SOLUTIONARY®
AN NTT GROUP SECURITY COMPANY

White Paper

Defense Strategies for Advanced Threats:

Mapping the SANS 20 Critical Security Controls to the Cyber Kill Chain

https://www.solutionary.com

(866) 333-2133

Defense Strategies for Advanced Threats: Mapping the SANS 20 Critical Security Controls to the Cyber Kill Chain

Contents

Introduction

Whether the term used is “Advanced Persistent Threat (APT),” “advanced threat” or “state-sponsored threat actor,” cyberattacks are increasing in sophistication and the amount of damage they can inflict. These attacks, frequently affiliated with governments or organized crime, have the resources, expertise and time necessary to meet their objectives. The advanced threat landscape has continued to evolve since the first Solutionary white paper on the topic in 2012 [1].

An increasingly common perspective in the cybersecurity industry is that organizations should expect to be compromised in the future (if they have not already been compromised) because a well-funded, state-sponsored adversary is likely to find a weakness in a targeted environment and obtain access. This is sound advice, and all organizations must develop, implement and test incident response processes to prepare for inevitable security incidents.

If an organization experiences an intrusion, however, it does not necessarily mean that they will experience a substantial loss of sensitive data. A critical time period exists during an attack – the period of time after the attacker has established a presence in the targeted environment, but before the attacker has been able to identify, access and exfiltrate key data. If an intrusion is detected before critical data is exfiltrated, the impact can be minimized. Organizations must develop capabilities not only to prevent successful attacks, but also to detect attacks in progress.

In this paper, Solutionary presents one approach to develop these capabilities. This approach maps the defensive techniques presented in the SANS 20 Critical Security Controls[2] to the attack phases described in the Cyber Kill Chain[3] (kill chain). By ensuring that controls exist to detect each step of the kill chain, organizations provide themselves with the best opportunity to detect attacks.

This white paper doesn’t provide a plan to stop advanced threats – because *that simply isn’t possible*. However, as the kill chain concept demonstrates, gaining entry is only part of the attack cycle. If an organization is compromised but can detect the compromise before critical data is exfiltrated, the attack’s impact can be minimized. Organizations should create as many opportunities as possible to detect an attack, both before and after an attacker has gained access.

[1] https://www.solutionary.com/resource-center/white-papers/the-advanced-persistent-threat/

[2] http://www.sans.org/critical-security-controls/

[3] http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf The term Cyber Kill Chain is copyright © Lockheed Martin.

The Kill Chain

The concept of the kill chain as a defensive approach for security has gained significant popularity based on the 2011 Lockheed Martin paper by Hutchins, Cloppert, and Amin that provided a detailed overview of the concept. The kill chain identifies seven phases of an attacker's progress so that appropriate countermeasures can be taken against each step. The seven steps of the kill chain are:

1. **Reconnaissance** consists of research, identification and selection of targets. Reconnaissance can include a number of facets, such as crawling the Internet for email addresses, social relationships or information on specific technologies used by the targeted organization.

2. **Weaponization** typically consists of coupling a remote access Trojan with an exploit into a deliverable payload. Application data files that contain exploits (such as Adobe Portable Document Format [PDF] or Microsoft Office documents) often serve as the weaponized deliverable, which can be transmitted via spear phishing attacks.

3. **Delivery** of the weapon to the target environment commonly uses mechanisms such as email attachments and websites hosting malicious content.

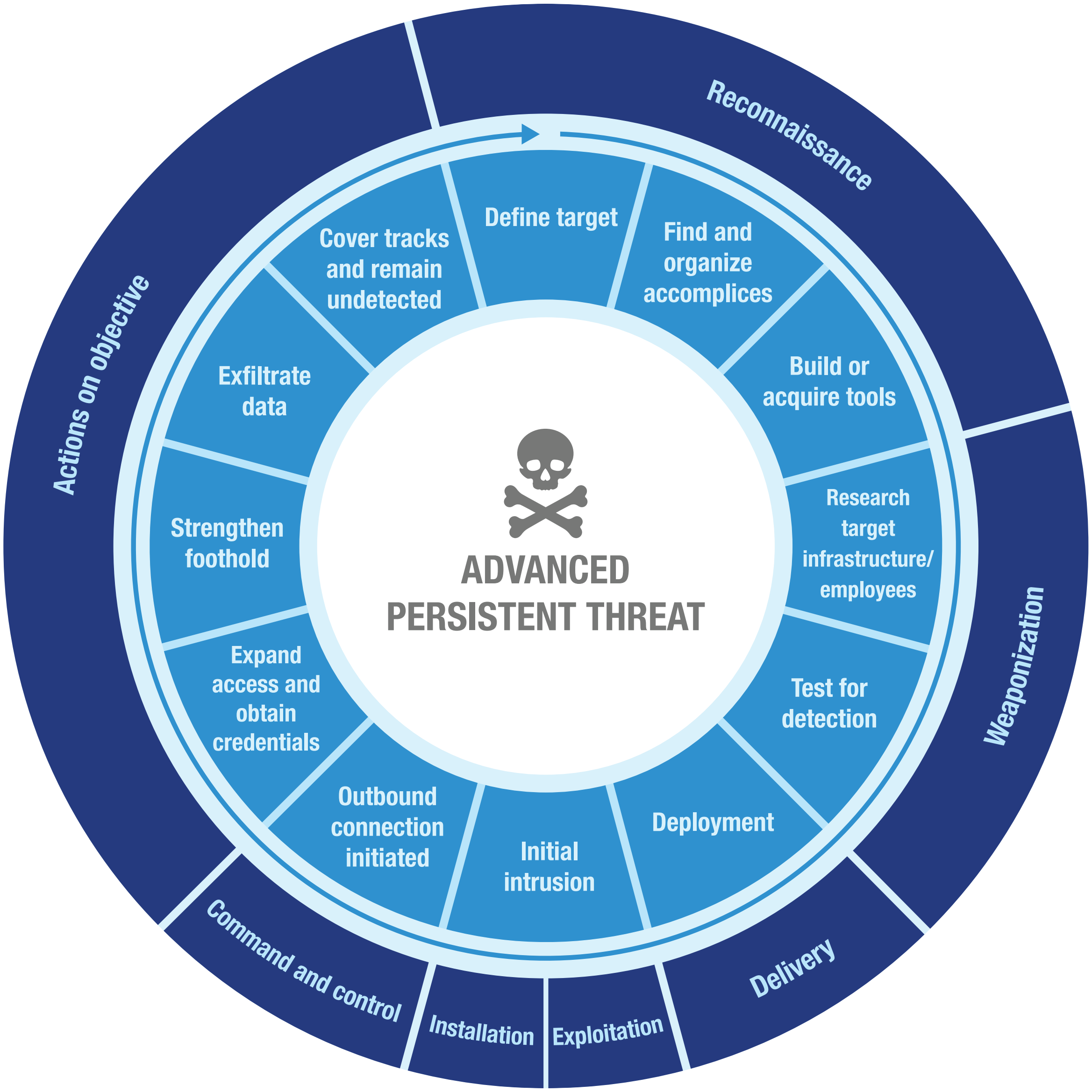
4. **Exploitation** triggers the intruder's maliciously-crafted code, which often targets a third-party application or operating system vulnerability.

5. **Installation** of a remote access Trojan or backdoor gives the attacker a foothold inside the environment.

6. **Command and Control/Exploration** – attacker-controlled hosts must connect outbound to an Internet-based control server to establish a Command and Control (C&C) communications channel. Advanced threats often require manual interaction after the initial compromise in order to explore and expand access and to identify internal targets of interest. This step includes performing internal reconnaissance, executing lateral movement to access additional systems and resources and creating additional access vectors to maintain persistence.

7. **Actions on Objectives** – after progressing through the first six phases, attackers begin taking action to achieve their original objectives. Typically, this objective is data exfiltration which involves collecting, encrypting and extracting information from the victim.

Just one successful mitigation step can disrupt the kill chain and stop the attack or significantly hinder a malicious actor's progress.



Why is the Kill Chain Important?

The kill chain provides a different way to think about attacks and how to defend against them. It considers an attack as a multi-step process instead of a single event. If organizations think about attacks as a process, they can implement controls which may detect, limit or stop the attack at each step in the process. One successful mitigation step can disrupt the kill chain and stop the attack or significantly hinder a malicious actor's progress.

In most advanced attacks, there is typically a period of time after an attacker gains access to a targeted environment and before sensitive data is actually accessed and exfiltrated. Very simply – once an attacker has gained access to an environment, they still need time to find what is most valuable, to familiarize themselves with the environment, expand and escalate their access and identify data to exfiltrate. This window between compromise and actual data loss has been termed “Exploration” by Steve Ocepek of SecureState[4] , (and as “Escalate Privileges”, “Internal Reconnaissance” and “Move Laterally” in the Mandiant Attack Lifecycle[5]) and is a critical timeframe because it provides an opportunity to respond to an intrusion before the worst-case scenario is realized. For the purposes of this paper, Exploration is considered part of the Command and Control step of the kill chain.

For the purposes of this paper, Exploration is considered part of the Command and Control step of the kill chain.

Although the 2013 Target Corporation breach was not a typical APT attack, it is instructive of the Exploration concept. The initial Target intrusion may not have been avoidable, but the disclosure of tens of millions of credit cards could have been avoided. After intruders established a presence in the network, Target missed numerous internal alerts that indicated malicious activity was occurring in the network. Effective response to these alerts could have reduced the impact of the breach.

The kill chain and Ocepek’s Exploration concept demonstrate that detecting malicious actors within an environment is as important as stopping those actors from gaining access in the first place. Organizations must place emphasis on detecting malicious actors already inside the environment as well as keeping attackers outside.

How can organizations develop a practical approach to this problem? Mapping the SANS Critical Security Controls to the steps of the kill chain, and ensuring that controls are in place for each step of the kill chain, is one approach.

Organizing SANS Critical Security Controls in Alignment with the Kill Chain

The SANS Critical Security Controls[6] is a commonly-accepted framework of 20 security controls where products, processes, architectures and services have demonstrated real-world effectiveness.

[4] http://blog.securestate.com/kill-chain/
[5] http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf
[6] http://www.sans.org/critical-security-controls

The following figure presents the Solutionary mapping of the 20 SANS Critical Security Controls to the attack kill chain phases. This mapping, and the detailed discussions that follow, can help organizations understand the controls that can provide protection against each stage of the kill chain and to identify areas of defensive strength, as well as areas where control gaps may exist.

THE ATTACKER KILL CHAIN AND SANS CRITICAL CONTROLS

Kill Chain Phase	SANS Critical Security Controls
Reconnaissance Research, identification and selection of targets.	**Understand How Your Organization Appears to Outsiders** • Inventory of Authorized and Unauthorized Devices (CSC 1) • Inventory of Authorized and Unauthorized Software (CSC 2) • Continuous Vulnerability Assessment and Remediation (SANS CSC 4) • Limitation and Control of Network Ports, Protocols, Services (SANS CSC 11) • Penetration Tests and Red Team Exercises (SANS CSC 20) • Beyond SANS: Targeted Threat Intelligence
Weaponization and Delivery Coupling a remote access trojan with an exploit into a deliverable payload and transmission to the client environment.	**Physical and Technical Controls to Detect Attacks** • Security Skills Assessment and Appropriate Training to Fill Gaps (SANS CSC 9) • Application Software Security (SANS CSC 6) • Boundary Defense (SANS CSC 13)
Exploitation and Installation After the weapon is delivered to victim host, exploitation triggers intruders' code that installs a remote access trojan or backdoor on the victim system to allow the attacker to maintain persistence inside the environment.	**Prevent, Detect and Respond to Malware** • Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations (SANS CSC 3) • Continuous Vulnerability Assessment and Remediation (SANS CSC 4) • Malware Defenses (SANS CSC 5)
Command and Control / Exploration Compromised hosts must connect outbound to Internet-based control servers to establish a Command and Control communications channel. Advanced threats require manual interaction after initial compromise in order to continue to explore and expand access in the environment, and to identify targets of interest.	**Detect Unauthorized Internal Activities** • Controlled Use of Administrative Privileges (SANS CSC 12) • Account Monitoring and Control (SANS CSC 16) • Maintenance, Monitoring, and Analysis of Audit Logs (SANS CSC 14) • Secure Network Engineering (SANS CSC 19) • Secure Configuration for Devices Like Firewalls, Routers, Switches (SANS CSC 10)

continued...

continued

THE ATTACKER KILL CHAIN AND SANS CRITICAL CONTROLS

Kill Chain Phase	SANS Critical Security Controls
Actions on Objectives Only after progressing through the first six phases, can intruders take actions to achieve their original objectives. Typically, this objective is data exfiltration which involves collecting, encrypting and extracting information from the victim environment.	**Detect Data Exfiltration** • Data Protection (SANS CSC 17) • Controlled Access Based on the Need to Know (SANS CSC 15) • Incident Response and Management (SANS CSC 18) • Beyond SANS: Detailed Outbound Traffic Analysis
SANS Critical Security Controls Not Directly Applicable • Wireless Access Control (SANS CSC 7) • Data Recovery Capability (SANS CSC 8)	

Control Strategies for Phases of the Kill Chain

This section presents an overview of each component of the kill chain. A list of recommended security controls, based on the SANS Critical Security Controls, is included for each step of the kill chain

Some controls may be relevant to more than one kill chain phase. Certain controls, such as Maintenance, Monitoring and Analysis of Audit Logs (SANS CSC #14) are relevant for every phase. This analysis describes each SANS control in the kill chain phases where the control can have the greatest impact.

Reconnaissance

In the Reconnaissance step of the kill chain, attackers gather information about the targeted organization. Reconnaissance can occur via Internet searches as well as low-level testing against the target infrastructure itself, via port scans or other testing.

Countermeasures for the Reconnaissance phase of attacks involve:

- Understanding what exists in the environment
- Limiting and testing what is exposed to the Internet
- Evaluating how the organization appears to outsiders

The SANS Critical Security Controls that can be used to protect against Reconnaissance activities are discussed below.

Inventory of Authorized and Unauthorized Devices (SANS CSC #1)

The first step in protecting an environment from advanced threats is understanding what needs to be protected. All organizations must have accurate inventories that identify their most critical assets to ensure that existing security programs (as well as future security investments) focus on the monitoring and protection of those assets.

The most critical aspect of this process is identification of systems that are of greatest value to the company, and that are most likely to be targeted by attackers. Security controls should emphasize the protection of these critical assets.

> The easiest way to reduce risk is to reduce the attack surface by periodically evaluating all services exposed to the Internet.

Inventory of Authorized and Unauthorized Software (SANS CSC #2)

Outdated or unauthorized software that is not properly maintained, or not appropriately decommissioned, can provide an entry point for attackers. Organizations must be aware of currently installed software, including software that is not formally approved. This list should include third-party add-ons that may not require administrator rights to install, such as Web browser plugins.

Limitation and Control of Network Ports, Protocols, and Services (SANS CSC #11)

The easiest way to reduce risk is to reduce the attack surface by periodically evaluating all services exposed to the Internet. Only devices and services with specific business justification should be accessible from the Internet.

Attack surface reviews should occur for the internal environment as well. Services permitted from Internet-facing DMZs to the internal network should be periodically reviewed, and services that traverse different network segments should be restricted. Effective access control can limit (and provide a mechanism for detecting) malicious access during the Exploration and Actions on Objectives phases of an attack.

Penetration Tests and Red Team Exercises (SANS CSC #20)

Penetration tests and red team exercises can be useful tools to understand how attackers would approach an environment in a real-world scenario. Penetration tests offer in-depth analysis, showing how individual vulnerabilities could be exploited or chained together to gain access.

Continuous Vulnerability Assessment and Remediation (SANS CSC #4)

While penetration tests and red team exercises provide periodic depth, vulnerability assessments and remediation provide continuous breadth. Regular assessments can identify vulnerabilities quickly and cost-effectively on an ongoing basis.

Weaponization and Delivery

In the Weaponization and Delivery phases, the attacker develops and delivers an exploit. While Weaponization and Delivery are two distinct phases in the formal kill chain process, Solutionary has combined them into one phase from a defense perspective, since the actions that can be taken against Weaponization are limited.

Countermeasures for the Weaponization and Delivery phases include technology to detect malicious software entering the environment and security awareness training for all employees, thereby enabling employees to detect malicious activity they may encounter.

The SANS Critical Security Controls that can be used to protect against kill chain Weaponization and Delivery activities are presented below.

Security Awareness Training (SANS CSC 9)

Many advanced attacks use social engineering to gain an initial foothold. Spear-phishing (phishing email targeting specific individuals) has been used as an initial attack vector in numerous publicized attacks. The common use of social engineering in advanced attacks highlights the importance of training critical employees, especially executives, financial personnel, research teams and other employees who have access to sensitive or confidential data. These groups must recognize potentially suspicious emails and social engineering attacks and be aware of proper incident response and notification procedures. Social networking sites are a growing source of personal information used by attackers to gather intelligence. It is important to have clear policies concerning access to these sites, as well as policies to remind employees about the type of information that is permissible to share on social media.

Beyond SANS – Targeted Threat Intelligence

A comprehensive perspective on how external attackers view an organization includes numerous components: the services and software that are exposed to the Internet, what people (employees and outsiders) are saying about the organization on social media and other online communication forums, as well as any potentially sensitive information that may be exposed online. A targeted threat intelligence service can assist in identification of developing threats.

Targeted threat intelligence services can also provide intelligence about threat actor groups, common reconnaissance and attack tactics, techniques and procedures (TTPs) used by the groups, and how these techniques could be utilized against the organization.

Application Software Security (SAN CSC #6)

Advanced attacks not involving social engineering often originate via Web application security vulnerabilities. Effective implementation of Web application security controls can protect against common attacks.

Organizations should adhere to secure programming and application deployment practices as defined by the Open Web Application Security Project (OWASP)[7] and ensure proper controls are implemented to validate and protect applications. Implementation of Web application firewalls (WAFs) has become an industry focus over the last several years, but this technology should not be considered a comprehensive solution. WAF capabilities must be reinforced with secure programming standards, static and dynamic source code review and application-specific security assessments.

Application security focuses not only on Web applications but also desktop applications. Initial network compromise is often achieved via exploitation of desktop application vulnerabilities. Desktop application patching and configuration management must be part of an overall security plan.

Boundary Defense (SANS CSC #13)

Detective measures must be in place for incoming and outgoing network traffic – intrusion detection systems for all TCP traffic, malware analysis for email and WAFs for Web applications. Beyond identification of known security alerts and signatures, network traffic analysis and protocol trending can detect deviations from established baselines which could indicate malicious activity.

Exploitation and Installation

In the Exploitation and Installation phases, the delivered attack is exploited and triggers the attacker’s code to install a remote access Trojan or backdoor, providing the attacker with access. While Exploitation and Installation are two distinct steps of the kill chain, they are combined here because of the close relationship between the two steps.

SANS Critical Security Controls that can protect against kill chain Exploitation and Installation activities are presented below.

[7] http://www.owasp.org

Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers (SANS CSC #3)

Assuming that malicious exploits will reach endpoint devices, the last measures of protection prior to Exploitation and Installation are the security controls on that endpoint. All end-user devices should implement hardening standards and be patched as efficiently as possible.

Continuous Vulnerability Assessment and Remediation (SANS CSC #4)

Continuous vulnerability assessment and remediation in the internal environment can be just as critical as in the external environment. Vulnerability remediation can make exploitation more difficult for an attacker.

Unfortunately, many organizations do not have a good plan for managing internal vulnerability assessments, nor do they use assessment data to become more resilient against attacks.

Unfortunately, many organizations do not have a good plan for managing internal vulnerability assessments, nor do they use assessment data to become more resilient against attacks. Vulnerability assessments should not just be a “punch list” of items to remediate, but should be viewed from a higher perspective to identify trends. These questions should be asked:

- Are most of these vulnerabilities related to patching?
- Are most of these vulnerabilities related to configuration issues?
- What is the root cause of these vulnerabilities?

Assessing the root cause can help organizations move from “fixing another round of vulnerabilities” to identifying the origins of problems and being able to prevent future occurrences.

Malware Defenses (SANS CSC #5)

Although advanced threats may not be detected by anti-virus (AV) software, AV can still be effective against less sophisticated attacks. Different AV products have different levels of effectiveness against various types of attacks. If possible, organizations should implement AV protection from multiple vendors. Layered defenses, such as desktop AV, Web and email gateway AV and protocol-aware proxies can reduce the likelihood of successful attacks.

Organizations should also invest in advanced detection engines that enable network-based threat detection. Many tools and products can provide a better view of what is occurring within the network. These products can also provide sandboxing capabilities, to capture and analyze malicious attack components safely.

Command and Control / Exploration

In the Command and Control (C&C) phase, a static presence has been established on the target network and communicates back to a Command and Control system so that a remote attacker can coordinate attacks manually.

This phase also represents a critical time frame in the attack as discussed in the introduction of this paper. This is the period of time after the attacker has established a presence in the environment, but before the attacker has been able to identify, access and exfiltrate key data. If a compromise is detected before critical data is exfiltrated, the attack's impact can be dramatically minimized.

It is critical to note that the controls in this phase should be focused on protecting high-value assets, as identified by SANS CSC #1 – Identification of Authorized and Unauthorized devices. Controlling access and use of administrative privileges is especially critical for high-value systems. Controls should also be implemented based on results of penetration tests or red team exercises targeted against critical data.

SANS Critical Security Controls that can be used to protect against kill chain Command and Control / Exploration activities are presented below.

Controlled Access Based on Need to Know (SANS CSC #15)

Limiting the users who can access particular pieces of data reduces the likelihood of an attacker accessing and exfiltrating that data. Segregation of duties can enforce this type of control and is extremely valuable for protecting organizational assets.

Data classification and handling guidelines can also identify sensitive data that should have limited access by employees, as well as data that may require additional security controls.

Controlled Use of Administrative Privileges (SANS CSC #12)

User accounts and permissions should be reviewed regularly to ensure that unnecessary or unused accounts are disabled or deleted, and that accounts have only the permissions required to fulfill their operational functions.

For applications performing highly-sensitive transactions (such as financial transfers), anomalous transactions should be identified and reviewed to ensure the activity is valid. User systems supporting mission-critical processes or transmitting mission-critical data should enforce stricter appropriate-use standards than typical user systems. For example, systems which perform financial transactions should be prohibited from general Internet browsing.

Critical systems should generate detailed security logs, which should be reviewed regularly to identify potential security events and anomalous activity.

Account Monitoring and Control (SANS CSC #16)

Advanced attacks often use compromised accounts to access sensitive data. Detailed auditing and monitoring of sensitive accounts can identify suspicious or unauthorized activity. Ensure that monitoring capabilities include information from internal DNS and directory services to identify user patterns and potentially malicious activity or unauthorized resource access requests.

Maintenance, Monitoring, and Analysis of Audit Logs (SANS CSC #14)

Critical systems should generate detailed security logs, which should be reviewed regularly to identify potential security events and anomalous activity. System security and applications logs can provide a wealth of information about network activity. The effectiveness of detective controls is dependent upon timely response to logs generated by the controls. Automated detection mechanisms can help detect potential malicious activity quickly.

Secure Network Engineering (SANS CSC #19)

Network isolation and segmentation of systems that directly access key assets can protect those assets from the general user population. As an example, customer service representative workstations that can access customer data should be on a separate network segment from the general user population.

Secure Configuration for Network Devices like Firewalls, Routers and Switches (SANS CSC #10)

Network devices should be deployed with secure builds in order to limit risks associated with attackers accessing the devices. Organizations must implement logical access controls and include network devices as a key part of their threat monitoring. Auditing and back-end authentication services (TACACS+, RADIUS, LDAP, etc.) are vital to ensuring that only authorized users can perform administrative tasks on these systems.

Controls that identify misuse and potential exfiltration of data are just as important as those that look for inbound malicious activity.

Actions on Objectives

In the Actions on Objectives phase, attackers attempt to locate, access and exfiltrate critical data.

SANS Critical Security Controls that can be used to protect against Actions on Objectives activities are presented below.

Data Protection (SANS CSC #17)

Data loss prevention (DLP) solutions can be implemented to monitor, detect and prevent the unauthorized use or transmission of critical data. Controls that identify misuse and potential exfiltration of data are just as important as those that look for inbound malicious activity.

Incident Response and Management (SANS CSC #18)

Organizations must implement an effective incident response program. This includes developing incident response policies, creating an incident response team and performing regular tests to ensure the team is effective in fulfilling its mission. It also includes regular training of technical personnel, mock exercises and testing using response scenarios, reviews and documentation/feedback of historical incidents.

It is critical to respond quickly and effectively to incidents, especially if an incident is being detected late in the kill chain process.

Conclusion

The kill chain, a phrase taken from military terminology, has been adapted by information security professionals to create a framework describing the stages of a cyberattack. It identifies a chain of events leading to a successful kill (exploit) of a target system.

In this paper, Solutionary has mapped the Cyber Kill Chain® (as defined by Lockheed Martin) to the SANS Critical Security Controls framework to gain a better understanding of how security controls can stop cyberattacks at various phases of an attack cycle. An attack can be detected and mitigated at various stages in the kill chain. The earlier this occurs, the better the outcome.

Beyond SANS - Detailed Outbound Traffic Analysis

Without exception, advanced attacks attempt to call back to their operators to receive instructions or to export critical data. Monitoring and analyzing outbound traffic to detect anomalous traffic patterns can alert an organization to potential command and control (C&C) and data exfiltration activity.

About Solutionary

Solutionary is the next generation managed security services provider (MSSP), focused on delivering managed security services, professional services and global threat intelligence. Comprehensive Solutionary security monitoring and security device management services protect traditional and virtual IT infrastructures, cloud environments and mobile data. Solutionary clients are able to optimize current security programs, make informed security decisions, achieve regulatory compliance and reduce costs. The patented, cloud-based ActiveGuard® service platform uses multiple detection technologies and advanced analytics to protect against advanced threats. The Solutionary Security Engineering Research Team (SERT) researches the global threat landscape, providing actionable threat intelligence, enhanced threat detection and mitigating controls. Experienced, certified Solutionary security experts act as an extension of clients' internal teams, providing industry-leading client service to global enterprise and mid-market clients in a wide range of industries, including financial services, healthcare, retail and government. Services are delivered 24/7 through multiple state-of-the-art Security Operations Centers (SOCs).

Solutionary Services include:

Managed Security Services

- Security Log Monitoring and Management
- Security Device Management
- Vulnerability Management

Professional Security Services

- Security Program Assessment
- Compromise Assessment
- CISO Advisory Services
- Targeted Threat Intelligence
- Incident Response
- Penetration Testing
- Social Engineering
- Governance, Risk and Compliance

Contact Solutionary at info@solutionary.com or 866-333-2133

Solutionary, an NTT Group security company, is the next generation managed security services provider (MSSP), focused on delivering managed security services and global threat intelligence.

SOLUTIONARY

https://www.solutionary.com

Solutionary, Inc.
9420 Underwood Avenue
Omaha, NE 68114