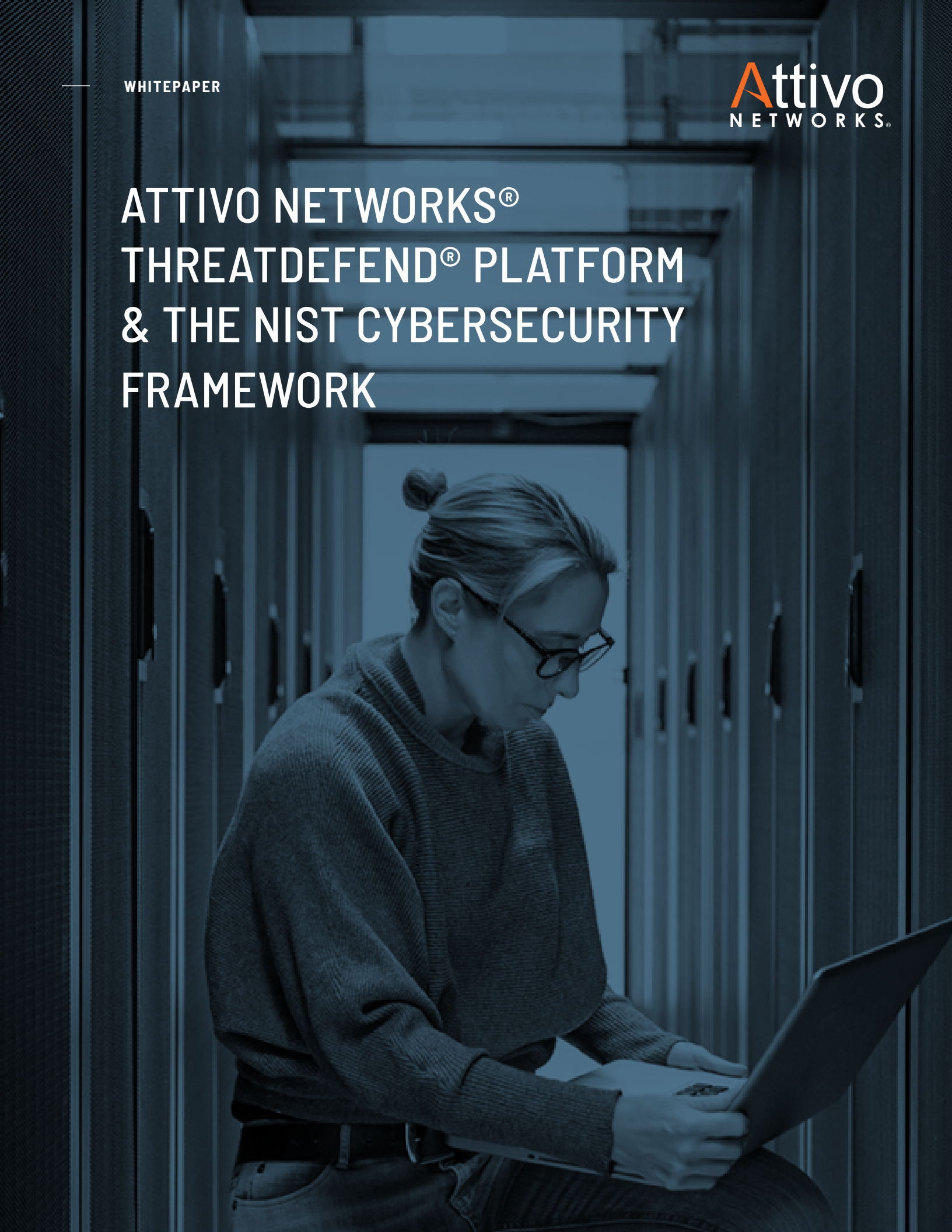
WHITEPAPER

Attivo NETWORKS®

ATTIVO NETWORKS® THREATDEFEND® PLATFORM & THE NIST CYBERSECURITY FRAMEWORK



INTRODUCTION

The National Institute of Standards and Technology (NIST) Cybersecurity Framework provides a policy framework of computer security guidance for how private sector organizations in the US can assess and improve their ability to prevent, detect, and respond to cyberattacks. Updated to v1.1 in April 2018, this voluntary framework consists of standards, guidelines, and best practices to help organizations manage cybersecurity risks. While initially designed for critical infrastructure, many organizations across all industries have applied it to be proactive about cyber risk management. More information about the framework is at https://www.nist.gov/cyberframework.

THE FRAMEWORK

The framework breaks down into three parts, "Core", "Profile," and "Tiers". The "Framework Core" contains an array of activities, outcomes, and approaches to cybersecurity. The "Framework Implementation Tiers" are used by an organization to clarify how it views cybersecurity risk for itself and its partners and the degree of sophistication of its management approach. A "Framework Profile" is a list of outcomes that an organization has chosen from the categories and subcategories based on its needs and risk assessments.

The NIST Cybersecurity Framework organizes its Core material into five Functions which it subdivides into a total of 23 Categories. For each category, it defines 108 Subcategories of cybersecurity outcomes and security controls. Each subcategory includes "Informative Resources" referencing specific sections of other information security standards, including ISO 27001, COBIT, NIST SP 800-53 Rev 4, ISA 62443, and the Council on Cybersecurity Critical Security Controls.

The Core Functions are:

IDENTIFY - Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.	
• ID.AM - Asset Management	• ID.BE - Business Environment
• ID.GV – Governance	• ID.SC - Supply Chain Risk Management
• IR.RA - Risk Assessment	• IR.RM - Risk Management Strategy
PROTECT - Develop and implement the appropriate safeguards to ensure the delivery of critical infrastructure services.	
• PR.AC - Access Control	• PR.IP - Information Protection Processes and Procedures
• PR.AT - Awareness and Training	• PR.MA - Maintenance
• PR.DS - Data Security	• PR.PT - Protective Technology
DETECT - Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.	
• DE.AW - Anomalies and Events	• DE.DP - Detection Processes
• DE.CM - Security Continuous Monitoring	

RESPOND - Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.	
• RS.RP - Response Planning	• RS.MI - Mitigation
• RS.CO - Communications	• RS.IM – Improvements
• RS.AN – Analysis	
RECOVER - Develop and implement the appropriate activities to maintain resilience plans and restore any capabilities or services impaired due to a cybersecurity event.	
• RC.RP - Recovery Planning	• RC.CO – Communications
• RC.IM – Improvements	

ATTIVO NETWORKS SUPPORT FOR THE NIST CYBERSECURITY FRAMEWORK

The Attivo Networks ThreatDefend® Platform identifies risks, provides least privileges access to data, and detects credential theft, privilege escalation, lateral movement, and target acquisition across endpoints, Active Directory (AD), clouds, and networks. Concealment technology hides critical AD objects, data, and credentials, while misdirection and deception decoys derail attack activities. Automated intelligence collection, attack analysis, and third-party integrations accelerate incident response. The platform includes BOTsink® deception servers, the Endpoint Detection Net suite for endpoint defenses, the ADSecure and ADAssessor solutions for Active Directory protection, and the IDEntitleX solution to protect cloud identities and entitlements.

In evaluating the ThreatDefend Platform against the NIST Cybersecurity Framework, Attivo Networks compared the solution against the NIST SP 800-53 Rev 4 controls referenced in each subcategory. The following table lists the specific reference controls and how the ThreatDefend Platform meets each one.

Visit https://attivonetworks.com/product/threatdefend/ for more information on the ThreatDefend Platform.

Control	Title	Product	Function
AC-10	CONCURRENT SESSION CONTROL	ThreatDefend Platform	Offers a policy for controlling several concurrent user sessions to the management interface.
AC-12	SESSION TERMINATION	ThreatDefend Platform	Offers a policy for session logout due to inactivity on the management interface.
AC-17	PRIVILEGED COMMANDS / ACCESS	ADSecure	Detects and prevents attackers that are trying to escalate privileges. Hides critical information to prevent attackers from advancing their goals.

Control	Title	Product	Function
AU-13	MONITORING FOR INFORMATION DISCLOSURE	DecoyDocs function	Determines if attackers have stolen a decoy document and the geolocation of the systems that opened it.
CA-2	SECURITY ASSESSMENTS	ADAssessor	Performs a continuous assessment of Active Directory and provides real-time analysis of AD attacks.
CA-7	CONTINUOUS MONITORING	ADAssessor	Continuously monitors AD vulnerabilities and audits misconfigurations that lead to privilege escalations and lateral movements.
CM-8	INFORMATION SYSTEM COMPONENT INVENTORY	BOTsink visibility functions	Automatically learns the network, including Adds and Changes, and tracks systems as they join or leave.
IR-4	INCIDENT HANDLING	BOTsink ThreatOps module	Incident response orchestration that creates repeatable playbooks using native partner integrations.
PM-5	INFORMATION SYSTEM INVENTORY	BOTsink visibility functions	Automatically learns the network, including Adds and Changes, and tracks systems as they join or leave.
RA-3	RISK ASSESSMENT	EDN ThreatPath	Identifies stored credential vulnerabilities and misconfigurations that allow an attacker to move laterally within the network.
RA-4	RISK ASSESSMENT UPDATE	EDN ThreatPath	Identifies stored credential vulnerabilities and misconfigurations that allow an attacker to move laterally within the network.
RA-5	VULNERABILITY SCANNING	EDN ThreatPath	Identifies stored credential vulnerabilities and misconfigurations that allow an attacker to move laterally within the network.
SC-19	VOICE OVER INTERNET PROTOCOL	BOTsink VOIP decoy	Detects attacks targeting Cisco VOIP Telephony devices.
SC-28	PROTECTION OF INFORMATION AT REST	DecoyDocs, BOTsink file server decoys	BOTsink file server decoys and DecoyDocs alert on unauthorized access.
SC-36	DISTRIBUTED PROCESSING AND STORAGE	Attivo Central Manager	Supports failover for High-Availability deployments.
SC-38	OPERATIONS SECURITY	ThreatDefend Platform	EDN ThreatPath identifies credential vulnerabilities at endpoints, while ADAssessor identifies them on Active Directory. The ThreatDefend Platform provides countermeasures.
SC-44	DETONATION CHAMBERS	BOTsink Malware Analysis Sandbox	Built-in malware analysis sandbox functions.

Control	Title	Product	Function
SI-3	MALICIOUS CODE PROTECTION, NON-SIGNATURE-BASED DETECTION, DETECT UNAUTHORIZED COMMANDS	ThreatDefend Platform	Offers malware sandbox used to analyze malicious code and understand TTPs. Detects threat behaviors without using relying on signatures. ADSecure also detects the use of unauthorized commands.
SI-4	INFORMATION SYSTEM MONITORING	ThreatDefend Platform	Detects reconnaissance, lateral movement, MITM, and AD attacks.
SI-5	SECURITY ALERTS, ADVISORIES, AND DIRECTIVES	ThreatDefend Platform	Generates alerts and gathers forensics for threat intelligence development.

From these reference controls, the ThreatDefend Platform meets the following 44 Framework subcategories:

Subcategory	Informative References	Attivo Solution
ID.AM-1: Physical devices and systems within the organization are inventoried	NIST SP 800-53 Rev. 4 CM-8, PM-5	CM-8, PM-5
ID.AM-2: Software platforms and applications within the organization are inventoried	NIST SP 800-53 Rev. 4 CM-8, PM-5	CM-8, PM-5
ID.RA-1: Asset vulnerabilities are identified and documented	NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5	RA-3, RA-5, SI-4, SI-5, CA-2, CA-7
ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources	NIST SP 800-53 Rev. 4 SI-5, PM-15, PM-16	SI-5
ID.RA-3: Threats, both internal and external, are identified and documented	NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12, PM-16	RA-3, SI-5
ID.RA-4: Potential business impacts and likelihoods are identified	NIST SP 800-53 Rev. 4 RA-2, RA-3, SA-14, PM-9, PM-11	RA-3
ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16	RA-3
PR.AC-3: Remote access is managed	NIST SP 800-53 Rev. 4 AC-1, AC-17, AC-19, AC-20, SC-15	AC-17
PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	NIST SP 800-53 Rev. 4 AC-4, AC-10, SC-7	AC-10
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)	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	AC-12
PR.DS-1: Data-at-rest is protected	NIST SP 800-53 Rev. 4 MP-8, SC-12, SC-28	SC-28
PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	NIST SP 800-53 Rev. 4 CM-8, MP-6, PE-16	CM-8
PR.DS-5: Protections against data leaks are implemented	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	SI-4

Subcategory	Informative References	Attivo Solution
PR.IP-7: Protection processes are improved	NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-8, PL-2, PM-6	CA-7
PR.IP-8: Effectiveness of protection technologies is shared	NIST SP 800-53 Rev. 4 AC-21, CA-7, SI-4	SI-4, CA-7
PR.IP-12: A vulnerability management plan is developed and implemented	NIST SP 800-53 Rev. 4 RA-3, RA-5, SI-2	RA-3, RA-5
PR.PT-4: Communications and control networks are protected	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	SC-19, SC-38, AC-17, SC-36
DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4	SI-4
DE.AE-2: Detected events are analyzed to understand attack targets and methods	NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, SI-4	SI-4, CA-7, IR-4
DE.AE-3: Event data are collected and correlated from multiple sources and sensors	NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, IR-8, SI-4	SI-4, CA-7, IR-4
DE.AE-4: Impact of events is determined	NIST SP 800-53 Rev. 4 CP-2, IR-4, RA-3, SI-4	RA-3, SI-4, IR-4
DE.AE-5: Incident alert thresholds are established	NIST SP 800-53 Rev. 4 IR-4, IR-5, IR-8	IR-4
DE.CM-1: The network is monitored to detect potential cybersecurity events	NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4	SI-4, CA-7
DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	NIST SP 800-53 Rev. 4 AC-2, AU-12, AU-13, CA-7, CM-10, CM-11	AU-13, CA-7
DE.CM-4: Malicious code is detected	NIST SP 800-53 Rev. 4 SI-3, SI-8	SI-3
DE.CM-5: Unauthorized mobile code is detected	NIST SP 800-53 Rev. 4 SC-18, SI-4, SC-44	SC-44, SI-4
DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	NIST SP 800-53 Rev. 4 CA-7, PS-7, SA-4, SA-9, SI-4	SI-4, CA-7
DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	NIST SP 800-53 Rev. 4 AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4	CM-8, SI-4, CA-7
DE.CM-8: Vulnerability scans are performed	NIST SP 800-53 Rev. 4 RA-5	RA-5
DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability	NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14	CA-2, CA-7
DE.DP-2: Detection activities comply with all applicable requirements	NIST SP 800-53 Rev. 4 AC-25, CA-2, CA-7, SA-18, SI-4, PM-14	SI-4, CA-2, CA-7
DE.DP-3: Detection processes are tested	NIST SP 800-53 Rev. 4 CA-2, CA-7, PE-3, SI-3, SI-4, PM-14	SI-4, CA-2, CA-7, SI-3

Subcategory	Informative References	Attivo Solution
DE.DP-4: Event detection information is communicated	NIST SP 800-53 Rev. 4 AU-6, CA-2, CA-7, RA-5, SI-4	RA-5, SI-4, CA-2, CA-7
DE.DP-5: Detection processes are continuously improved	NIST SP 800-53 Rev. 4, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14	RA-4, SI-4, CA-2, CA-7
RS.RP-1: Response plan is executed during or after an incident	NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR-8	IR-4
RS.CO-3: Information is shared consistent with response plans	NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4	RA-5, SI-4, CA-2, CA-7, IR-4
RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	NIST SP 800-53 Rev. 4 SI-5, PM-15	SI-5
RS.AN-1: Notifications from detection systems are investigated	NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, PE-6, SI-4	SI-4, CA-7, IR-4
RS.AN-3: Forensics are performed	NIST SP 800-53 Rev. 4 AU-7, IR-4	IR-4
RS.AN-4: Incidents are categorized consistent with response plans	NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-5, IR-8	IR-4
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)	NIST SP 800-53 Rev. 4 SI-5, PM-15	SI-5
RS.MI-1: Incidents are contained	NIST SP 800-53 Rev. 4 IR-4	IR-4
RS.MI-2: Incidents are mitigated	NIST SP 800-53 Rev. 4 IR-4	IR-4
RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	NIST SP 800-53 Rev. 4 CA-7, RA-3, RA-5	RA-3, RA-5

CONCLUSION

Deception and concealment technologies are powerful defense mechanisms that bridge gaps attackers can exploit when they successfully penetrate a perimeter defense. By adding the Attivo Networks ThreatDefend Platform to the security stack, organizations gain early and accurate visibility, detection, and prevention of attacks that evade existing controls while gaining capabilities that help them meet the guidance set forth by the NIST Cybersecurity Framework.

ABOUT ATTIVO NETWORKS®

Attivo Networks®, the leader in identity detection and response, delivers a superior defense for preventing privilege escalation and lateral movement threat activity. Customers worldwide rely on the ThreatDefend® Platform for unprecedented visibility to risks, attack surface reduction, and attack detection. The portfolio provides patented innovative defenses at critical points of attack, including at endpoints, in Active Directory, and cloud environments. Attivo has 150+ awards for technology innovation and leadership. www.attivonetworks.com