WHITEPAPER

Attivo NETWORKS®

ATTIVO NETWORKS® THREATDEFEND™ PLATFORM AND 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 of 2018, this voluntary framework consists of standards, guidelines, and best practices to help organizations manage cybersecurity risks. While originally 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 located at https://www.nist.gov/cyberframework.

THE FRAMEWORK

The framework is divided 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 are subdivided 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
- IR.RA - Risk Assessment
- IR.RM - Risk Management Strategy
- ID.SC - Supply Chain Risk Management

PROTECT - Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.

- PR.AC - Access Control
- PR.AT - Awareness and Training
- PR.DS - Data Security
- PR.IP - Information Protection Processes and Procedures
- PR.MA - Maintenance
- 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 plans for resilience and to restore any capabilities or services that were 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™ Deception and Response Platform provides extensive support to meet the guidance set forth by the NIST Cybersecurity Framework. It is comprised of the Attivo BOTsink® Deception server, ThreatStrike™ Endpoint Deception Suite, ThreatPath™ Visibility solution, DecoyDocs for Data Loss Tracking, and ThreatOps™ Incident Response Playbooks. With the most comprehensive deception solution covering the widest attack surfaces, the ThreatDefend Platform efficiently and accurately detects attackers already inside the network, early in the attack cycle through network, endpoint, application, and data decoys. These deceptions are projected to user networks, datacenters, and specialized networks such as ICS-SCADA, IoT, or POS whether on premises, in the cloud, or at remote or branch offices.

The platform automatically learns the environment and crafts mirror-match decoys for the highest authenticity. The Attivo Networks solution is easy to deploy and operate, requiring little effort to manage, while providing unparalleled visibility to credential-based attacks, Man-in-the-Middle activity, Active Directory attacks, reconnaissance, and attacker lateral movement. It can detect known and unknown attacks with engagement-based, forensic-backed alerts that reduce mean-time-to-detect with high fidelity and accuracy. The platform's numerous third-party integrations reduce mean-time-to-respond, accelerating the incident response process while providing offense-based intelligence for a proactive defense.

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.

CONTROL	TITLE	PRODUCT	FUNCTION
AU-13	MONITORING FOR INFORMATION DISCLOSURE	DecoyDocs	Determines if a decoy document was stolen and the geolocation of the systems that opened it.
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.
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	ThreatPath	Identifies stored credential vulnerabilities and misconfigurations that allow an attacker to move laterally within the network.
RA-4	RISK ASSESSMENT UPDATE	ThreatPath	Identifies stored credential vulnerabilities and misconfigurations that allow an attacker to move laterally within the network.
RA-5	VULNERABILITY SCANNING	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 fileshare decoys	BOTsink fileshare decoys and DecoyDocs alert on unauthorized access.
SC-38	OPERATIONS SECURITY	ThreatDefend Platform	ThreatPath identifies vulnerabilities, the ThreatDefend Platform provides the countermeasures to protect the network.
SC-44	DETONATION CHAMBERS	BOTsink Malware Analysis Sandbox	Built-in malware analysis sandbox functions.
SI-4	INFORMATION SYSTEM MONITORING	ThreatDefend Platform	The platform detects reconnaissance, lateral movement, MITM, and AD attacks.
SI-5	SECURITY ALERTS, ADVISORIES, AND DIRECTIVES	ThreatDefend Platform	The platform generates alerts and threat intelligence.

From these reference controls, the ThreatDefend Platform meets the following 32 Framework subcategories.

SUBCATEGORY	INFORMATIVE REFERENCES	ATTIVO DECEPTION
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
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.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
PR.IP-8: Effectiveness of protection technologies is shared	NIST SP 800-53 Rev. 4 AC-21, CA-7, SI-4	SI-4
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
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

SUBCATEGORY	INFORMATIVE REFERENCES	ATTIVO DECEPTION
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
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
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
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
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
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
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
DE.CM-8: Vulnerability scans are performed	NIST SP 800-53 Rev. 4 RA-5	RA-5
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
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
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
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
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
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

SUBCATEGORY	INFORMATIVE REFERENCES	ATTIVO DECEPTION
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-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

Deception Technology is a powerful threat detection mechanism that bridges gaps left open and exploitable by attackers when adversaries successfully penetrate a perimeter defense. By adding the Attivo Networks® ThreatDefend™ Platform to the security stack, organizations gain early and accurate eyes-inside-the-network visibility to attacks that either bypass existing controls or are perpetrated by malicious actors already inside the network, while gaining capabilities that help them meet the guidance set forth by the NIST Cybersecurity Framework.

ABOUT ATTIVO NETWORKS

Attivo Networks® provides real-time detection and analysis of inside-the-network threats. The Attivo ThreatDefend™ Deception and Response Platform detects stolen credentials, ransomware, and targeted attacks within user networks, data centers, clouds, SCADA, IoT, and other specialized attack surfaces by deceiving an attacker into revealing themselves. Comprehensive attack analysis and forensics provide actionable alerts, and native integrations automate the blocking, quarantine, and threat hunting of attacks for accelerated incident response. The company has won over 50 awards for its technology innovation and leadership.

For more information, visit www.attivonetworks.com.