WHITE PAPER

HOW ARUBA SECURITY SOLUTIONS SUPPORT NIST COMPLIANCE

aruba
a Hewlett Packard Enterprise company

TABLE OF CONTENTS

OVERVIEW

In April 2018 NIST released their long-anticipated update to their Cybersecurity Framework, version 1.1, designed to help organizations of all sizes improve their overall risk management pursuant to the CyberSecurity Enhancement Act of 2014.

The Framework Core is a set of recommended security activities and outcomes and is organized into five major Functions:

- Identify
- Protect
- Detect
- Respond
- Recover

Each Function is further subdivided into sub-categories which describe a specific outcome along with the associated references to other standards such as COBIT and ISO/IEC—there are over 100 subcategories in total.

Given its mission to provide risk management guidelines across a wide spectrum of security activities, the Framework Core is very broad and covers a comprehensive list of recommendations. As such, no product or even a single vendor can provide support for all 100+ outcomes. Nevertheless, it is important to understand how an individual or group of products can support NIST compliance, and to what extent. With a mapping of products and capabilities to the Framework Core matrix, organizations can see where there is coverage and where gaps might exist.

The purpose of this white paper is to describe how the products and technologies in the Aruba 360 Secure Fabric can contribute to overall NIST compliance. The 360 Fabric is a security architecture in which Aruba security products can deliver on the individual NIST mandates. As is outlined below, Aruba can contibute to over 40 of the 100+ subcategories across all the Functions and in aggregate significantly enhance an organization's ability to mitigate risk and respond to attacks before they do damage.

ABOUT THE ARUBA SECURITY SOLUTIONS: THE 360 SECURE FABRIC

The Aruba 360° Secure Fabric gives security and IT teams a simpler way to quickly detect and respond to advanced cyberattacks across multi-vendor infrastructures, supporting a wide range of enterprises and securing anywhere from hundreds to millions of users and devices.

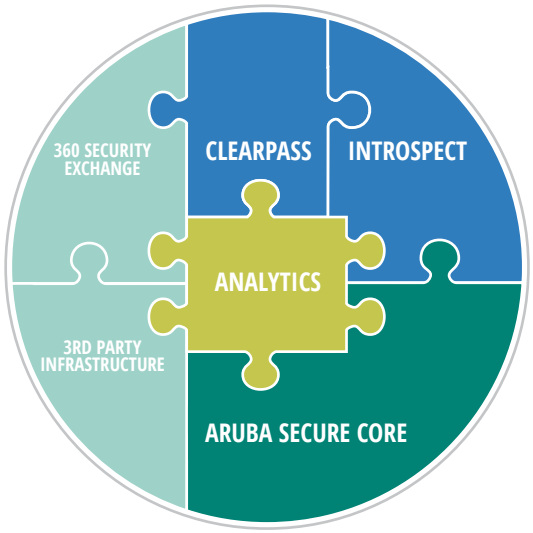

Figure 1: The Aruba 360 Secure Fabric provides an integrated security framework for IT and security teams to provide 360 degrees of protection, centered around analytics.

Components of the Aruba 360 Secure Fabric include the following:

- **Aruba Secure Infrastructure:** essential security capabilities embedded in the foundation for all of Aruba's Wi-Fi access points, switches and wireless controllers. With Aruba Secure Infrastructure, IT administrators can be assured that network devices such as switches and wireless access points have not been compromised.
- **Aruba IntroSpect User and Entity Behavior Analytics (UEBA):** a family of continuous monitoring and advanced attack detection software, that uses machine learning to spot small changes in behavior that often indicate attacks that have evaded traditional security defenses. Machine learning algorithms create Risk Scores based on the severity of an attack to prioritize incident investigations for security teams.
- **Aruba ClearPass:** a robust secure network access control (NAC) and policy management solution providing device discovery and closed-loop, authentication and authorization and attack response, through built-in integration with Aruba IntroSpect and other third party security solutions.
- **Aruba 360 Security Exchange:** this is the Aruba technology partner ecosystem consisting of more than 140 leading security and IT solution providers who collaborate with Aruba to offer pre-integrated, best-in-class enterprise security solutions.

These are the components that will be cross-referenced to the NIST framework as described below.

IDENTIFY

In this part of the Framework the foundation for all subsequent security activities is established. The recommendations are focused on helping an organization understand what assets are critical to their organization and how to develop policies to protect them, while bringing people and process together in a coordinated set of activities.

With ClearPass, Aruba provides an effective mechanism for defining and implementing risk-based policies that capture what roles and privileges an organization wants to assign to users and devices, while anticipating what actions to take in the event of a compromise. Given IntroSpect's encyclopedia understanding of the internal threat environment, it is an excellent clearinghouse for external threat intelligence as well as internal attack behaviors.

Subcategory	Aruba Product	Use Case	Informative References
ID.AM-1: Physical devices and systems within the organization are inventoried	ClearPass Policy Manager	Device discovery and profiling via multiple passive and active techniques.	• CIS CSC 1 • COBIT 5 BAI09.01, BAI09.02 • ISA 62443-2-1:2009 4.2.3.4 • ISA 62443-3-3:2013 SR 7.8 • ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 • NIST SP 800-53 Rev. 4 CM-8, PM-5
ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stake-holders (e.g., suppliers, customers, partners) are established	ClearPass Policy Manager	Authrizations established based on a wide variety of factors in including org role, devices used, etc. Special emphasis on TACACS+ admin access to switches.	• CIS CSC 17, 19 • COBIT 5 APO01.02, APO07.06, APO13.01, DSS06.03 • ISA 62443-2-1:2009 4.3.2.3.3 • ISO/IEC 27001:2013 A.6.1.1 • NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	IntroSpect UEBA	Focuses analytics and prioritizes risk scores on the basis of high value assets and actors.	• COBIT 5 APO10.01, BAI04.02, BAI09.02 • ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3 • NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14
ID.GV-1: Organizational cybersecurity policy is established and communicated	ClearPass Policy Manager	Rich policy engine that defines access privileges to IT resources based on multiple variables.	• CIS CSC 19 • COBIT 5 APO01.03, APO13.01, EDM01.01, EDM01.02 • ISA 62443-2-1:2009 4.3.2.6 • ISO/IEC 27001:2013 A.5.1.1 • NIST SP 800-53 Rev. 4 -1 controls from all security control families
ID.GV-4: Governance and risk management processes address cybersecurity risks	ClearPass Policy Manager	Organization policies emboddied in ClearPass access control policies.	• COBIT 5 EDM03.02, APO12.02, APO12.05, DSS04.02 • ISA 62443-2-1:2009 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 • ISO/IEC 27001:2013 Clause 6 • NIST SP 800-53 Rev. 4 SA-2, PM-3, PM-7, PM-9, PM-10, PM-11
ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources	IntroSpect UEBA	Accepts wide variety of threat intelligence feeds vis STIX/TAXII or custom integrations.	• CIS CSC 4 • COBIT 5 BAI08.01 • ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 • ISO/IEC 27001:2013 A.6.1.4 • NIST SP 800-53 Rev. 4 SI-5, PM-15, PM-16
ID.RA-3: Threats, both internal and external, are identified and documented	IntroSpect UEBA	Machine learning-based analytics use both super-vised and unsupervised models to detect attacks on the inside before they do damage.	• CIS CSC 4 • COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04 • ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 • ISO/IEC 27001:2013 Clause 6.1.2 • NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12, PM-16
ID.RA-6: Risk responses are identified and prioritized	ClearPass Policy Manager	The same policy-based mechanisms that authorize IT access can be used to respond to threats and attackes (quarantine, block, etc.).	• CIS CSC 4 • COBIT 5 APO12.05, APO13.02 • ISO/IEC 27001:2013 Clause 6.1.3 • NIST SP 800-53 Rev. 4 PM-4, PM-9

PROTECT

Once the critical assets, actors and processes are identified with the associated risks in case of compromise, the next step in the Foundation is to define protective controls. This is where the entire Aruba security portfolio delivers results. This ranges from wired and wireless hardware tamper-proofing to military-grade encryption to ClearPass' policies for identity-based network access control backed by machine learning-driven attack detection and response via IntroSpect.

Subcategory	Aruba Product	Use Case	Informative References
PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	ClearPass Policy Manager	CPPM authenticates directly to up-to-date identity systems of record and authorizes access based on legitimate credentials and associated privileges.	• CIS CSC 1, 5, 15, 16 • COBIT 5 DSS05.04, DSS06.03 • ISA 62443-2-1:2009 4.3.3.5.1 • ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 • ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3 • NIST SP 800-53 Rev. 4 AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11
PR.AC-2: Physical access to assets is managed and protected	Wireless Access Points	Aruba does not store encryption keys in access to eliminate potential for physical compromise of encryption.	• COBIT 5 DSS01.04, DSS05.05 • ISA 62443-2-1:2009 4.3.3.3.2, 4.3.3.3.8 • ISO/IEC 27001:2013 A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2 • NIST SP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE-5, PE-6, PE-8
PR.AC-3: Remote access is managed	VIA VPN Client RAP VPN-based Wireless Access Point ClearPass Policy Manager	Multiple ways to control and secure remote access. CPPM enforces access policies based on level of remote protection.	• CIS CSC 12 • COBIT 5 APO13.01, DSS01.04, DSS05.03 • ISA 62443-2-1:2009 4.3.3.6.6 • ISA 62443-3-3:2013 SR 1.13, SR 2.6 • ISO/IEC 27001:2013 A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1 • NIST SP 800-53 Rev. 4 AC-1, AC-17, AC-19, AC-20, SC-15
PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	ClearPass Policy Manager	Role-based access control based on organization policies enforced in network infrastructure.	• CIS CSC 3, 5, 12, 14, 15, 16, 18 • COBIT 5 DSS05.04 • ISA 62443-2-1:2009 4.3.3.7.3 • ISA 62443-3-3:2013 SR 2.1 • ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5 • NIST SP 800-53 Rev. 4 AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24
PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	ClearPass Policy Manager Swtiches Wireless Access Points	Through the use of role-based access control ClearPass enables a single user or device policy to be enforced seamlessly across wired, wireless or remote access and can segment traffic based on role attributes.	• CIS CSC 9, 14, 15, 18 • COBIT 5 DSS01.05, DSS05.02 • ISA 62443-2-1:2009 4.3.3.4 • ISA 62443-3-3:2013 SR 3.1, SR 3.8 • ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3 • NIST SP 800-53 Rev. 4 AC-4, AC-10, SC-7
PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	ClearPass Policy Manager	ClearPass automatically-binds identity authentication IT access priviliges via inter-actions with IDM systems such as Active Directory.	• CIS CSC, 16 • COBIT 5 DSS05.04, DSS05.05, DSS05.07, DSS06.03 • ISA 62443-2-1:2009 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 • ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 • ISO/IEC 27001:2013, A.7.1.1, A.9.2.1 • NIST SP 800-53 Rev. 4 AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3

Subcategory	Aruba Product	Use Case	Informative References
PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	ClearPass Policy Manager	ClearPass supports a wide range of authentication techniques including multi-factor authentication.	• CIS CSC 1, 12, 15, 16 • COBIT 5 DSS05.04, DSS05.10, DSS06.10 • ISA 62443-2-1:2009 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9 • ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 • ISO/IEC 27001:2013 A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 • NIST SP 800-53 Rev. 4 AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11
PR.DS-2: Data-in-transit is protected	Switches Wireless Access Points	Traffic is encrypted using WPA-2 and Suite B level encryption.	• CIS CSC 13, 14 • COBIT 5 APO01.06, DSS05.02, DSS06.06 • ISA 62443-3-3:2013 SR 3.1, SR 3.8, SR 4.1, SR 4.2 • ISO/IEC 27001:2013 A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 • NIST SP 800-53 Rev. 4 SC-8, SC-11, SC-12
PR.DS-5: Protections against data leaks are implemented	IntroSpect UEBA	Machine learning models look for large data movements combined with other indications of compromised to detect data exfiltration.	• CIS CSC 13 • COBIT 5 APO01.06, DSS05.04, DSS05.07, DSS06.02 • ISA 62443-3-3:2013 SR 5.2 • ISO/IEC 27001:2013 A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.10.1.1, A.11.1.4, A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 • NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4
PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	Switches Wireless Access Points	Use of TPM hardware ensures hardware has not been tampered with and that the boot process is secure.	• CIS CSC 2, 3 • COBIT 5 APO01.06, BAI06.01, DSS06.02 • ISA 62443-3-3:2013 SR 3.1, SR 3.3, SR 3.4, SR 3.8 • ISO/IEC 27001:2013 A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4 • NIST SP 800-53 Rev. 4 SC-16, SI-7
PR.IP-3: Configuration change control processes are in place	ClearPass Policy Manager	TACACS+ support ensures that only authorized admins can change network device configurations	• CIS CSC 3, 11 • COBIT 5 BAI01.06, BAI06.01 • ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 • ISA 62443-3-3:2013 SR 7.6 • ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 • NIST SP 800-53 Rev. 4 CM-3, CM-4, SA-10
PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	IntroSpect UEBA ClearPass Policy Manager	IntroSpect provides playbooks that inform the security team how to respond to an attack. ClearPass Policy Manager defines actions that can be taken in response to an attack.	• CIS CSC 19 • COBIT 5 APO12.06, DSS04.03 • ISA 62443-2-1:2009 4.3.2.5.3, 4.3.4.5.1 • ISO/IEC 27001:2013 A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3 • NIST SP 800-53 Rev. 4 CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17
PR.PT-4: Communications and control networks are protected	Switches Wireless Access Points	Secure storage of encryption keys. Device hardening via TPM. TACACS+ support ensures that only authorized admins change network settings.	• CIS CSC 8, 12, 15 • COBIT 5 DSS05.02, APO13.01 • ISA 62443-3-3:2013 SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 • ISO/IEC 27001:2013 A.13.1.1, A.13.2.1, A.14.1.3 • NIST SP 800-53 Rev. 4 AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43

DETECT

Aruba IntroSpect User and Entity Behavior Analytics is front and center for the Detect section of the Foundation because it utilizes machine learning to find small changes in behavior that are often indicative of attacks that have evaded traditional defenses. The continuous monitoring that IntroSpect provides is particularly important because even when security policies and procedures are followed and controls are in place, users who have opened the wrong email attachment or visited the wrong website may be inadvertently compromised—and it's their credentials that are propagating the exploit.

Subcategory	Aruba Product	Use Case	Informative References
DE.AE-2: Detected events are analyzed to understand attack targets and methods	IntroSpect UEBA	Machine learning models and rules detect gestating attacks. Consolidated forensic evidence enables security team to rapidly investigate the cause and impact to formulate a response plan.	• CIS CSC 3, 6, 13, 15 • COBIT 5 DSS05.07 • ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 • ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 • ISO/IEC 27001:2013 A.12.4.1, A.16.1.1, A.16.1.4 • NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, SI-4
DE.AE-3: Event data are collected and correlated from multiple sources and sensors	IntroSpect UEBA	IntroSpect is the only UEBA solution that collects and analyzes packets, flows, logs and alerts.	• CIS CSC 1, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16 • COBIT 5 BAI08.02 • ISA 62443-3-3:2013 SR 6.1 • ISO/IEC 27001:2013 A.12.4.1, A.16.1.7 • NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
DE.AE-4: Impact of events is determined	IntroSpect UEBA	Risk scores based on detecting small changes in behavior combined with clearly malicious activity put every event in context.	• CIS CSC 4, 6 • COBIT 5 APO12.06, DSS03.01 • ISO/IEC 27001:2013 A.16.1.4 • NIST SP 800-53 Rev. 4 CP-2, IR-4, RA-3, SI-4
DE.AE-5: Incident alert thresholds are established	IntroSpect UEBA	Security teams can take a range of actions based on risk score. Variables include raw score (1-100), rate of change value of the asset involved, etc.	• CIS CSC 6, 19 • COBIT 5 APO12.06, DSS03.01 • ISA 62443-2-1:2009 4.2.3.10 • ISO/IEC 27001:2013 A.16.1.4 • NIST SP 800-53 Rev. 4 IR-4, IR-5, IR-8
DE.CM-1: The network is monitored to detect potential cybersecurity events	IntroSpect UEBA Switches Wireless Access Points	IntroSpect is the only UEBA solution that collects and analyzes packets. Aruba switches generated security alerts based on the traffic they see. Aruba wireless controllers generate logs that describe wireless network activity.	• CIS CSC 1, 7, 8, 12, 13, 15, 16 • COBIT 5 DSS01.03, DSS03.05, DSS05.07 • ISA 62443-3-3:2013 SR 6.2 • NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4
DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	IntroSpect UEBA	User identity is tied to IT activity including device and address history which is analyzed for anomalous behavior and malicious activity.	• CIS CSC 5, 7, 14, 16 • COBIT 5 DSS05.07 • ISA 62443-3-3:2013 SR 6.2 • ISO/IEC 27001:2013 A.12.4.1, A.12.4.3 • NIST SP 800-53 Rev. 4 AC-2, AU-12, AU-13, CA-7, CM-10, CM-11
DE.CM-5: Unauthorized mobile code is detected	ClearPass Policy Manager	ClearPass integrates with Enterprise Mobility Management solutions such as MobileIron, AirWatch, InTune, etc. This allows ClearPass to change access privileges based on the security state of the mobile device: protections, rogue applications, jail breaks, etc.	• CIS CSC 7, 8 • COBIT 5 DSS05.01 • ISA 62443-3-3:2013 SR 2.4 • ISO/IEC 27001:2013 A.12.5.1, A.12.6.2 • NIST SP 800-53 Rev. 4 SC-18, SI-4, SC-44

Subcategory	Aruba Product	Use Case	Informative References
DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	IntroSpect UEBA	IntroSpect monitors any entity accessing IT resources, including partners or external parties.	• COBIT 5 APO07.06, APO10.05 • ISO/IEC 27001:2013 A.14.2.7, A.15.2.1 • NIST SP 800-53 Rev. 4 CA-7, PS-7, SA-4, SA-9, SI-4
DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	ClearPass Policy Manager IntroSpect UEBA	ClearPass will detect and prevent unauthorized access. Should an authorized user or device become compromised, IntroSpect will detect the changes in behavior indicative of an attack.	• CIS CSC 1, 2, 3, 5, 9, 12, 13, 15, 16 • COBIT 5 DSS05.02, DSS05.05 • ISO/IEC 27001:2013 A.12.4.1, A.14.2.7, A.15.2.1 • NIST SP 800-53 Rev. 4 AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4
DE.DP-2: Detection activities comply with all applicable requirements	IntroSpect UEBA	Machine learning models deliver a complementary dimension of attack detection for traditional defenses that use rule, pattern matching and other static techniques.	• COBIT 5 DSS06.01, MEA03.03, MEA03.04 • ISA 62443-2-1:2009 4.4.3.2 • ISO/IEC 27001:2013 A.18.1.4, A.18.2.2, A.18.2.3 • NIST SP 800-53 Rev. 4 AC-25, CA-2, CA-7, SA-18, SI-4, PM-14
DE.DP-4: Event detection information is communicated	IntroSpect UEBA	IntroSpect aggregates and analyzes a wide range of IT activity data (events) and stores it in an easily-accessible forensic database. Security analysts have “one click” access to key information for incident investigations.	• CIS CSC 19 • COBIT 5 APO08.04, APO12.06, DSS02.05 • ISA 62443-2-1:2009 4.3.4.5.9 • ISA 62443-3-3:2013 SR 6.1 • ISO/IEC 27001:2013 A.16.1.2, A.16.1.3 • NIST SP 800-53 Rev. 4 AU-6, CA-2, CA-7, RA-5, SI-4

RESPOND

The timing and effectiveness of attack response is often the difference between a small incident and a headline-making crisis. IntroSpect is particularly effective in collecting and presenting the forensic information the security teams need to quickly understand the situation, make decisions and implement actions. In some cases, customers have measured up to 30 hours of savings in their incident response process. From an attack response perspective, IntroSpect and ClearPass are seamlessly integrated such that the ClearPass policy engine can take the appropriate action based on pre-define remediation procedures—from re-authentication to quarantine to block. ClearPass can execute the same attack response based on signals or alerts from third party security solutions as well.

Subcategory	Aruba Product	Use Case	Informative References
RS.RP-1: Response plan is executed during or after an incident	IntroSpect UEBA ClearPass Policy Manager	IntroSpect includes play-books of standard incident response activities that are available to the entire security team. ClearPass policies capture attack responses based on the serverity of the incident and the assets involved.	• CIS CSC 19 • COBIT 5 APO12.06, BAI01.10 • ISA 62443-2-1:2009 4.3.4.5.1 • ISO/IEC 27001:2013 A.16.1.5 • NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR-8
RS.AN-1: Notifications from detection systems are investigated	IntroSpect UEBA	Organizations can use the IntroSpect incident investiga-tion system directly from the console, or via established SOC workflow through deep integration with SIEM products such as ArcSight, QRadar, Splunk etc.	• CIS CSC 4, 6, 8, 19 • COBIT 5 DSS02.04, DSS02.07 • ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 • ISA 62443-3-3:2013 SR 6.1 • ISO/IEC 27001:2013 A.12.4.1, A.12.4.3, A.16.1.5 • NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, PE-6, SI-4
RS.AN-2: The impact of the incident is understood	IntroSpect UEBA	Introspect's historical record of forensic information enables the security team to immediately assess who is involved in an attack, who they communicated with and what other resources were involved.	• COBIT 5 DSS02.02 • ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 • ISO/IEC 27001:2013 A.16.1.4, A.16.1.6 • NIST SP 800-53 Rev. 4 CP-2, IR-4
RS.AN-3: Forensics are performed	IntroSpect UEBA	IntroSpect provides a full fornesic record of all the relevant security behavior for a user, system or device and delivers that in in a consolidated view for the security analyst.	• COBIT 5 APO12.06, DSS03.02, DSS05.07 • ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 • ISO/IEC 27001:2013 A.16.1.7 • NIST SP 800-53 Rev. 4 AU-7, IR-4
RS.AN-4: Incidents are categorized consistent with response plans	IntroSpect UEBA ClearPass Policy Manager	IntroSpect will describe and categorize incidents based on the importance of the users or systems involved and ClearPass will take the actions consistent with pre-defined response plans.	• CIS CSC 19 • COBIT 5 DSS02.02 • ISA 62443-2-1:2009 4.3.4.5.6 • ISO/IEC 27001:2013 A.16.1.4 • NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-5, IR-8
RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)	IntroSpect UEBA	Based on the deep forensic record that has been tagged with the relevant threat data, an analyst can use the IntroSpect threat hunting system to look for and find indications of compromise that have been discovered by scans, external threat feeds, etc.	• CIS CSC 4, 19 • COBIT 5 EDM03.02, DSS05.07 • NIST SP 800-53 Rev. 4 SI-5, PM-15

Subcategory	Aruba Product	Use Case	Informative References
RS.MI-1: Incidents are contained	ClearPass Policy Manager	Once an attack or incident has been identified, the ClearPass position as "gate-keeper" of the network can be used to either manually or automatically take actions to contain it.	• CIS CSC 19 • COBIT 5 APO12.06 • ISA 62443-2-1:2009 4.3.4.5.6 • ISA 62443-3-3:2013 SR 5.1, SR 5.2, SR 5.4 • ISO/IEC 27001:2013 A.12.2.1, A.16.1.5 • NIST SP 800-53 Rev. 4 IR-4
RS.MI-2: Incidents are mitigated	ClearPass Policy Manager	Actions that ClearPass can take include: re-authentication, bandwidth control, quarantine and block.	• CIS CSC 4, 19 • COBIT 5 APO12.06 • ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.10 • ISO/IEC 27001:2013 A.12.2.1, A.16.1.5 • NIST SP 800-53 Rev. 4 IR-4

RECOVER

As noted above, the ClearPass policy manager leverages its position as "gatekeeper" on the network to take an action in response to an attack that will fit into a larger incident response process. ClearPass can quarantine devices and users so they will not do damage and issue a trouble ticket so the IT team can follow up and clean up the infected endpoint.

Subcategory	Aruba Product	Use Case	Informative References
RC.IM-1: Recovery plans incorporate lessons learned	IntroSpect UEBA ClearPass Policy Manager	IntroSpect playbooks can be updated to reflect learnings from previous incidents as well as the ClearPass policies associated with the remediation.	• COBIT 5 APO12.06, BAI05.07, DSS04.08 • ISA 62443-2-1:2009 4.4.3.4 • ISO/IEC 27001:2013 A.16.1.6, Clause 10 • NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
RC.IM-2: Recovery strategies are updated	IntroSpect UEBA ClearPass Policy Manager	Both IntroSpect and ClearPass provide multiple paths for updating by the security team with customized UI's for analytics, workflow and remediation improvements.	• COBIT 5 APO12.06, BAI07.08 • ISO/IEC 27001:2013 A.16.1.6, Clause 10 • IST SP 800-53 Rev. 4 CP-2, IR-4, IR-8

SUMMARY

The Aruba security portfolio provides a unique set of controls and support for the NIST CyberSecurity Framework v1.1. The mapping of solutions to the updated Framework leverages the broad range of secure infrastructure, policy-based access control and post-admission behavioral monitoring offered by the Aruba 360 Secure Fabric. Most importantly, Aruba's integration with a broad range of security and general IT solutions means that those products can complement and add to what Aruba is delivering to comprehensively cover the NIST recommendations.

aruba
a Hewlett Packard Enterprise company

3333 SCOTT BLVD | SANTA CLARA, CA 95054
1.844.473.2782 | T: 1.408.227.4500 | FAX: 1.408.227.4550 | INFO@ARUBANETWORKS.COM

www.arubanetworks.com