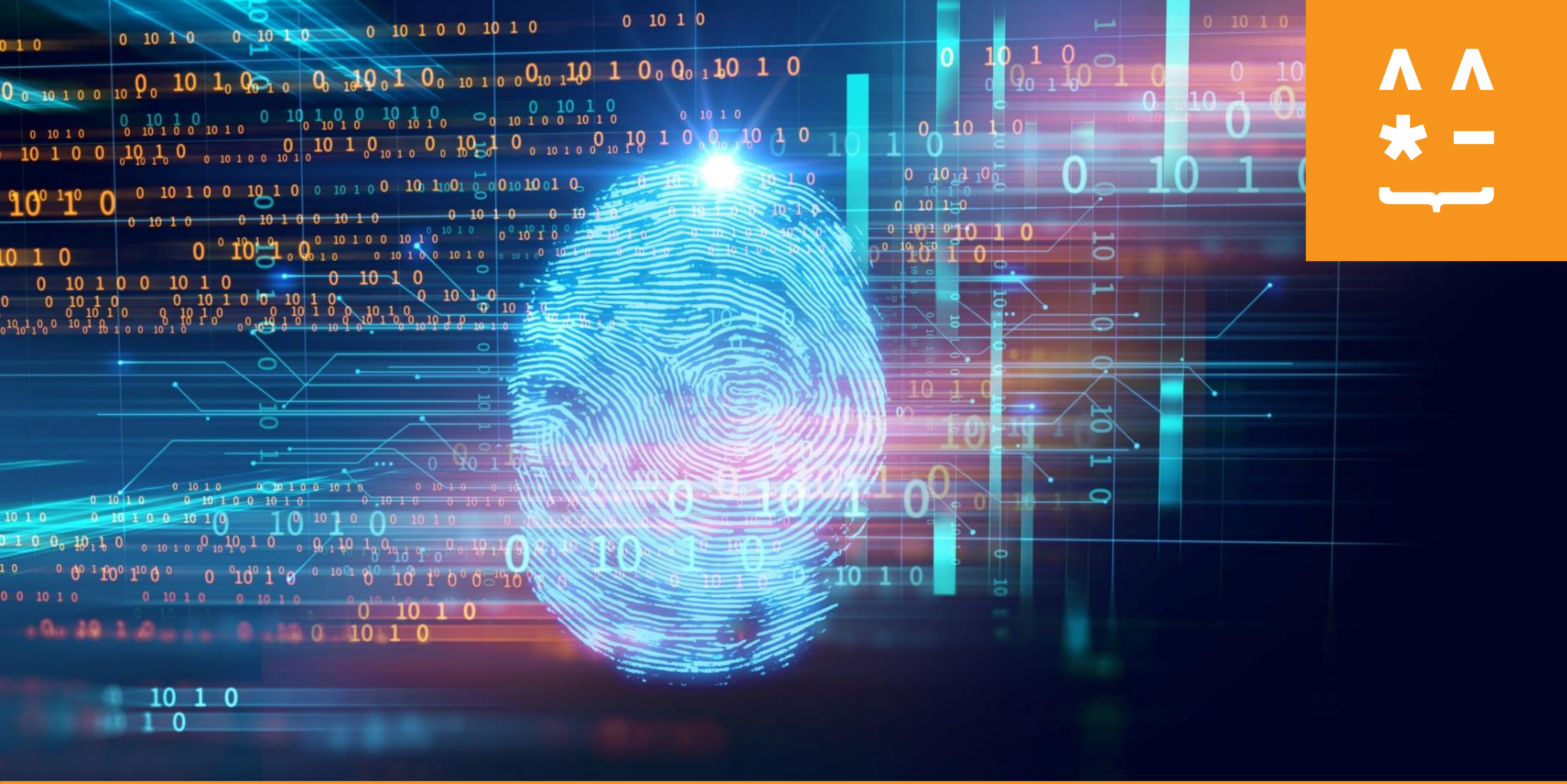


Illusive Networks

WHITE PAPER

May 2020

Achieving Cyber Resilience for CMMC Level 5 Compliance

Achieving Cyber Resilience for CMMC Level 5 Compliance

Recent attacks on defense contractors have degraded the federal government's supply chains. For example, a ransomware attack against Visser Precision, a parts manufacturer for defense contractors, led to missile antenna schematics and many other sensitive documents being posted online. A similar attack against Communications and Power Industries, an electronics manufacturer and defense contractor, caused nearly every computer in the company to be compromised.

To better protect supply chains, the federal government is encouraging many agencies and contractors to have cyber resiliency. NIST Special Publication (SP) 800-160 Volume 2 (v2) defines cyber resiliency as "the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources." The Department of Homeland Security (DHS) recently required that all federal agencies implement aspects of the NIST guidelines in support of the Continuous Diagnostics and Mitigation (CDM) and Trusted Internet Connections (TIC) programs. DHS has also released the High Value Asset Control Overlay, which specifies how federal agencies must protect their high-value assets, as defined in OMB Memorandum M-17-09.

Cyber resiliency is particularly important when advanced persistent threats (APTs) are targeting an environment. APTs typically enter an environment through an asset that is relatively easy to compromise, such as in a social engineering attack on an inattentive user to gain access to their laptop. Then the attacker stealthily moves through the environment, from asset to asset, until they gain unauthorized access to a high-value asset. While intrusion detection systems and other traditional detection approaches monitor environments for things that look strange, their lack of sensitivity sometimes leads to high false positive rates, and struggles identifying stealthier APTs. Without cyber resilience, it is more difficult to find a new or previously unseen APTs within all the noise.

In addition to NIST and DHS's recommendations for federal agency cyber resiliency, DoD released the first version of its Cybersecurity Maturity Model Certification (CMMC) model in January 2020. Defense contractors will be required to comply with CMMC in order to be eligible for future DoD acquisitions, with each acquisition requiring a certain minimum CMMC level. In the CMMC model, the two highest levels both address APTs, with Level 5 requiring more robust protection than Level 4. Only defense contractors that can meet CMMC Level 5 requirements will be able to bid on the widest range of DoD contracts, especially those that require handling the most sensitive data.

Cyber Resiliency Techniques for CMMC Level 5

Achieving CMMC Level 5 requires using several cyber resiliency techniques that work together. For thwarting APTs, four techniques are particularly important:

- Deception is deceiving attackers. Using deception makes it harder for attackers to find their targets, which wastes attacker resources and slows down attacks. SP 800-160v2 defines four approaches for deception:
    - » Obfuscation is concealing information from attackers. Encrypting data is a basic obfuscation method, as is hiding a file. A more sophisticated obfuscation is immersing real information within real-looking but bogus information so that attackers can't differentiate them.
    - » Disinformation is giving attackers bad information in the hopes that attackers will act on it and thus be exposed as malicious. For example, a fake password could be placed on a host to appear as a cached credential.
    - » Misdirection is guiding attackers to false resources. A simple type of misdirection is the use of a honeypot, which is primarily intended for studying attacker behavior, not stopping APTs. A more sophisticated form of misdirection is saturating an environment with false resources.
    - » Tainting is planting false resources rigged with hidden abilities or characteristics. An example is setting up a beacon within a particular file so when an attacker opens or copies that file, the beacon triggers an alert.
- Unpredictability is changing resources in ways attackers cannot anticipate, such as randomly changing when a daily activity starts or which server a host connects to for a service. Attackers who can predict what will occur, and how and when it will occur, can take advantage of that information when planning their attacks.
- Analytic monitoring is looking for signs of attacks and understanding their significance. There are many forms of analytic monitoring, including the use of vulnerability scanners, intrusion detection systems, and forensic tools.
- Privilege restriction is enforcing access control policies. A basic method is the use of operating system access control features. More complex methods involve changing privileges on the fly, such as lowering the privileges of an account that is deemed to be high risk in the current context.

NIST SP 800-160v2 contains over 10 pages of information on cyber resiliency techniques, including definitions of over a dozen techniques and possible approaches for implementing each of those techniques. The techniques mentioned in this paper are based on the concepts defined in SP 800-160v2.

Cyber resiliency techniques used together can be highly effective at finding and stopping APTs. APTs will always find a way to enter an environment, so the goal with cyber resiliency is to locate the APTs and remove or divert them before they reach the high-value assets they target. That means slowing attackers down and making them easier to find. This is where the Illusive Networks platform shines. Let's take a closer look at how Illusive can help your company achieve cyber resiliency and CMMC Level 5 compliance.

Preempting APTs

Preempting APTs—preventing them from being able to move through an environment—is a critical part of cyber resiliency. Illusive Networks' Attack Surface Manager (ASM) gives defenders the perspective attackers have once they establish a beachhead, showing how assets can be connected to each other through protocols like SSH, RDP, FTP, and HTTPS, as well as cached credentials and credentials held in memory. ASM runs agentless binaries on each asset which look for credentials, exploitable services, and other ways attackers could use to jump from one asset to another. This exploitability analysis identifies pathways from asset to asset that are often unknown to or overlooked by defenders.

By exposing the hidden pathways within an environment, ASM shows how an attacker could reach any asset from another. This is incredibly useful for preempting APTs because it shows paths to each high-value asset from low-value ones. ASM performs critical asset identification as part of its processes, with human input, to flag those assets that have particularly valuable data or resources, as well as assets with a large number of users (which typically have numerous associated administrative credentials). ASM considers these assets the "crown jewels" that APTs are most likely to pursue as their ultimate targets. These are exactly the types of high-value assets that CMMC is striving to ensure contractors safeguard.

After identifying the crown jewels and analyzing the pathways towards them, ASM's binaries then remediate the environment's attack surface by cleaning up assets to remove unneeded pathways, and by frequently re-checking the assets and automating their cleanup again going forward. Minimizing the number of pathways through this cyber hygiene process is a form of privileged access limitation that greatly reduces attackers' options for moving through an environment.

Detecting and Responding to APTs

Preempting APTs will slow them down but not stop them. They still need to be detected and appropriate response actions initiated. Illusive Networks' Attack Detection System (ADS) and Attack Intelligence System (AIS) support cyber resilience by executing the deception, unpredictability, and analytic monitoring techniques together.

Once the unneeded attack pathways are gone, ADS creates distributed deceptions—lots of them—that appear to establish new and enticing pathways towards crown jewels. False credentials, documents, devices, file shares, networks, emails, even browser histories, plus emulations of cameras, printers, switches, and other resources—there will be several times as many distributed deceptions as there are legitimate resources. All the deceptions are carefully crafted so they fit into the environment, like using hostnames consistent with real ones.

Detecting and Responding to APTs (cont'd)

When an attacker looks at this environment, most of what they see is deception, but of course they don't know that. The deceptions look authentic. Odds are high that if they try to connect to a host, or use an account, or access a file share, they will unknowingly be interacting with a deception. That will immediately trigger an incident and start the forensics process. Through analytic monitoring, ASM has already been collecting information on attacker behavior, and after the incident is triggered, AIS will generate a forensic timeline—a list of events with all the commands, domain name queries, network connections, and other important data for the offending asset shown in time order. This provides human analysts with the information they need to quickly assess what has happened and act to stop the APT early in the attack lifecycle.

Even if an attacker doesn't choose a deceptive host or account or file share for their first move, odds are higher that they'll engage with a deception the second time as they attempt to move closer to their ultimate target. Deceptions blanket the network to such a degree that the likelihood of an APT reaching a high-value asset through the pathways without being detected is nearly impossible, making the defender's environment incredibly hostile to attackers. Also, the odds of anyone with benign intentions trying to use any of the deceptions is extremely low, as they are hidden where only an attacker would be looking for them. This means the alerts Illusive's platform generates are high fidelity, and analysts can take each of them seriously with confidence.

Next Steps

By using ASM to clean up the real pathways, ADS to generate deceptive versions of pathways, and AIS to detect and analyze any attempted use of the deceptive pathways, an organization can trick attackers into revealing themselves, enabling APTs to be stopped and removed from the environment before they can do significant damage. This is a critical part of achieving the cyber resiliency needed for CMMC Level 5, the key to being able to bid on the widest range of DoD contracts.

Securing the DoD supply chain from malicious actors—most likely malicious insiders in the third-party relationship ecosystem—requires a lateral movement detection layer. By implementing deception for early detection, the CMMC Level 5 requirements for APT protection using deception are fully addressed. The deception-based detection approach creates the highest probability of positive early detection by making every endpoint a lateral movement sensor.

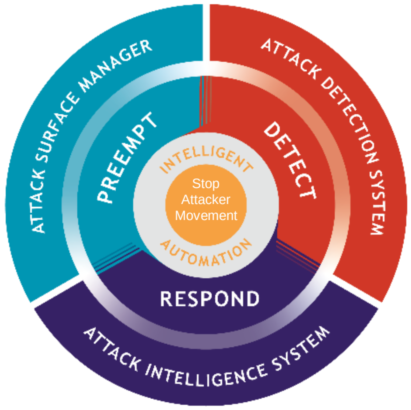
Illusive Networks at a Glance

Who We Are

Illusive Networks uses next-generation deception technology to stop cyber-attacks by detecting and disarming attackers, destroying their decision-making processes, and depriving them of the means to laterally move towards attack targets. Illusive's inescapable deceptions eliminate high-risk pathways to critical systems, force attackers to reveal themselves early in the threat lifecycle, and capture real-time forensics that accelerate incident response. Built on agentless automation and requiring very little security team support, Illusive immediately shifts the advantage to defenders, freeing precious resources from the complicated and data-heavy approaches that overload them today. For more information, visit www.illusivenetworks.com, or contact us at info@illusivenetworks.com.

The Illusive Platform

Illusive has beaten well over 100 of the world's most advanced and aggressive red teams. How? The Illusive Platform is engineered by people steeped in nation-state cyber intelligence and defense with tactical understanding of how attackers operate. Purpose-built to help you simply and easily identify real threats, Illusive's three core elements work in tandem to help you paralyze attackers and stop them in their tracks.



Sign up for a solution demo and see the full power of making your environment hostile to attackers with the Illusive Platform.

Attack Surface Manager

Perpetually Remove Attack Pathways

Attack Surface Manager preempts attacks by continuously identifying and removing errant credentials, connections, and pathways attackers leverage to move sideways on a network, as well as the data they use to fuel their attacks. A clean cyber environment denies attackers the keys they need to move forward.

Attack Detection System

Make Your Environment a Trap

Attack Detection System replaces the real data that was found and removed by Attack Surface Manager with deceptive data that authentically mimics the information attackers expect to see. Once Attack Detection System tricks attackers into engagement with deceptive data, they are forced to reveal their presence to defenders at the earliest point in the post-breach attack lifecycle.

Attack Intelligence System

Remediate with Real-Time Forensics

Attack Intelligence System springs into action when a deception is tripped to deliver rich, real-time source and target forensics that pinpoint the attacker's location and violation, providing the incident response team with a fully-formed incident notification that cuts research and investigation time by more than two-thirds.

Appendix: Mapping the Illusive Platform's Capabilities to DoD, NIST, and DHS Guidance

This appendix shows how the security capabilities provided by the Illusive Platform map to cyber resiliency guidance from DoD, NIST, and DHS. The common terminology used to express the capabilities is NIST SP 800-53 security controls.

First is a periodic table showing the CMMC/Cyber Resilience Overlay controls, which are based on the SP 800-53 controls listed in Appendix G of NIST SP 800-160v2. The 15 shaded cells are all supported by the Illusive Platform.

AC-4	**AU-6**				**SI-4**	**SI-20**
CA-7	CA-8	**IR-4**	**IR-5**	**SR-3**	IA-3	IA-10
CM-2	CM-7	CM-8	**RA-3**	**RA-5**	**RA-9**	**RA-10**
SC-26	**SC-28**	**SC-30**	SC-35	**SC-40**	SC-44	SA-15

Next is a table based on the Periodic Table of HVA Overlay Controls from the DHS High Value Asset Control Overlay. The Illusive Platform supports the 19 shaded cells.

PE-3												**CA-3**
AC-2	AC-3										**CA-5**	CA-6
AC-4	**AC-6**										**CA-7**	**CA-9**
AC-17	AC-20	**AU-2**	**AU-6**	**AU-9**	**AU-10**	AU-15	CM-5	CM-6	CM-8	PL-2	PL-8	PL-10
SC-3	**SC-5**	**SC-7**	SC-8	SC-18	SC-28	RA-1	IA-2	**IA-3**	**IA-5**	CP-8	CP-9	CP-10
PM-7	PM-9	PM-10	PM-12	**IR-4**	**IR-5**	**RA-5**	SA-4	**SA-9**	SA-11	S1-2	SI-3	**SI-4**

Finally, the table below lists all 61 critical controls and sub-controls required for protection against APTs that the Illusive ASM, ADS, and AIS support when working together. This combines what is required for CMMC and what is required for HVAs in a single list.

NIST SP 800-53 Control Mapping		Illusive Application Mapping
AC : Access Control		
AC-2(6)	ACCOUNT MANAGEMENT | DYNAMIC PRIVILEGE MANAGEMENT	ASM - Automated Remediation (Dynamic Reconfiguration) of Lateral Movement Errant Credentials and Connections
AC-2(7)(b)	ACCOUNT MANAGEMENT | PRIVILEGED USER ACCOUNTS | ROLE-BASED SCHEMES: Monitors privileged role assignments	ASM - Credential and Connection Exploitability Analysis
AC-2(7)(c)	ACCOUNT MANAGEMENT | PRIVILEGED USER ACCOUNTS | ROLE-BASED SCHEMES: Takes [Assignment: organization-defined actions] when privileged role assignments are no longer appropriate.	ASM - Privileged Access Exploitability Analysis and Remediation
AC-2(8)	ACCOUNT MANAGEMENT | DYNAMIC ACCOUNT MANAGEMENT	ASM - Automated Remediation (Dynamic Reconfiguration) of Lateral Movement Errant Credentials and Connections
AC-2(12)	ACCOUNT MANAGEMENT | ACCOUNT MONITORING FOR ATYPICAL USAGE	ASM - Credential and Connection Exploitability Analysis
AC-6	LEAST PRIVILEGE	ASM - Privileged Access Exploitability Analysis and Remediation
AC-6(1)	LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS	ASM - Privileged Access Exploitability Analysis and Remediation
AC-6(2)	LEAST PRIVILEGE | NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS	ASM - Privileged Access Exploitability Analysis and Remediation
AC-6(3)	LEAST PRIVILEGE | NETWORK ACCESS TO PRIVILEGED COMMANDS	ASM - Privileged Access Exploitability Analysis and Remediation
AC-6(5)	LEAST PRIVILEGE | PRIVILEGED ACCOUNTS	ASM - Privileged Access Exploitability Analysis and Remediation
AC-6(6)	LEAST PRIVILEGE | PRIVILEGED ACCESS BY NON-ORGANIZATIONAL USERS	ASM - Privileged Access Exploitability Analysis and Remediation
AC-6(7)	LEAST PRIVILEGE | REVIEW OF USER PRIVILEGES	ASM - Privileged Access Exploitability Analysis and Remediation
AC-6(8)	LEAST PRIVILEGE | PRIVILEGE LEVELS FOR CODE EXECUTION	ASM - Privileged Access Exploitability Analysis and Remediation
AC-6(10)	LEAST PRIVILEGE | PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS	ASM - Privileged Access Exploitability Analysis and Remediation

(cont'd)

NIST SP 800-53 Control Mapping		Illusive Application Mapping
AU : Audit and Accountability		
AU-2	EVENT LOGGING	ADS/AIS - Forensics Report Attributes
AU-6	AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING	ASM - Credential and Connection Exploitability Analysis, Crown Jewel Identification, Pathways Analysis
AU-6(3)	AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | CORRELATE AUDIT RECORD REPOSITORIES	ASM - Credential and Connection Exploitability Analysis
AU-6(5)	AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | INTEGRATED ANALYSIS OF AUDIT RECORDS	ASM - Credential and Connection Exploitability Analysis, Crown Jewel Identification, Pathways Analysis with Export/APIs
AU-6(6)	AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | CORRELATION WITH PHYSICAL MONITORING	ASM - Credential and Connection Exploitability Analysis
AU-6(8)	AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | FULL TEXT ANALYSIS OF PRIVILEGED COMMANDS	ASM - Credential and Connection Exploitability Analysis; AIS - Forensics On Demand
AU-9(2)	PROTECTION OF AUDIT INFORMATION | STORE ON SEPARATE PHYSICAL SYSTEMS OR COMPONENTS	ASM - Credential and Connection Exploitability Analysis; AIS - Forensics Data Collection
AU-9(4)	PROTECTION OF AUDIT INFORMATION | ACCESS BY SUBSET OF PRIVILEGED USERS	ASM - Credential and Connection Exploitability Analysis; AIS - Forensics Data Collection
AU-9(6)	PROTECTION OF AUDIT INFORMATION | READ-ONLY ACCESS	ASM - Credential and Connection Exploitability Analysis; AIS - Forensics Data Collection
AU-10	NON-REPUDIATION	ADS/AIS - Forensics Data Collection and Forensics Timeline
CA : Assessment, Authorization, and Monitoring		
CA-7(3)	CONTINUOUS MONITORING | TREND ANALYSES	ASM - Credential and Connection Exploitability Analysis
CA-7(5)	CONTINUOUS MONITORING | CONSISTENCY ANALYSIS	ASM - Credential and Connection Exploitability Analysis
CA-9	INTERNAL SYSTEM CONNECTIONS	ASM - Connection Exploitability Analysis, Crown Jewels and Pathways
IA: Identification and Authentication		
IA-5(13)	AUTHENTICATOR MANAGEMENT | EXPIRATION OF CACHED AUTHENTICATORS	ASM - Errant Cached Credential Clean Up Policy

(cont'd)

NIST SP 800-53 Control Mapping		Illusive Application Mapping
IR : Incident Response		
IR-4(1)	INCIDENT HANDLING | AUTOMATED INCIDENT HANDLING PROCESSES	ADS/AIS - Incident Alerts and Forensics
IR-4(6)	INCIDENT HANDLING | INSIDER THREATS - SPECIFIC CAPABILITIES	ADS/AIS - Incident Alerts and Forensics
IR-4(9)	INCIDENT HANDLING | DYNAMIC RESPONSE CAPABILITY	ADS/AIS - Incident Alert Handling/SIEM/SDL Integration and Forensics Reporting
IR-4(11)	INCIDENT HANDLING | INTEGRATED INCIDENT RESPONSE TEAM	ADS/AIS - Incident Alert Handling/SIEM/SDL Integration and Forensics Reporting
IR-4(12)	INCIDENT HANDLING | MALICIOUS CODE AND FORENSIC ANALYSIS	ASM - Suspicious Files; AIS - Incident Alert Integration and Forensics Reporting
IR-4(13)	INCIDENT HANDLING | BEHAVIOR ANALYSIS	ADS/AIS - Alert Integration and Forensics Reporting
IR-5	INCIDENT MONITORING	ADS/AIS - Forensics on Demand, Incident Alerts and Forensics
IR-5(1)	INCIDENT MONITORING | AUTOMATED TRACKING / DATA COLLECTION / ANALYSIS	ADS/AIS - Incident Alerts and Forensics
RA : Risk Assessment		
RA-3(3)	RISK ASSESSMENT | DYNAMIC THREAT AWARENESS	ASM - Credential and Connection Exploitability Analysis
RA-5(5)	VULNERABILITY MONITORING AND SCANNING | PRIVILEGED ACCESS	ASM - Credential and Connection Exploitability Analysis
RA-5(6)	VULNERABILITY MONITORING AND SCANNING | AUTOMATED TREND ANALYSES	ASM - Dashboard Trending of Credential and Connection Exploitability Analysis
RA-9	CRITICALITY ANALYSIS	ASM - Credential and Connection Exploitability Analysis, Pathways, Crown Jewels
RA-10	THREAT HUNTING	ADS - Deceptive Artifacts and Alerts

(cont’d)

NIST SP 800-53 Control Mapping		Illusive Application Mapping
SC : System and Communications Protection		
SC-5(1)	DENIAL OF SERVICE PROTECTION | RESTRICT ABILITY TO ATTACK OTHER SYSTEMS	ADS - Deception Based Detection; AIS - Incident Alerts and Forensics
SC-7(10)	BOUNDARY PROTECTION | PREVENT EXFILTRATION	ADS - Deception Based Detection; AIS - Incident Alerts and Forensics
SC-23(3)	SESSION AUTHENTICITY | UNIQUE SYSTEM-GENERATED SESSION IDENTIFIERS	ADS - Deceptive Connection Artifacts, Decoys and Emulations
SC-26	DECOYS	ADS - Decoys and Emulations
SC-30	CONCEALMENT AND MISDIRECTION	ADS - Deceptive Connection Artifacts, Decoys and Emulations
SC-30(2)	CONCEALMENT AND MISDIRECTION | RANDOMNESS	ADS - Deceptive Credentials and Connections
SC-30(3)	CONCEALMENT AND MISDIRECTION | CHANGE PROCESSING AND STORAGE LOCATIONS	ADS - Deceptive Connections, Shares and Beaconing Files
SC-30(4)	CONCEALMENT AND MISDIRECTION | MISLEADING INFORMATION	ADS - Deceptive Artifacts, Decoys and Emulations
SC-30(5)	CONCEALMENT AND MISDIRECTION | CONCEALMENT OF SYSTEM COMPONENTS	ADS - Deceptive Artifacts, Decoys and Emulations
SC-40(3)	WIRELESS LINK PROTECTION | IMITATIVE OR MANIPULATIVE COMMUNICATIONS DECEPTION	ADS - Deceptive Connections

(cont’d)

NIST SP 800-53 Control Mapping		Illusive Application Mapping
SI : System and Information Integrity		
SI-4(1)	SYSTEM MONITORING | SYSTEM-WIDE INTRUSION DETECTION SYSTEM	ADS - Deceptive Artifacts, Decoys and Emulations
SI-4(2)	SYSTEM MONITORING | AUTOMATED TOOLS AND MECHANISMS FOR REAL-TIME ANALYSIS	ADS - Deceptive Artifacts; AIS - Incident Alerts and Forensics
SI-4(3)	SYSTEM MONITORING | AUTOMATED TOOL AND MECHANISM INTEGRATION	ADS/AIS - Rest API Integration
SI-4(4)	SYSTEM MONITORING | INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC	ADS/AIS - Forensics on Demand
SI-4(7)	SYSTEM MONITORING | AUTOMATED RESPONSE TO SUSPICIOUS EVENTS	ADS/AIS - Decoy Artifacts and Alerts, REST API integration; Integration with SIEM/SOAR and Forensics on Demand
SI-4(11)	SYSTEM MONITORING | ANALYZE COMMUNICATIONS TRAFFIC ANOMALIES	ADS/AIS - Forensics on Demand
SI-4(17)	SYSTEM MONITORING | INTEGRATED SITUATIONAL AWARENESS	ADS/AIS - Forensics on Demand
SI-4(18)	SYSTEM MONITORING | ANALYZE TRAFFIC AND COVERT EXFILTRATION	ADS/AIS - Forensics on Demand
SI-4(24)	SYSTEM MONITORING | INDICATORS OF COMPROMISE	ADS/AIS - Deceptive Artifacts, Decoys and Emulations; Incident Alerts, Forensics and Integration with SIEM/SOAR
SI-20	TAINTING	ADS - Deceptive Artifacts

Illusive Networks stops attack movement from anywhere to anywhere by creating a hostile environment for attackers. Illusive shrinks the true attack surface to preempt attacks, creates the illusion of an expanded attack surface with deceptions for early detection of attacks in motion, and provides rich, real-time forensics that speeds response with actionable insights.

Agentless and intelligence-driven, Illusive deception technology enables organizations to avoid operational disruption and business losses by proactively intervening in the attack process so they can function with greater confidence in today’s complex, hyper-connected world.

Visit us: www.illusivenetworks.com

Email us: info@illusivenetworks.com

Call us:: US: +1 844.455.8748
EMEA / AsiaPac: +972 73.272.4006

Find us: