk assessment for the development process, securing the development environment, secure engineering principles, new acquisition security, security requirements related to public networks, checking and testing the implementation of security requirements, repository management, version control, change control, and protection of test data. Dispel also includes automated security vulnerability assessments in our software. Our data sources for security alerts are: (i) MITRE's Common Vulnerabilities and Exposures (CVE) List, (ii) a combination of machine learning and human review to detect vulnerabilities in public commits on GitHub, (iii) maintainer security advisories on GitHub, and (iv) WhiteSource. Dispel uses the Common Vulnerability Scoring System version 3.1 for scoring security alerts. While Dispel conducts security reviews and testing, continuous testing across these formats is not conducted.	Yes

SVV-4	**Penetration testing**	A process shall be employed to identify and characterize security-related issues via tests that focus on discovering and exploiting security vulnerabilities in the product.	Dispel conducts penetration testing on a periodic basis.	Yes
SVV-5	**Independence of testers**	A process shall be employed to ensure that individuals performing testing are independent from the developers who designed and implemented the product according to Table 3. The levels of independence are defined as follows: • None – no independence required. Developer can perform the testing. • Independent person – the person who performs the testing cannot be one of the developers of the product. • Independent department – the person who performs the testing cannot report to the same first line manager as any developers of the product. Alternatively, they could be a member of a quality assurance (QA) department. • Independent organization – the person who performs the testing cannot be part of the same organization as any developers of the product. An organization can be a separate legal entity, a division of a company or a department of a company that reports to a different executive such as a vice president or similar level.	Dispel contracts with independent third-parties for penetrating testing. Within the organization, testing reviews are conducted by independent personnel from those developing the product.	Yes

IEC 62443-4-1 Practice 6 – Management of Security Related Issues

Part	Title	Requirement	Dispel Product/Feature	
DM-1	**Receiving notifications of security-related issues**	A process shall exist for receiving and tracking to closure security-related issues in the product reported by internal and external sources including at a minimum: A) Security verification and validation testers; B) Suppliers of third-party components used in the product; C) Product developers and testers; and D) Product users including integrators, asset owners, and maintenance personnel. NOTE External security verification and validation testers include researchers.	Dispel maintains two programs for responding to security-related issues: programmatic issues and data breaches. Programmatic issues are addressed by Dispel's security response program. Dispel's Data Breach Response and Notification Procedure (A.16 Data Breach Response and Notification Procedure) provides general principles and approach model to respond to, and mitigate breaches of personal data (a "personal data breach") in set circumstances. This Procedure may also be applicable for any other type of security incident The Procedure lays out the general principles and actions for successfully managing the response to a data breach as well as fulfilling the obligations surrounding the notification to Supervisory Authorities and individuals as required by the EU GDPR. The Data Breach Response Process is initiated when anyone who notices that a suspected/alleged or actual data breach occurs, and any member of the Data Breach Response team is notified. The team is responsible to determine if the breach should be considered a breach affecting personal data.	Yes

DM-2	Reviewing security-related issues	A process shall exist for ensuring that reported security-related issues are investigated in a timely manner to determine their: A) Applicability to the product; B) Verifiability; and, C) Threats that trigger the issue. NOTE Timeliness is driven by market forces.	Dispel maintains a process for handling reported security-related issues in a timely manner.	Yes
DM-3	Assessing security-related issues	A process shall be employed for analysing security-related issues in the product to include: A) Assessing their impact with respect to: 1) The actual security context in which they were discovered; 2) The product's security context (see Clause 6); and, 3) The product's defense in depth strategy (see Clause 7); B) Severity as defined by a vulnerability scoring system (for example, CVSS); C) Identifying all other products/product versions containing the security-related issue (if any); D) Identifying the root causes of the issue; and E) Identifying related security issues. For root cause analysis, a methodical approach such as that described in IEC 62740 [25] may be employed.	Dispel's response to security-related issues includes investigations of all of the categories in DM-3. Root cause analysis is performed when issues affect client SCADA systems.	Yes

DM-4	Addressing security-related issues	A process shall be employed for addressing security-related issues and determining whether to report them based on the results of the impact assessment (see 10.4). The supplier shall establish an acceptable level of residual risk that shall be applied when determining an appropriate way to address each issue. Options include one or more of the following: A) Fixing the issue through one or more of the following: 1) Defense in depth strategy or design change; 2) Addition of one or more security requirements and/or capabilities; 3) Use of compensating mechanisms; and/or, 4) Disabling or removing features; B) Creating a remediation plan to fix the problem; C) Deferring the problem for future resolution (reapply this requirement at some time in the future) and specifying the reason(s) and associated risk(s); D) Not fixing the problem if the residual risk is below the established acceptable level of residual risk. In all cases, the following shall be done as well: A) Inform other processes of the issue or related issue(s), including processes for other products/product revisions; and, B) Inform third parties if problems found in included third-party source code. When security-related issues are resolved recommendations to prevent similar errors from occurring in the future shall be evaluated. This process shall include a periodic review of open security-related issues to ensure that issues are being addressed appropriately. This periodic review shall at a minimum occur during each release or iteration cycle. NOTE When the resolution decision is to fix the security-related issue in the product implementation, the timing of the release of the fix can result in a patch (see Clause 12) or the fix can be deferred until the next release.	Dispel discloses vulnerabilities on a confidential basis. Specific rules relates to disclosure may apply, including regulations governing personal data breaches. In such circumstances Dispel's Data Breach Response and Notification Procedure (A.16 Data Breach Response and Notification Procedure) provides general principles and approach model to respond to, and mitigate breaches of personal data (a "personal data breach") in set circumstances. This Procedure may also be applicable for any other type of security incident.	Yes

DM-5	Disclosing security-related issues	A process shall be employed for informing product users about reportable security-related issues (see 10.5) in supported products in a timely manner with content that includes but is not limited to the following information: A) Issue description, vulnerability score as per CVSS or a similar system for ranking vulnerabilities, and affected product version(s); and, B) description of the resolution. NOTE 1 The description of the resolution can include references to installation of patches (see Clause 12). NOTE 2 Timeliness is driven by market forces. The strategy for handling third-party component vulnerabilities discovered by the product developer should take into account the possibility of premature public disclosure by the third party component supplier.	Dispel discloses reportable security-related issues to clients when required and in a manner consistent with those requirements. Dispel investigates all reported security concerns, and determines in its judgement whether notifications are necessary. Such determinations include the risk to production environments and issue resolution timing.	Yes
DM-6	**Periodic review of security defect management practice**	A process shall be employed for conducting periodic reviews of the security-related issue management process. Periodic reviews of the process shall, at a minimum, examine security-related issues managed through the process since the last periodic review to determine if the management process was complete, efficient, and led to the resolution of each security-related issue. Periodic reviews of the security-related issue management process shall be conducted at least annually.	Dispel conducts periodic reviews of security-related issue management processes. This review process is laid out in the A.14.1 Secure Development Policy, A.15 Supplier Security Policy	Yes

IEC 62443-4-1 Practice 7 – Security Update Management

Part	Title	Requirement	Dispel Product/Feature	
SUM-1	**Security update qualification**	A process shall be employed for verifying that 1) security updates created by the product developer address the intended security vulnerabilities; 2) security updates do not introduce regressions, including but not limited to patches created by: A) The product developer; B) Suppliers of components used in the product; and, C) Suppliers of components or platforms on which the product depends. The process should include a confirmation that update is not contradicting other operational, safety or legal constraints.	Dispel works on an agile development cycle. We try to push code to production as often as safely possible, so bugs get fixed quickly. We like to have second sets of eyes look at code. When code moves from a feature branch to staging to production, it is subject to a code review when the pull request is made to merge the branch into staging. Dispel manages bug fix updates via a ticketing system. When security updates go through the development cycle, they are subject to code review.	Yes

SUM-2	**Security update documentation**	A process shall be employed to ensure that documentation about product security updates is made available to product users that includes but is not limited to: A) The product version number(s) to which the security patch applies; B) Instructions on how to apply approved patches manually and via an automated process; C) Description of any impacts that applying the patch to the product can have, including reboot; D) Instructions on how to verify that an approved patch has been applied; and E) Risks of not applying the patch and mediations that can be used for patches that are not approved or deployed by the asset owner.	Dispel product patches are implemented by Dispel. For applications installed on endpoints, Dispel pushes auto-updates to those endpoints and prompts the user to allow their installation. Auto-updates identify product versions and determine which modifications are appropriate.	Yes
SUM-3	**Dependent component or operating system security update documentation**	A process shall be employed to ensure that documentation about dependent component or operating system security updates is made available to product users that includes but is not limited to: A) Stating whether the product is compatible with the dependent component or operating system security update; and B) For security updates that are unapproved by the product vendor, the mitigations that can be used in lieu of not applying the update.	Dispel applications check for operations system compatibility before installation. Some verification is performed by the OS manufacturer. For example, on iOS devices the Dispel application is distributed via Apple, who is responsible for checking Dispel-device compatibility. For installations that are not monitored by the manufacturer, Dispel provides component and operating system requirements in our documentation.	Yes

SUM-4	**Security update delivery**	A process shall be employed to ensure that security updates for all supported products and product versions are made available to product users in a manner that facilitates verification that the security patch is authentic.	Security patches pushed to users are signed by MD5 hash and code signatures. For apps distributed by Apple for iOS and macOS, Dispel updates are signed with keys shared with Apple to verify a patch is authentic. For Microsoft apps, Dispel uses Windows code signing.	Yes
SUM-5	**Timely delivery of security patches**	A process shall be employed to define a policy that specifies the timeframes for delivering and qualifying (see 11.2) security updates to product users and to ensure that this policy is followed. At a minimum, this policy shall consider the following factors: A) The potential impact of the vulnerability; B) Public knowledge of the vulnerability; C) Whether published exploits exist for the vulnerability; D) The volume of deployed products that are affected; and, E) The availability of an effective mitigation in lieu of the patch.	Dispel does not have a specific policy addressing the timeframes in which security updates must be rolled out. Identified vulnerabilities are treated on a case-by-case basis, and prioritized according to their severity, business needs, and the size of the impacted audience.	Yes

IEC 62443-4-1 Practice 8 – Security Guidelines

Part	Title	Requirement	Dispel Product/Feature	
SG-1	**Product defense in depth**	A process shall exist to create product user documentation that describes the security defense in depth strategy for the product to support installation, operation and maintenance that includes: A) Security capabilities implemented by the product and their role in the defense in depth strategy; B) Threats addressed by the defense in depth strategy; and C) Product user mitigation strategies for known security risks associated with the product, including risks associated with legacy code.	Dispel provides extensive documentation detailing defense in depth strategies. These are both publicly available on our website at https://dispel.io/security and in greater detail under NDA.	Yes
SG-2	**Defense in depth measures expected in the environment**	A process shall be employed to create product user documentation that describes the security defense in depth measures expected to be provided by the external environment in which the product is to be used (see Clause 6). NOTE These measures can also come from 10.5.	Dispel provides defense in depth diagrams in accordance with the Purdue Enterprise Reference Architecture of the client's system. This incorporates security layouts beyond Dispel's own environment, giving an opportunity to review the entire security context.	Yes

SG-3	**Security hardening guidelines**	A process shall be employed to create product user documentation that includes guidelines for hardening the product when installing and maintaining the product. The guidelines shall include, but are not limited to, instructions, rationale and recommendations for the following: A) integration of the product, including third-party components, with its product security context (see Clause 6); B) integration of the product's application programming interfaces/protocols with user applications; C) applying and maintaining the product's defense in depth strategy (see Clause 7); D) Configuration and use of security options/capabilities in support of local security policies, and for each security option/capability: 1) Its contribution to the product's defense in depth strategy (see Clause 7); 2) Descriptions of configurable and default values that include how each affects security along with any potential impact each has on work practices; and 3) Setting/changing/deleting its value; E) Instructions and recommendations for the use of all security-related tools and utilities that support administration, monitoring, incident handling and evaluation of the security of the product; F) Instructions and recommendations for periodic security maintenance activities; G) Instructions for reporting security incidents for the product to the product supplier; and H) Description of the security best practices for maintenance and administration of the product.	Dispel provides clients with advisory services covering product hardening. During procurement, Dispel works with clients to identify their security requirements. This helps dictate what Dispel features must be used, and their configuration. Features include additional defense in depth technologies, including isolation techniques.	Yes

SG-4	**Secure disposal guidelines**	A process shall be employed to create product user documentation that includes guidelines for removing the product from use. The guidelines shall include, but is not limited to, instructions and recommendations for the following: A) Removing the product from its intended environment (see Clause 6); B) Including recommendations for removing references and configuration data stored within the environment; C) Secure removal of data stored in the product; and, D) secure disposal of the product to prevent potential disclosure of data contained in the product that could not be removed as described in c) above.	Dispel provides documentation on our support portal for proper removal of Dispel applications from endpoints. The Dispel Operations Team assists when removing Dispel Wicket ESI virtual appliances from on-premise hardware.	Yes
SG-5	**Secure operation guidelines**	A process shall be employed to create product user documentation that describes: A) Responsibilities and actions necessary for users, including administrators, to securely operate the product; and, B) Assumptions regarding the behavior of the user/administrator and their relationship to the secure operation of the product.	Dispel provides documentation on our support portal covering the responsibilities and actions necessary for users to securely operate the product and provide guidance for proper behavior.	Yes

SG-6	**Account management guidelines**	A process shall be employed to create product user documentation that defines user account requirements and recommendations associated with the use of the product that includes, but is not limited to: A) User account permissions (access control) and privileges (user rights) needed to use the product, including, but not limited to operating system accounts, control system accounts and data base accounts; and B) Default accounts used by the product (for example, service accounts) and instructions for changing default account names and passwords.	Dispel provides documentation on our support portal covering how user account permissions, roles, and responsibilities should be configured. The console itself also provides guidance in real time to aid with user decisions. Documentation also covers instructions for changing account names and passwords. Dispel does not permit "default" accounts or passwords.	Yes
SG-7	**Documentation review**	A process shall be employed to identify, characterize and track to closure errors and omissions in all user manuals including the security guidelines to include: A) Coverage of the product's security capabilities; B) Integration of the product with its intended environment (see Clause 6); and, C) Assurance that all documented practices are secure.	Dispel's user manual system tracks changes and affords users to provide feedback on the quality of documentation. Internal comments may be made and tracked within the user manual system as well.	Yes

Mapping For IEC 62443-4-2: Technical Security Requirements For IACS Components

IEC 62443-4-2 serves to map the guidance found in IEC 62443-3-3 down to the components out of which control systems are formed.

IEC 62443-4-2 FR 1 – Identification and Authentication Control

Part	Title	Requirement	Dispel Product/Feature	
CR 1.1	**Human user identification and authentication**	Components shall provide the capability to identify and authenticate all human users according to IEC 62443-3-3 SR 1.1 on all interfaces capable of human user access. This capability shall enforce such identification and authentication on all interfaces that provide human user access to the component to support segregation of duties and least privilege in accordance with applicable security policies and procedures. This capability may be provided locally by the component or by integration into a system level identification and authentication system.	Each human user must log in using a minimum of a unique username and complex password to access any Dispel interface capable of human user access. Each human user is uniquely identified by their username and password. Identification and authentication are handled either entirely by Dispel or by, with, or through a customer-provided user management and authentication mechanism. For example, in the case of multifactor authentication, Dispel supports TOTP authentication tools (QR code style) such as Google Authenticator, Microsoft Authenticator, 1Password, Authy, etc. Dispel also supports FIDO U2F hardware tokens such as Yubikeys, and RSA SecurID tokens. Dispel integrates with Active Directory, LDAP, Okta, and native OS biometric authentication systems including Apple Touch ID and Windows Hello in apps.	Yes

CR 1.2	**Software process and device identification and authentication**	Components shall provide the capability to identify itself and authenticate to any other component (software application, embedded devices, host devices and network devices), according to IEC 62443-3-3 SR1.2. If the component, as in the case of an application, is running in the context of a human user, in addition, the identification and authentication of the human user according to IEC 62443-3-3 SR1.1 may be part of the component identification and authentication process towards the other components.	All Dispel components are able to identify and authenticate themselves with other components within and related to, a remote access deployment in accordance with IEC 62443-3-3 SR 1.2. This 'handshake' action takes place at the Wicket External Systems Integrator component when opening a portal down to equipment inside of the OT perimeter and at the Virtual Desktop component when establishing a connection to an end component.	Yes
CR 1.3	**Account management**	Components shall provide the capability to support the management of all accounts directly or integrated into a system that manages accounts according to IEC 62443-3-3 SR 1.3.	Dispel includes a user account management system; providing tools for adding, updating, removing, and permissioning users. Dispel also integrates with commonly used user management tools such as Microsoft Active Directory, LDAP, and Okta.	Yes

CR 1.4	**Identifier management**	Components shall provide the capability to integrate into a system that supports the management of identifiers and/or provide the capability to support the management of identifiers directly according to IEC 62443-3-3 SR 1.4.	Dispel supports identifier-based management for users and groups. The system allows restrictions on how a user is allowed to access control systems (via a VDI, or through a VPN application) and then what ports, IPs, and protocols they may use in that control environment. While it is strongly discouraged, Dispel does support access by general accounts (e.g., a "Control Room" master user account). However, a human user or machine account is supposed to be tied to a unique identifier.	Yes
CR 1.5	**Authenticator management**	Components shall provide the capability to: A) Support the use of initial authenticator content; B) Support the recognition of changes to default authenticators made at installation time; C) Function properly with periodic authenticator change/refresh operation; and D) Protect authenticators from unauthorized disclosure and modification when stored, used and transmitted.	Dispel supports authenticator's for proving identity. A user account has a salted and hashed password associated with their login. User accounts do not have default passwords. Passwords and tokens are always transmitted under strong encryption (e.g., AES-256 with 4096-bit keys). During login, the service generates and grants a user a session. User sessions automatically expire after a set period of time. Refresh and change operations trigger a customer-defined action on the relevant component.	Yes

CR 1.5 RE 1	Hardware security for authenticators	The authenticators on which the component rely shall be protected via hardware mechanisms.	For deployments requiring Hardware Security Modules (HSMs), key management is performed through a single-tenanted FIPS 140-2 Level 3 validated HSM or client-supplied FIPS 140-2 Level 4 validated HSM. While this option exists, we wish to stress that it is not typically used due to the costs associated with it.	Yes
CR 1.6	**Wireless access management**	The wireless access management requirements are network-component-specific and can be located as requirements for network-components in Clause 15.	Please see NDR 1.6. This requirement is met.	Yes
NDR 1.6	**Wireless access management**	A network device supporting wireless access management shall provide the capability to identify and authenticate all users (humans, software processes or devices) engaged in wireless communication.	Dispel provides remote access to control systems via a Wicket ESI – a virtual or hardware appliance. In either case, the backhaul from the Wicket ESI is a known quantity, which means all connections to the control system are uniform in their use of a particular backhaul. All traffic attempting to reach the Control System must undergo the same rigorous authorization requirements, and may be monitored, as well as recorded, per the Dispel customer's specifications.	Yes

NDR 1.6 RE 1	Unique identification and authentication	The network device shall provide the capability to uniquely identify and authenticate all users (humans, software processes or devices) engaged in wireless communication.	Dispel provides remote access to control systems via a Wicket ESI – a virtual or hardware appliance. In either case, the backhaul from the Wicket ESI is a known quantity, which means all connections to the control system are uniform in their use of a particular backhaul. All users attempting to reach the Control System are uniquely identified.	Yes
CR 1.7	**Strength of password-based authentication**	For components that utilize password-based authentication, those components shall provide or integrate into a system that provides the capability to enforce configurable password strength according to internationally recognized and proven password guidelines.	Dispel passwords enforce password strength based on a minimum length, and combination of uppercase characters, special characters, and numbers.	Yes
CR 1.7 RE 1	Password generation and lifetime restrictions for human users	Components shall provide, or integrate into a system that provides, the capability to protect against any given human user account from reusing a password for a configurable number of generations. In addition, the component shall provide the capability to enforce password minimum and maximum lifetime restrictions for human users. These capabilities shall conform to commonly accepted security industry practices. The component should provide the capability to prompt the user to change their password upon a configurable time prior to expiration.	Dispel components do not themselves prevent the re-use of old passwords, or enforce lifetime restrictions for passwords. For customers needing such restrictions, Dispel integrates with their LDAP, Active Directory, or other identity management system.	Yes

CR 1.7 RE 2	Password lifetime restrictions for all users (human, software process, or device)	Components shall provide, or integrate into a system that provides, the capability to enforce password minimum and maximum lifetime restrictions for all users.	Dispel components do not themselves prevent the re-use of old passwords, or enforce lifetime restrictions for passwords. For customers needing such restrictions, Dispel integrates with their LDAP, Active Directory, or other identity management system.	Yes
CR 1.8	**Public key infrastructure certificates**	When public key infrastructure (PKI) is utilized, the component shall provide or integrate into a system that provides the capability to interact and operate in accordance with IEC 62443-3-3 SR1.8.	Dispel uses industry-standard PKI methods for key management including VPN sessions and TLS certificates.	Yes

CR 1.9	**Strength of public key-based authentication**	For components that utilize public-key-based authentication, those components shall provide directly or integrate into a system that provides the capability within the same IACS environment to: A) Validate certificates by checking the validity of the signature of a given certificate; B) Validate the certificate chain or, in the case of self-signed certificates, by deploying leaf certificates to all hosts that communicate with the subject to which the certificate is issued; C) Validate certificates by checking a given certificate's revocation status; D) Establish user (human, software process or device) control of the corresponding private key; E) Map the authenticated identity to a user (human, software process or device); and, F) Ensure that the algorithms and keys used for the public key authentication conform to 8.5.	Dispel PKI is used to identify Dispel's identity to users in circumstances such as TLS. Users are not authenticated using PKI. In this context, Dispel complies with the steps listed here.	Yes
CR 1.9 RE 1	Hardware security for public key-based authentication	Components shall provide the capability to protect critical, long-lived private keys via hardware mechanisms.	Dispel uses PKI for TLS, not user authentication. In the TLS context, hardware mechanisms are used to protect private keys.	Yes

CR 1.10	**Authenticator feedback**	When a component provides an authentication capability, the component shall provide the capability to obscure feedback of authenticator information during the authentication process.	Dispel provides general feedback to users to obscure what information may be accurate during authentication. For example, if an invalid username or password is used during authentication the system replies that an invalid username/password was used. Or, when a password reset is made the system replies "If that account exists, it will receive an email shortly."	Yes
CR 1.11	**Unsuccessful login attempts**	When a component provides an authentication capability, the component shall provide the capability to: A) Enforce a limit of a configurable number of consecutive invalid access attempts by any user (human, software process or device) during a configurable time period; and B) Deny access for a specified period of time or until unlocked by an administrator when this limit has been reached. An administrator may unlock an account prior to the expiration of the timeout period.	Dispel locks a user account after a set number of failed consecutive logins. Locked out accounts must be manually re-enabled. Idling is prevented through the use of virtual desktops with Administrator defined maximum lifespans.	Yes

CR 1.12	**System use notification**	When a component provides local human user access/HMI, it shall provide the capability to display a system use notification message before authenticating. The system use notification message shall be configurable by authorized personnel.	For customers seeking to meet this requirement (along with many others within the IEC 62443 framework, for that matter), Dispel requires the use of a virtual desktop - on which a system use notification may be placed. In addition, a system use notification can be presented to the User as part of form-based access request procedures (where implemented).	Yes
CR 1.13	**Access via untrusted networks**	The access via untrusted networks requirements are component-specific and can be located as requirements for each specific component type in Clauses 12 through 15.	Please see NDR 1.13. This requirement is met.	Yes
NDR 1.13	**Access via untrusted networks**	The network device supporting device access into a network shall provide the capability to monitor and control all methods of access to the network device via untrusted networks.	All methods of access to a Dispel network are monitored and controlled per a least-trust model.	Yes
NDR 1.13 RE 1	Explicit access request approval	The network device shall provide the capability to deny access requests via untrusted networks unless explicitly approved by an assigned role.	All access to a Dispel network via untrusted networks must be approved, either on a case-by-case basis, or on a user-by-user basis, by an assigned role.	Yes

CR 1.14	**Strength of symmetric key-based authentication**	For components that utilize symmetric keys, the component shall provide the capability to: A) Establish the mutual trust using the symmetric key; B) Store securely the shared secret (the authentication is valid as long as the shared secret remains secret); C) Restrict access to the shared secret; and, D) Ensure that the algorithms and keys used for the symmetric key authentication conform to 8.5.	All components within a Dispel network that rely upon a symmetric key use keys and associated algorithms that meet or exceed CNSA Suite guidelines (e.g., AES-256 with 4096-bit keys for the initial key exchange). The secret is stored securely, and access to the shared secret is restricted.	Yes
CR 1.14 RE 1	Hardware security for symmetric key-based authentication	Components shall provide the capability to protect critical, long lived symmetric keys via hardware mechanisms.	For deployments requiring Hardware Security Modules (HSMs), key management is performed through a single-tenanted FIPS 140-2 Level 3 validated HSM or client-supplied FIPS 140-2 Level 4 validated HSM. While this option exists, we wish to stress that it is not typically used due to the costs associated with it.	Yes

IEC 62443-4-2 FR 2 – Use Control

Part	Title	Requirement	Dispel Product/Feature	
CR 2.1	**Authorization enforcement**	Components shall provide an authorization enforcement mechanism for all identified and authenticated users based on their assigned responsibilities.	Dispel provides device, protocol, process, and session-level access control which, by definition, leads to an identical degree of authorization mapping. This capability is enforced at multiple levels within the Dispel product. For human users, single-use virtual desktops ensure session-level segmentation and excel at protocol and process segmentation against determined adversaries. The network infrastructure spanning the distance from the user to the Wicket ESI located at the Control System can be set to self-destruct after each session is concluded, providing a safeguard that task segregation is achieved temporally. At the Wicket ESI, user-session-specific whitelisting of underlying equipment serves as a failsafe for human users connecting through a virtual desktop interface.	Yes

CR 2.1 RE 1	Authorization enforcement for all users (humans, software processes and devices)	Components shall provide an authorization enforcement mechanism for all users based on their assigned responsibilities and least privilege.	Dispel provides device, protocol, process, and session-level access control which, by definition, leads to an identical degree of authorization mapping. This capability is enforced at multiple levels within the Dispel product. For human users, single-use virtual desktops ensure session-level segmentation and excel at protocol and process segmentation against determined adversaries. For machine users, this responsibility necessarily falls instead to the network infrastructure and Wicket ESI, which both hold roles as bastion components. The network infrastructure spanning the distance from the user to the Wicket ESI located at the Control System can be set to self-destruct after each session is concluded, providing a safeguard that task segregation is achieved temporally. At the Wicket ESI, user-session-specific whitelisting of underlying equipment serves as a failsafe for human users connecting through a virtual desktop interface, and as the primary mechanism for providing such protection in the case of machine users.	Yes

CR 2.1 RE 2	Permission mapping to roles	Components shall, directly or through a compensating security mechanism, provide for an authorized role to define and modify the mapping of permissions to roles for all human users. Roles should not be limited to fixed nested hierarchies in which a higher-level role is a super set of a lesser privileged role. For example, a system administrator should not necessarily encompass operator privileges.	Dispel addresses this objective with two converging procedures. First, authorized users are allowed to define or modify the mapping of permissions to a human user through the management console. Second, if the customer so chooses, Dispel's remote access system can be set to require a form be completed by the person requesting access or a change to their access permissions. In this second situation, two humans – the user and administrator – are able to define precisely what it is that a person is going to be given access too. This technique serves to reduce the risk of an administrator assigned a permission set that is broader than needed by the user. Roles are not set to proscribed nested hierarchies.	Yes

CR 2.1 RE 3	Supervisor override	Components shall support a supervisor manual override for a configurable time or sequence of events.	First, authorized users are allowed to define or modify the mapping of permissions to a human user through the management console at any time. Virtual desktops are set with time-to-live conditions, allowing an administrator to cleanly configure the time during which an authorization set are held open. Wicket ESIs control equipment whitelisting and can be reconfigured at any time as well. The stated requirement of SR 2.1 RE 3, however, is clarified in the "Note" section to be in reference to emergency situations; the goal being to allow a supervisor to expand a permission set without forcing the operator to log out and log in again to obtain access to the broadened capabilities. In practice, not all permissions can be overridden without a new session being created – the reason being that different equipment sets require different applications to run them, and Dispel virtual desktops are not launched with applications irrelevant to the equipment to which a user is granted access. For this reason, we have assigned this section a Partial Coverage rating.	Yes

CR 2.1 RE 4	Dual approval	Components shall support dual approval when action can result in serious impact on the industrial process. Dual approval should be limited to actions which require a very high level of confidence that they will be performed reliably and correctly. Requiring dual approval provides emphasis to the seriousness of consequences that would result from failure of a correct action. An example of a situation in which dual approval is required would be a change to a set point of a critical industrial process. Dual approval mechanisms should not be employed when an immediate response is necessary to safeguard HSE consequences, for example, emergency shutdown of an industrial process.	An administrator can specify that dual approval is required to access a specific part of the control system.	Yes
CR 2.2	**Wireless use control**	If a component supports usage through wireless interfaces it shall provide the capability to integrate into the system that supports usage authorization, monitoring and restrictions according to commonly accepted industry practices.	Dispel does support usage through a wireless connection down to an on-premise component called a Wicket External Systems Integrator (a Wicket ESI). The Wicket ESI can be integrated into a system that supports usage authorization, monitoring and restrictions according to commonly accepted industry practices.	Yes
CR 2.3	**Use control for portable and mobile devices**	There is no component level requirement associated with IEC 62443-3-3 SR 2.3.		Yes

CR 2.4	**Mobile code**	The use control requirements for mobile code are component-specific and can be located as requirements for each specific component type in Clauses 12 through 15.	For those reading this document without a copy of IEC 62443 in front of them, "mobile code" is defined to include such things as Java, JavaScript, ActiveX, and Portable Document Format (PDF), to name a few. To meet this section, as well as IEC 62443-3-3 SR 2.4 and SR 2.4 RE 1, Dispel typically does not permit the upload of files to the single-use virtual desktop that forms a part of the remote access system. However, there are times when customers want to push mobile code up to virtual desktops. In these situations, certificate checks can be required, and virus scans can be performed. All activities, including those involving mobile code, are monitored in Dispel deployments when the appropriate logging and recording packages are included by the customer. Please see HDR 2.4 and NDR 2.4 for relevant discussion of this topic. EDR 2.4 is not applicable to Dispel systems.	Yes

SAR 2.4	**Mobile code**	In the event that a software application utilizes mobile code technologies, that application shall provide the capability to enforce a security policy for the usage of mobile code technologies. The security policy shall allow, at a minimum, the following actions for each mobile code technology used on the software application: A) Control execution of mobile code; B) Control which users (human, software process, or device) are allowed to transfer mobile code to/from the application; C) Control the execution of mobile code based on the results of an integrity check prior to the code being executed.	Not applicable.	Not Applicable
SAR 2.4 RE 1	Mobile code authenticity check	The application shall provide the capability to enforce a security policy that allows the device to control execution of mobile code based on the results of an authenticity check prior to the code being executed.	Not applicable.	Not Applicable

EDR 2.4	**Mobile code**	In the event that an embedded device utilizes mobile code technologies, the embedded device shall provide the capability to enforce a security policy for the usage of mobile code technologies. The security policy shall allow, at a minimum, the following actions for each mobile code technology used on the embedded device: A) Control execution of mobile code; B) Control which users (human, software process, or device) are allowed to upload mobile code to the device; C) Control the execution of mobile code based on the results of an integrity check prior to the code being executed.	Not applicable.	Not Applicable
EDR 2.4 RE 1	Mobile code authenticity check	The embedded device shall provide the capability to enforce a security policy that allows the device to control execution of mobile code based on the results of an authenticity check prior to the code being executed.	Not applicable.	Not Applicable

HDR 2.4	**Mobile code**	In the event that a host device utilizes mobile code technologies, that host device shall provide the capability to enforce a security policy for the usage of mobile code technologies. The security policy shall allow, at a minimum, the following actions for each mobile code technology used on the host device: A) Control execution of mobile code; B) Control which users (human, software process, or device) are allowed to upload mobile code to the host device; and, C) Control the code execution based upon integrity checks on the mobile code and prior to the code being executed.	Dispel's virtual desktop components can, at times, be considered Host Devices under the IEC 62443 framework. All Dispel virtual desktops permit the enforcement of security policies which control the execution of mobile code, define whether a user can upload code to the host device as well as from where that mobile code may be uploaded, and perform integrity checks upon the uploaded code prior to it being executed.	Yes
HDR 2.4 RE 1	Mobile code authenticity check	The host device shall provide the capability to enforce a security policy that allows the device to control execution of mobile code based on the results of an authenticity check prior to the code being executed.	Dispel's virtual desktop components can, at times, be considered Host Devices under the IEC 62443 framework. All Dispel virtual desktops permit the enforcement of a security policy whereby mobile code can only be run after a positive authenticity result comes back on the mobile code.	Yes

NDR 2.4	**Mobile code**	In the event that a network device utilizes mobile code technologies, the network device shall provide the capability to enforce a security policy for the usage of mobile code technologies. The security policy shall allow, at a minimum, the following actions for each mobile code technology used on the network device: A) Control execution of mobile code; B) Control which users (human, software process, or device) are allowed to transfer mobile code to/from the network device; and, C) Control the code execution based upon integrity checks on mobile code and prior to the code being executed.	The only component of a Dispel system that can utilize mobile code technology if permitted by the customer is a Dispel virtual desktop. These components provide the customer with the ability to control the execution of mobile code; control what users, processes, or devices can transfer mobile code to/from the component; and control code execution based upon integrity checks prior to the code's execution.	Yes
NDR 2.4 RE 1	Mobile code authenticity check	The network device shall provide the capability to enforce a security policy that allows the device to control execution of mobile code based on the results of an authenticity check prior to the code being executed.	The only component of a Dispel system that can utilize mobile code technology if permitted by the customer is a Dispel virtual desktop. These components provide the customer with the ability to control the execution of mobile code; control what users, processes, or devices can transfer mobile code to/from the component; and control code execution based upon integrity checks prior to the code's execution.	Yes

CR 2.5	**Session lock**	If a component provides a human user interface, whether accessed locally or via a network, the component shall provide the capability: A) to protect against further access by initiating a session lock after a configurable time period of inactivity or by manual initiation by the user (human, software process or device); and, B) for the session lock to remain in effect until the human user who owns the session, or another authorized human user, re-establishes access using appropriate identification and authentication procedures.	Dispel accomplishes this task by assigning time-to-live restrictions on its virtual desktops. Virtual desktops may also be manually destroyed prior to their pre-specified time to live by an administrator at any time. For a human user to restore access to the system, they must re-present appropriate credentials to the Dispel system.	Yes
CR 2.6	**Remote session termination**	If a component supports remote sessions, the component shall provide the capability to terminate a remote session either automatically after a configurable time period of inactivity, manually by a local authority, or manually by the user (human, software process or device) who initiated the session.	Dispel accomplishes this task by assigning time-to-live restrictions on its virtual desktops. Virtual desktops may also be manually destroyed prior to their pre-specified time to live by an administrator at any time.	Yes
CR 2.7	**Concurrent session control**	Components shall provide the capability to limit the number of concurrent sessions per interface for any given user (human, software process or device).	Dispel provides for configurable limits on the number and type of concurrent sessions per interface for any given user.	Yes

CR 2.8	**Auditable events**	Components shall provide the capability to generate audit records relevant to security for the following categories: A) Access control; B) Request errors; C) Control system events; D) Backup and restore event; E) Configuration changes; and F) Audit log events. Individual audit records shall include: A) Timestamp; B) Source (originating device, software process or human user account); C) Category; D) Type; E) Event ID; and F) Event result.	Dispel provides the listed audit entry categories.	Yes
CR 2.9	**Audit storage capacity**	Components shall: A) Provide the capability to allocate audit record storage capacity according to commonly recognized recommendations for log management; and, B) Provide mechanisms to protect against a failure of the component when it reaches or exceeds the audit storage capacity.	Audit storage is performed on a dedicated log server tied to storage arrays set to client-specified redundancy and retention levels. Please note the storage space allocation is typically set to exceed the theoretical maximum data the relevant components could produce over a defined audit retention period.	Yes

CR 2.9 RE 1	Warn when audit record storage capacity threshold reached	Components shall provide the capability to issue a warning when the allocated audit record storage reaches a configurable threshold.	Dispel provides a warning when allocated audit record storage space reaches a configurable threshold. Please note the storage space allocation is typically set to exceed the theoretical maximum data the relevant components could produce over a defined audit retention period.	Yes
CR 2.10	**Response to audit processing failures**	Components shall: A) Provide the capability to protect against the loss of essential services and functions in the event of an audit processing failure; and B) Provide the capability to support appropriate actions in response to an audit processing failure according to commonly accepted industry practices and recommendations.	Dispel's logging and audit systems sit in a segmented area from those systems responsible for performing essential services and functions. An alert is provided when a log server experiences a failure.	Yes
CR 2.11	**Timestamps**	Components shall provide the capability to create timestamps (including date and time) for use in audit records.	All components provide timestamps as part of their log feeds.	Yes
CR 2.11 RE 1	Time synchronization	Components shall provide the capability to create timestamps that are synchronized with a system wide time source.	All components are synchronized to Coordinated Universal Time over NTP. Most are either Stratum 3 or Stratum 4.	Yes
CR 2.11 RE 2	Protection of time source integrity	The time synchronization mechanism shall provide the capability to detect unauthorized alteration and cause an audit event upon alteration.	Time source integrity is structurally embedded through a cross referencing mechanism that relies upon multiple Stratum 0 devices. This error-checking system does not distinguish between unauthorized and signal degradation-induced changes.	Yes

CR 2.12	**Non-repudiation**	If a component provides a human user interface, the component shall provide the capability to determine whether a given human user took a particular action. Control elements that are not able to support such capability shall be listed in component documents.	Dispel can provide session recordings of all activities performed by a user through a virtual desktop. Session recording is rendered as an optional service.	Yes
CR 2.12 RE 1	Non-repudiation for all users	Components shall provide the capability to determine whether a given user (human, software process or device) took a particular action.	Logging at each component within a Dispel remote access deployment provides time-stamped associations between each individual action and the user associated with that action. As a further point of assurance against parallel transmissions, any connection that passes through a Dispel remote access channel runs through at least one single-tenanted conduit that can be traced back to one, and only one, specific user (human, software process, or device).	Yes
EDR 2.13	**Use of physical diagnostic and test interfaces**	Embedded devices shall protect against unauthorized use of the physical factory diagnostic and test interface(s) (e.g. JTAG debugging).	Not Applicable.	Not Applicable
EDR 2.13 RE 1	Active monitoring	Embedded devices shall provide active monitoring of the device's diagnostic and test interface(s) and generate an audit log entry when attempts to access these interface(s) are detected.	Not Applicable.	Not Applicable

HDR 2.13	**Use of physical diagnostic and test interfaces**	Host devices shall protect against unauthorized use of the physical factory diagnostic and test interface(s) (e.g. JTAG debugging).	Dispel's virtual desktop components can, at times, be considered Host Devices under the IEC 62443 framework. Dispel virtual desktops, when allocated to a User, restrict that User to an Administrator-defined scope of actions.	Yes
HDR 2.13 RE 1	Active monitoring	Host devices shall provide active monitoring of the device's diagnostic and test interface(s) and generate an audit log entry when attempts to access these interface(s) are detected.	Dispel's virtual desktop components can, at times, be considered Host Devices under the IEC 62443 framework. Dispel virtual desktops speak syslog and can supply a feed for when attempts are made to access diagnostic and test interfaces. Further, Dispel virtual desktops provide screen recording and live streaming.	Yes
NDR 2.13	**Use of physical diagnostic and test interfaces**	Network devices shall protect against unauthorized use of the physical factory diagnostic and test interface(s) (e.g. JTAG debugging).	All Dispel systems prevent use of physical factory diagnostic and test interfaces on the Dispel platform without authorization.	Yes
NDR 2.13 RE 1	Active monitoring	Network devices shall provide active monitoring of the device's diagnostic and test interface(s) and generate an audit log entry when attempts to access these interface(s) are detected.	All Dispel systems provide active monitoring of, amongst other things, the diagnostic and test interfaces, generating log entries when attempts to access these interfaces are detected.	Yes

IEC 62443-4-2 FR 3 – System integrity

Part	Title	Requirement	Dispel Product/Feature	
CR 3.1	**Communication integrity**	Components shall provide the capability to protect integrity of transmitted information.	Data sent over Dispel's remote access system traverses a colorless core, moving target defense software defined wide area network built over any of 7 major commercial public cloud provider or, depending upon the customer, private or government clouds. Except if specified by the customer, Dispel encrypts all transmission within the network such that they exceed CNSA Suite guidelines – specifically, by using AES-256 with independent 4096-bit keys used for the initial key exchange. SR 3.1 goes further in the supplemental guidance section, however, in calling for hardening of hardware components to meet relevant environmental risks to signal integrity. Dispel provides ruggedized form-factor Wicket ESIs to the specifications of the customer. While case-by-case, typical ruggedized Wicket ESI form factors are tested to align with IEC 60068-2-64 and IEC 60068-2-27.	Yes
CR 3.1 RE 1	Communication authentication	Components shall provide the capability to verify the authenticity of received information during communication.	Data traversing a Dispel moving target defense software defined wide area network is sent between whitelisted components tunneled together using AES-256 wrappers established with independent 4096-bit keys that cycle every few minutes. Authenticity is therefore verified both through encryption (is the decrypted packet parse-able?) and origin.	Yes

CR 3.2	**Protection from malicious code**	The protection from malicious code requirements are component-specific and can be located as requirements for each specific component type in Clauses 12 through 15.	Please see EDR 3.2, HDR 3.2, and NDR 3.2. This section is met where applicable.	Yes
SAR 3.2	**Protection from malicious code**	The application product supplier shall qualify and document which protection from malicious code mechanisms are compatible with the application and note any special configuration requirements.	Not Applicable.	Not Applicable
EDR 3.2	**Protection from malicious code**	The embedded device shall provide the capability to protect from installation and execution of unauthorized software.	Not Applicable.	Not Applicable
HDR 3.2	**Protection from malicious code**	There shall be mechanisms on host devices that are qualified by the IACS product supplier to provide protection from malicious code. The IACS product supplier shall document any special configuration requirements related to protection from malicious code.	Dispel's virtual desktop components can, at times, be considered Host Devices under the IEC 62443 framework. Dispel virtual desktops, in such situations, are deployed with antivirus software.	Yes

HDR 3.2 RE 1	Report version of code protection	The host device shall automatically report the software and file versions of protection from malicious code in use (as part of overall logging function).	Dispel's virtual desktop components can, at times, be considered Host Devices under the IEC 62443 framework. Dispel virtual desktops are launched from golden images which query for the latest available versions of antivirus software to be loaded onto the virtual desktop. Log reports from the virtual desktop and launch engine correlate to yield the name(s) and file version(s) of antivirus software running on the virtual desktop.	Yes
NDR 3.2	**Protection from malicious code**	The network device shall provide for protection from malicious code.	All Dispel components work towards meeting the spirit as well as letter of NDR 3.2 at multiple levels, including antivirus, authenticity checks, and process whitelisting.	Yes
CR 3.3	**Security functionality verification**	Components shall provide the capability to support verification of the intended operation of security functions according to IEC 62443-3-3 SR3.3.	When testing of the nature described in IEC 62443-3-3 SR 3.3 and its supplemental guidance section arise, Dispel not only provides the customer with the ability to have testers assess the live system, but also provides the customer with a replica environment the testers can run initial verifications against without potentially destabilizing operations. Tests may be scripted/automated or manual in nature and may be run during normal or offline operations.	Yes

CR 3.3 RE 1	Security functionality verification during normal operation	Components shall provide the capability to support verification of the intended operation of security functions during normal operations. This RE needs to be carefully implemented to avoid detrimental effects. It may not be suitable for safety systems.	When testing of the nature described in IEC 62443-3-3 SR 3.3 and its supplemental guidance section arise, Dispel not only provides the customer with the ability to have testers assess the live system, but also provides the customer with a replica environment the testers can run initial verifications against without potentially destabilizing operations. Tests may be scripted/automated or manual in nature and may be run during normal or offline operations.	Yes
CR 3.4	**Software and information integrity**	Components shall provide the capability to perform or support integrity checks on software, configuration and other information as well as the recording and reporting of the results of these checks or be integrated into a system that can perform or support integrity checks.	Every component within a Dispel system supplies syslog data that can be directed to a configurable logging and monitoring server. Further, virtual desktop components contain antivirus software to perform integrity checks, the results of which can then be passed to supporting recording and reporting systems.	Yes
CR 3.4 RE 1	Authenticity of software and information	Components shall provide the capability to perform or support authenticity checks on software, configuration and other information as well as the recording and reporting of the results of these checks or be integrated into a system that can perform or support authenticity checks.	Every component within a Dispel system supplies syslog data that can be directed to a configurable logging and monitoring server. Included within this data stream are alarms related to change point detection. This system can be supported by being connected to a logging and monitoring server supplied with contextual data that would enhance the likelihood of detecting malicious software, configuration attempts, or other activities.	Yes

CR 3.4 RE 2	Automated notification of integrity violations	If the component is performing the integrity check, it shall be capable of automatically providing notification to a configurable entity upon discovery of an attempt to make an unauthorized change.	Every component within a Dispel system supplies syslog data that can be directed to a configurable logging and monitoring server. Included within this data stream are alarms related to change point detection.	Yes
CR 3.5	**Input validation**	Components shall validate the syntax, length and content of any input data that is used as an industrial process control input or input via external interfaces that directly impacts the action of the component.	Dispel can provide syntactical, length, and content analysis of inputs through its virtual desktop component.	Yes
CR 3.6	**Deterministic output**	Components that physically or logically connect to an automation process shall provide the capability to set outputs to a predetermined state if normal operation as defined by the component supplier cannot be maintained.	Dispel's Wicket ESI can be set to a predetermined state of either Fail-to-Closed or Fail-to-Open if the Wicket or connected systems cease to function properly.	Yes
CR 3.7	**Error handling**	Components shall identify and handle error conditions in a manner that does not provide information that could be exploited by adversaries to attack the IACS.	Dispel supplies verbose error messages when systems have experienced failures that, if reviewed by a Dispel employee or trained third party with appropriate access credentials, can permit troubleshooting to take place efficiently. These error messages do not reveal information that would aid an attacker in damaging the Dispel system further.	Yes

CR 3.8	**Session integrity**	Components shall provide mechanisms to protect the integrity of communications sessions including: A) The capability to invalidate session identifiers upon user logout or other session termination (including browser sessions); B) The capability to generate a unique session identifier for each session and recognize only session identifiers that are system-generated; and C) The capability to generate unique session identifiers with commonly accepted sources of randomness.	Users are only able to reach a virtual desktop supplied by Dispel using Microsoft Remote Desktop Protocol which, in turn, relies upon a uniquely generated session ID to maintain the connection. When a session is terminated, the associated virtual desktop is destroyed. This achieves the same outcome as invalidating the session ID, as there is nothing to which the session ID can associate any longer. While the Microsoft Remote Desktop Protocol application is commonly used, there is no reason to believe that session IDs generated by the application are created with an acceptable degree of randomness. To overcome this, Dispel relies upon a combination of IP Whitelisting at the virtual desktop level, and the randomly generated locations of these virtual desktops, to prevent the hijacking for which IEC 62443-3-3 SR 3.8 RE 3 was written, which maps to CR 3.8(c).	Yes
CR 3.9	**Protection of audit information**	Components shall protect audit information, audit logs, and audit tools (if present) from unauthorized access, modification and deletion.	Where Dispel is in control of the storage of audit information rather than the customer, Dispel has audit records stored on WORM data tapes stored in secured, geographically dispersed facilities supplied and maintained by Partners (for example, Amazon Web Services' S3 Glacier Deep Archive).	Yes

CR 3.9 RE 1	Audit records on write-once media	Components shall provide the capability to store audit records on hardware-enforced write-once media.	Where Dispel is in control of the storage of audit information rather than the customer, Dispel has audit records stored on WORM data tapes.	Yes
CR 3.10	**Support for updates**	The support for updates requirements are component-specific and can be located as requirements for each specific device type in Clauses 12 through 15.	Please see EDR 3.10, HDR 3.10, and NDR 3.10. This section is met where applicable.	Yes
EDR 3.10	**Support for updates**	The embedded device shall support the ability to be updated and upgraded.	Not Applicable.	Not Applicable
EDR 3.10 RE 1	Update authenticity and integrity	The embedded device shall validate the authenticity and integrity of any software update or upgrade prior to installation.	Not Applicable.	Not Applicable
HDR 3.10	**Support for updates**	Host devices shall support the ability to be updated and upgraded.	Dispel's virtual desktop components can, at times, be considered Host Devices under the IEC 62443 framework. Dispel virtual desktops are single use, being updated and upgraded through self-destruction and replacement.	Yes
HDR 3.10 RE 1	Update authenticity and integrity	Host devices shall validate the authenticity and integrity of any software update or upgrade prior to installation.	Dispel's virtual desktop components can, at times, be considered Host Devices under the IEC 62443 framework. Dispel virtual desktops are built from golden images which query for the latest versions of all software components. The authenticity of each software component is checked as part of the build process.	Yes

NDR 3.10	**Support for updates**	Network devices shall support the ability to be updated and upgraded.	In meeting NDR 3.10 in the spirit as well as letter, one must recognize that each component of a Dispel system is launched on a virtual machine and that these virtual machines are not updated or upgraded once launched. Rather, "updates" and "upgrades" are performed by destroying and replacing the relevant virtual machines whenever an update or upgrade is required. This condenses the attack surface further than the authors of NDR 3.10 had envisioned as possible for network components. The system as a whole, then, supports the ability of updates and upgrades but, at its most granular level, deliberately does not permit updates or upgrades.	Yes
NDR 3.10 RE 1	Update authenticity and integrity	Network devices shall validate the authenticity and integrity of any software update or upgrade prior to installation.	In meeting NDR 3.10 in the spirit as well as letter, one must recognize that each component of a Dispel system is launched on a virtual machine and that these virtual machines cannot be updated or upgraded once launched. Rather, "updates" and "upgrades" are performed by destroying and replacing the relevant virtual machines. Integrity and verification checks for such updates and upgrades are performed at launch.	Yes
CR 3.11	**Physical tamper resistance and detection**	The physical tamper resistance and detection requirements are component-specific and can be located as requirements for each specific device type in Clauses 12 through 15.	Please see EDR 3.11, HDR 3.11, and NDR 3.11. This section is met where applicable.	Yes

EDR 3.11	**Physical tamper resistance and detection**	The embedded device shall provide tamper resistance and detection mechanisms to protect against unauthorized physical access into the device.	Not Applicable.	Not Applicable
EDR 3.11 RE 1	Notification of a tampering attempt	The embedded device shall be capable of automatically providing notification to a configurable set of recipients upon discovery of an attempt to make an unauthorized physical access. All notifications of tampering shall be logged as part of the overall audit logging function.	Not Applicable.	Not Applicable
HDR 3.11	**Physical tamper resistance and detection**	Host devices shall provide the capability to support tamper resistance and detection mechanisms to protect against unauthorized physical access into the device.	Dispel's virtual desktop components can, at times, be considered Host Devices under the IEC 62443 framework. These virtual desktops are positioned, except where specified by the customer, on public clouds. The specifics of each public cloud provider's physical security processes are beyond the scope of this report. However, all public cloud providers in the Dispel inventory supply physical security reports that may be supplied upon request.	Yes

HDR 3.11 RE 1	Notification of a tampering attempt	Host devices shall be capable of automatically providing notification to a configurable set of recipients upon discovery of an attempt to make an unauthorized physical access. All notifications of tampering shall be logged as part of the overall audit logging function.	Dispel's virtual desktop components can, at times, be considered Host Devices under the IEC 62443 framework. These virtual desktops are positioned, except where specified by the customer, on public clouds. Most public cloud providers provide reports to Dispel when unauthorized physical access is discovered or attempted. When HDR 3.11 RE 1 compliance is required, Dispel restricts cloud usage to those public clouds that provide tampering report feeds.	Yes
NDR 3.11	**Physical tamper resistance and detection**	Network devices shall provide tamper resistance and detection mechanisms to protect against unauthorized physical access into the device.	Dispel's systems are almost entirely positioned on virtual machines launched on public clouds. The specifics of each public cloud provider's physical security processes are beyond the scope of this report. However, all public cloud providers in the Dispel inventory supply physical security reports that may be supplied upon request or automatically directed to a monitoring platform via a feed. The one component that, often as not, is deployed on a hardware device on-premises is a Dispel Wicket External Systems Integrator (a Wicket ESI). The Wicket ESI, where conformance with NDR 3.11 is required, is launched on a tamper resistant, alarmed, hardware platform.	Yes

NDR 3.11 RE 1	Notification of a tampering attempt	Network devices shall be capable of automatically providing notification to a configurable set of recipients upon discovery of an attempt to make an unauthorized physical access. All notifications of tampering shall be logged as part of the overall audit logging function.	Dispel's systems are almost entirely positioned on virtual machines launched on public clouds. The specifics of each public cloud provider's physical security processes are beyond the scope of this report. However, all public cloud providers in the Dispel inventory supply physical security reports that may be supplied upon request or automatically directed to a monitoring platform via a feed. The one component that, often as not, is deployed on a hardware device on-premises is a Dispel Wicket External Systems Integrator (a Wicket ESI). The Wicket ESI, where conformance with NDR 3.11 is required, is launched on a tamper resistant, alarmed, hardware platform which can provide a feed of such tampering to a log server.	Yes
CR 3.12	**Provisioning product supplier roots of trust**	The provisioning product supplier roots of trust requirements are component-specific and can be located as requirements for each specific device type in Clauses 12 through 15.	Please see EDR 3.12, HDR 3.12, and NDR 3.12. This section is met where applicable.	Yes
HDR 3.12	**Provisioning product supplier roots of trust**	Host devices shall provide the capability to provision and protect the confidentiality, integrity, and authenticity of product supplier keys and data to be used as one or more "roots of trust" at the time of manufacture of the device.	Dispel's virtual desktop components can, at times, be considered Host Devices under the IEC 62443 framework. These virtual desktops are positioned, except where specified by the customer, on public clouds. These virtual desktops protect the confidentiality, integrity, and authenticity of private keys.	Yes

EDR 3.12	**Provisioning product supplier roots of trust**	Embedded devices shall provide the capability to provision and protect the confidentiality, integrity, and authenticity of product supplier keys and data to be used as one or more "roots of trust" at the time of manufacture of the device.	Not Applicable.	Not Applicable
NDR 3.12	**Provisioning product supplier roots of trust**	Network devices shall provide the capability to provision and protect the confidentiality, integrity, and authenticity of product supplier keys and data to be used as one or more "roots of trust" at the time of manufacture of the device.	In meeting NDR 3.13 in the spirit as well as letter of section 15.10.2, one must recognize that each component of a Dispel system is launched on a virtual machine and that many of these virtual machines cannot be reconfigured once launched. In short, NDR 3.13 is not applicable to all components. However, for those components that can be reconfigured, or to which additional software may be added, data defining trusted origins is supplied to the virtual machine as part of that component's instantiation.	Yes
CR 3.13	**Provisioning asset owner roots of trust**	The provisioning asset owner roots of trust requirements are component-specific and can be located as requirements for each specific device type in Clauses 12 through 15.	Please see EDR 3.13, HDR 3.13, and NDR 3.13. This section is met where applicable.	Yes

EDR 3.13	**Provisioning asset owner roots of trust**	Embedded devices shall: A) Provide the capability to provision and protect the confidentiality, integrity, and authenticity of asset owner keys and data to be used as "roots of trust"; and, B) Support the capability to provision without reliance on components that may be outside of the device's security zone.	Not Applicable.	Not Applicable
HDR 3.13	**Provisioning asset owner roots of trust**	Host devices shall: A) Provide the capability to provision and protect the confidentiality, integrity, and authenticity of asset owner keys and data to be used as "roots of trust"; and, B) Support the capability to provision without reliance on components that may be outside of the device's security zone.	Dispel's virtual desktop components can, at times, be considered Host Devices under the IEC 62443 framework. These virtual desktops can independently generate and protect private keys.	Yes

NDR 3.13	**Provisioning asset owner roots of trust**	Network devices shall: A) Provide the capability to provision and protect the confidentiality, integrity, and authenticity of asset owner keys and data to be used as "roots of trust"; and, B) Support the capability to provision without reliance on components that may be outside of the device's security zone.	In meeting NDR 3.13 in the spirit as well as letter of section 15.10.2, one must recognize that each component of a Dispel system is launched on a virtual machine and that many of these virtual machines cannot be reconfigured once launched. In short, NDR 3.13 is not applicable to all components. However, for those components that can be reconfigured, or to which additional software may be added, data defining trusted origins is supplied to the virtual machine as part of that component's instantiation.	Yes
CR 3.14	**Integrity of the boot process**	The integrity of the boot process requirements are component-specific and can be located as requirements for each specific device type in Clauses 12 through 15.	Please see EDR 3.14, HDR 3.14, and NDR 3.14. This section is met where applicable.	Yes
EDR 3.14	**Integrity of the boot process**	Embedded devices shall verify the integrity of the firmware, software, and configuration data needed for the component's boot and runtime processes prior to use.	Not Applicable.	Not Applicable
EDR 3.14 RE 1	Authenticity of the boot process	Embedded devices shall use the component's product supplier roots of trust to verify the authenticity of the firmware, software, and configuration data needed for the component's boot process prior to it being used in the boot process.	Not Applicable.	Not Applicable

HDR 3.14	**Integrity of the boot process**	Host devices shall verify the integrity of the firmware, software, and configuration data needed for the component's boot process prior to it being used in the boot process.	Dispel's virtual desktop components can, at times, be considered Host Devices under the IEC 62443 framework. These virtual desktops are launched from golden images – the integrity of which is verified as part of the boot process.	Yes
IEC 62443-4-2 HDR 3.14 RE 1	Authenticity of the boot process	Host devices shall use the component's product supplier roots of trust to verify the authenticity of the firmware, software, and configuration data needed for the component's boot process prior to it being used in the boot process.	Dispel's virtual desktop components can, at times, be considered Host Devices under the IEC 62443 framework. All firmware, software, and configuration data needed for the boot process is verified prior to use in the boot process.	Yes
NDR 3.14	**Integrity of the boot process**	Network devices shall verify the integrity of the firmware, software, and configuration data needed for the component's boot process prior to it being used in the boot process.	All Dispel components verify the integrity of firmware, software, and configuration data prior to use in the boot process.	Yes
NDR 3.14 RE 1	Authenticity of the boot process	Network devices shall use the component's product supplier roots of trust to verity the authenticity of the firmware, software, and configuration data needed for the component's boot process prior to it being used in the boot process.	All Dispel components verify the integrity of firmware, software, and configuration data against Dispel roots of trust prior to use in the boot process.	Yes

IEC 62443-4-2 FR 4 – Data Confidentiality

Part	Title	Requirement	Dispel Product/Feature	
CR 4.1	**Information confidentiality**	Components shall: A) Provide the capability to protect the confidentiality of information at rest for which explicit read authorization is supported; and, B) Support the protection of the confidentiality of information in transit as defined in IEC 62443-3-3 SR 4.1.	The only data stored at rest within a Dispel network is audit data. All audit data stored at rest is encrypted using AES 256. The Dispel's networks are colorless core, meaning all data, irrespective of its confidentiality tier or external factors such as zone traversal, is encrypted to the same level. The standard encryption treatment employed by Dispel in 2022 is to encrypt data with AES 256 using 4096-bit keys for the initial key exchange.	Yes
CR 4.2	**Information persistence**	Components shall provide the capability to erase all information, for which explicit read authorization is supported, from components to be released from active service and/or decommissioned.	All drives are re-encrypted then scrubbed to zero prior to their release from active service or decommissioning.	Yes

CR 4.2 RE 1	Erase of shared memory resources	Components shall provide the capability to protect against unauthorized and unintended information transfer via volatile shared memory resources. Volatile memory resources are those that generally do not retain information after being released to memory management. However, there are attacks against random access memory (RAM) which might extract key material or other confidential data before it is actually over-written. Therefore, when volatile shared memory is released back to the control system for use by a different user, all unique data and connections to unique data need to be purged from the resource so it is not visible or accessible to the new user.	All RAM is re-encrypted then scrubbed to zero as part of the decommissioning process.	Yes
CR 4.2 RE 2	Erase verification	Components shall provide the capability to verify that the erasure of information occurred.	Components are verified for erasure at the re-encryption stage.	Yes
CR 4.3	**Use of cryptography**	If cryptography is required, the component shall use cryptographic security mechanisms according to internationally recognized and proven security practices and recommendations.	Dispel's components meet or exceed CNSA Suite guidelines except in client-specified situations (eg: exceptionally low bandwidth environments).	Yes

IEC 62443-4-2 FR 5 – Restricted Data Flow

Part	Title	Requirement	Dispel Product/Feature	
CR 5.1	**Network segmentation**	Components shall support a segmented network to support zones and conduits, as needed, to support the broader network architecture based on logical segmentation and criticality.	Dispel's system supplies user, device, protocol, and network-level segmentation that can be mapped to a broader segmentation initiative or itself serve as the driver of that segmentation initiative.	Yes
CR 5.2	**Zone boundary protection**	The zone boundary protection requirements are network-component-specific and can be located as requirements for network devices in Clause 15.	Please see NDR 5.2, NDR 5.2 RE 1, NDR 5.2 RE 2, and NDR 5.2 RE 3. These requirements are met.	Yes
NDR 5.2	**Zone boundary protection**	A network device at a zone boundary shall provide the capability to monitor and control communications at zone boundaries to enforce the compartmentalization defined in the risk-based zones and conduits model.	Dispel's Wicket External System Integrator network component (a Wicket ESI) sits at the zone boundary. These components, along with their supporting Dispel components, monitor and control communications at the boundary.	Yes
NDR 5.2 RE 1	Deny all, permit by exception	The network component shall provide the capability to deny network traffic by default and allow network traffic by exception (also termed deny all, permit by exception).	All Dispel networks run on a deny-all, permit by exception model.	Yes
NDR 5.2 RE 2	Island mode	The network component shall provide the capability to protect against any communication through the control system boundary (also termed island mode).	Dispel network component provide the ability to lock down all inbound communications by destroying the network itself.	Yes

NDR 5.2 RE 3	Fail close	The network component shall provide the capability to protect against any communication through the control system boundary when there is an operational failure of the boundary protection mechanisms (also termed fail close).	Dispel network components fail-to-close except when expressly reconfigured by a customer to fail-to-open.	Yes
CR 5.3	**General-purpose person-to-person communication restrictions**	The general-purpose person-to-person communication restriction requirements are network component-specific and can be located as requirements for network devices in Clause 15.	Please see NDR 5.3. This requirement is met.	Yes
NDR 5.3	**General purpose, person-to-person communication restrictions**	A network device at a zone boundary shall provide the capability to protect against general purpose, person-to-person messages from being received from users or systems external to the control system.	Dispel networks rely upon protocol, device, IP, and port whitelisting as well as authentication barriers to prevent a user or system external to the control system from sending an unauthorized general purpose or person-to-person message.	Yes
CR 5.4	**Application partitioning**	There is no component level requirement associated with IEC 62443-3-3 SR 5.4.		Yes

IEC 62443-4-2 FR 6 – Timely Response To Events

Part	Title	Requirement	Dispel Product/Feature	
CR 6.1	**Audit log accessibility**	Components shall provide the capability for authorized humans and/or tools to access audit logs on a read-only basis.	Dispel provides customers with the ability to specify the manner in which audit logs are stored. By default, audit logs are stored on in-ear tape open write once, read many data tapes (LTO WORM).	Yes
CR 6.1 RE 1	Programmatic access to audit logs	Components shall provide programmatic access to audit records by either using an application programming interface (API) or sending the audit records to a centralized system.	Audit logs are sent to a centralized recording server which itself supplies an API.	Yes
CR 6.2	**Continuous monitoring**	Components shall provide the capability to be continuously monitored using commonly accepted security industry practices and recommendations to detect, characterize and report security breaches in a timely manner.	All components speak syslog which can be tied back to a monitoring system.	Yes

IEC 62443-4-2 FR 7 – Resource Availability

Part	Title	Requirement	Dispel Product/Feature	
CR 7.1	**Denial of service protection**	Components shall provide the capability to maintain essential functions when operating in a degraded mode as the result of a DoS event.	Components will continue to operate at lower bandwidths experienced as a result of a DoS event.	Yes
CR 7.1 RE 1	Manage communication load from component	Components shall provide the capability to mitigate the effects of information and/or message flooding types of DoS events.	Dispel manages communication loads by employing IP whitelisting between network components, being outbound-only at the Wicket ESI for establishing a connection to the first point in a remote access network, and for being unresponsive to inbound communications on all components once a connection is established (other than from that one IP address, of course). These actions have the effect of mitigating the risk of at DoS event taking place.	Yes
CR 7.2	**Resource management**	Components shall provide the capability to limit the use of resources by security functions to protect against resource exhaustion.	Dispel's components are positioned in virtualized environments which allow their resource consumption rates to be capped without relying upon any other part of the Dispel system functioning properly.	Yes
CR 7.3	**Control system backup**	Components shall provide the capability to participate in system level backup operations in order to safeguard the component state (user- and system-level information). The backup process shall not affect the normal component operations.	All backup data on Dispel's system is run from resource pools that are independent of those used to support normal component operations.	Yes

CR 7.3 RE 1	Backup integrity verification	Components shall provide the capability to validate the integrity of backed up information prior to the initiation of a restore of that information.	Dispel's components recover and reconstitute from "golden images" whose validity can themselves be checked to meet CR 7.3 RE 1.	Yes
CR 7.4	**Control system recovery and reconstitution**	Components shall provide the capability to be recovered and reconstituted to a known secure state after a disruption or failure.	Dispel's components recover and reconstitute from "golden images", which are known, secure, states.	Yes
CR 7.5	**Emergency power**	There is no component level requirement associated with IEC 62443-3-3 SR 7.5.		Yes
CR 7.6	**Network and security configuration settings**	Components shall provide the capability to be configured according to recommended network and security configurations as described in guidelines provided by the control system supplier. The component shall provide an interface to the currently deployed network and security configuration settings.	All Dispel components can be configured through the Dispel management console.	Yes
CR 7.6 RE 1	Machine-readable reporting of current security settings	Components shall provide the capability to generate a report listing the currently deployed security settings in a machine-readable format.	Dispel supplies an API through which security settings can be pulled from all deployed components.	Yes
CR 7.7	**Least functionality**	Components shall provide the capability to specifically restrict the use of unnecessary functions, ports, protocols and/or services.	All Dispel deployments are launched with protocol, process, port, and IP whitelists.	Yes
CR 7.8	**Control system component inventory**	Components shall provide the capability to support a control system component inventory according to IEC 62443-3-3 SR 7.8.	Supporting IEC 62443-3-3 SR 7.8, all Dispel components are listed along with their specifications in the Dispel management console.	Yes

END

About Dispel
Dispel supplies secure remote access platforms for industrial control systems. Dispel serves over 44 million people and partners from offices in New York, Austin, Boston, Denver, Virginia, and Tokyo.

Dispel, LLC
61 Greenpoint Ave,
Suite 634
Brooklyn, NY 11222

dispel.io

For more information
enterprise@dispel.io
+1-917-268-5190

Printed September 8, 2022

Utilities and manufacturers use Dispel for secure remote access to their industrial control systems. Dispel serves over 44 million people and partners every day from offices in New York, Austin, Virginia, and Tokyo.

dispel.com | enterprise@dispel.com