Advancing Zero Trust Maturity Throughout the Automation and Orchestration Pillar

Executive summary

The security of government and industry information and services is predicated on timely responsiveness to cybersecurity threats. Automation and orchestration can respond to threats much faster than manual methods alone, which may not be fast enough to prevent compromise or damage.

The automation and orchestration pillar is the set of Zero Trust capabilities that automates security actions and reactions based on defined processes and security policies across the enterprise, with a focus on speed and scale. Automation is the use of software to control repetitive tasks, and orchestration is the coordination of IT processes and workflows to ensure proper management of tasks. By implementing and maturing automation and orchestration capabilities, an organization can become much more resilient to ever increasing and increasingly sophisticated cyber intrusion attempts, even partially successful ones.

This pillar emphasizes dynamic security responses across the enterprise using policy orchestration to enforce policy decisions; critical process automation to improve efficiency; artificial intelligence / machine learning where applicable to further improve automation; security orchestration, automation, and response (SOAR) to weave together response actions; data exchange standardization to enable interoperability among capabilities; and security operations and incident response coordination, plans, and abilities. This cybersecurity information sheet (CSI) describes these automation and orchestration pillar capabilities and recommendations for reaching increasing maturity levels.

Introduction

Zero Trust (ZT) is an "evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources." [1] Unlike a traditional perimeter-based network security model, a ZT approach is primarily focused on data and services protection through the enforcement of dynamic trust policies between enterprise assets and subjects (end users, applications, and other non-human entities that request information from resources). To facilitate the development, deployment, and operations of the ZT framework and security model, Department of Defense (DoD) guidance organizes the capabilities of ZT into seven pillars that work together to provide a comprehensive and effective security model. Those pillars are User, Device, Network and Environment, Data, Application and Workload, Visibility and Analytics, and Automation and Orchestration. Automation and orchestration are the automated implementation and integration of the other pillars for dynamic, rapid, and scalable effects.

Automation is intended to reduce the burden on network defenders, but it is not without risk. In addition, adversarial tactics are increasingly being automated along with the use of artificial intelligence (AI), resulting in compromises occurring with increasing speed, frequency, and complexity. Automated systems are necessary to respond to these threats at the requisite tempo, but must also be designed with security in mind or systems will remain just as likely to become compromised as they were pre-automation. [2] While automation creates repeatable processes that make injected human error detectable, it also risks simply automating human error should foundational models not be designed carefully and tested continuously.

Cybersecurity incidents are on the rise due in part to automation of common techniques, such as phishing, which as of 2020 accounted for the origination of over 90% of reported breaches. [3] The ZT model mitigates this problem by limiting access to only what is needed and assuming that a breach is inevitable or has already occurred.

The recommendations provided in this cybersecurity information sheet (CSI) are focused on improving the ability of an organization to detect cyber threats and decrease response times to common threats. The recommendations also focus on automation of routine tasks, allowing resources to be focused on investigation of anomalies associated with advanced tactics, techniques, and procedures (TTPs). Through the automation and orchestration process, operations are defined through the development

of playbooks based on detection and effective responses, which coordinate and combine various security capabilities to secure data and resources.

A playbook for ZT is a structured set of predetermined actions designed to execute within an automated workflow, activated as needed to address and mitigate incidents. Additionally, playbooks automate security workflows so that analysts can spend more time performing analysis and investigation. The following cybersecurity practices are employed in ZT to assist in the automated efforts of security operations centers (SOC) by underpinning and enabling playbooks to act quickly and effectively against advanced and emerging threats: AI and machine learning (ML), security information and event management (SIEM), and user and entity behavior analysis (UEBA). [3] Additionally, security orchestration, automation, and response (SOAR) combines these tools to form a security layer against cybersecurity threats by providing continuous monitoring, real-time reactions to intrusions, and a baseline of expected behavior to raise alerts for unexpected behaviors.

This ZT CSI provides guidelines and best practices for maturing the capabilities of the ZT automation and orchestration pillar. Adoption of ZT is part of the National Cybersecurity Strategy to build a defensible, resilient digital ecosystem. [5]

Audience

This CSI provides guidance primarily intended for National Security System (NSS), DoD, and Defense Industrial Base (DIB) networks, but may also be useful for other owners and operators protecting their critical information and systems from sophisticated malicious actors. Guidance for other system owners and operators is also available via the National Institute of Standards and Technology (NIST), [1] and the Cybersecurity and Infrastructure Security Agency (CISA). [6] This guidance is aligned with DoD efforts and guidance to include the DoD's Cybersecurity Reference Architecture (CSRA) Version 5.0, [7] the DoD Zero Trust Reference Architecture (ZT RA), [8] and the DoD ZT Strategy. [9]

Background

The President's Executive Order on Improving the Nation's Cybersecurity (EO 14028) [10] and National Security Memorandum 8 (NSM-8) [12] direct the Federal Civilian

Executive Branch (FCEB) agencies and NSS owners and operators to develop and implement a ZT cybersecurity framework.

In the Embracing a Zero Trust Security Model CSI, the concept of ZT is defined and contextualized along with the undergirding principles of the seven pillars. The pillars are composed of capabilities that enable progressive maturity across a comprehensive ZT framework. [12] The capabilities described in this CSI are intended to continually mature cybersecurity protections, responses, and operations over time. Progression of capabilities in each of the seven pillars should be seen as a cycle of continuous improvement based on evaluation and monitoring of threats.

This CSI offers guidance in accordance with the DoD ZT RA maturity scale of preparation, baseline, intermediate, and advanced. It also complements the ZT Portfolio Management Office (PfMO) guidance for achieving "target" and “advanced” levels. [9]

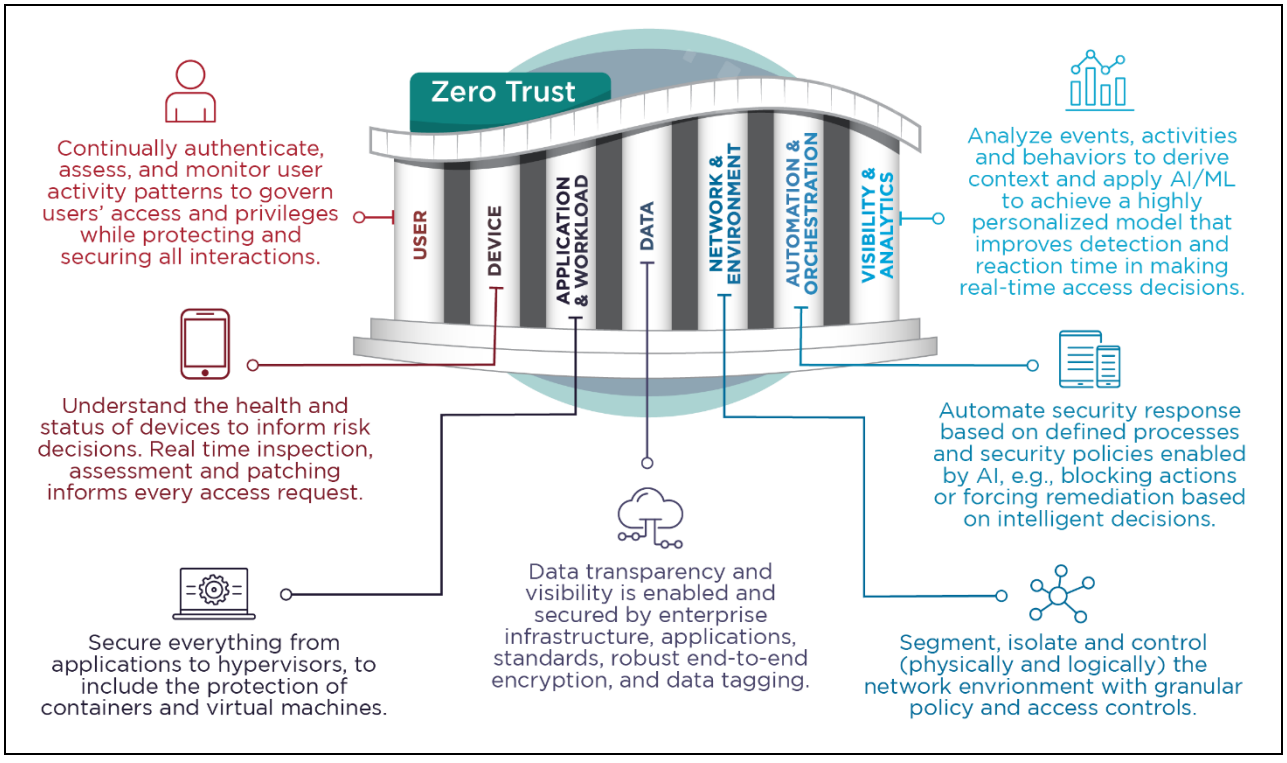

Figure 1: Description of the seven pillars of Zero Trust

Figure 1 displays the seven ZT pillars, including the automation and orchestration pillar. The capabilities and milestones for this pillar of the ZT maturity model will be described in detail throughout this document. The seven ZT pillars are not independent as each pillar depends on or aligns with the capabilities in the other pillars.

Automation and orchestration pillar

The automation and orchestration pillar in the ZT framework is designed to facilitate automating manual security and other applicable processes to take policy-based actions across the enterprise with speed and at scale. This pillar details the use of SOAR to improve security and decrease response times, and SIEM and other automated security tools to assist in managing disparate security systems. Processes must be defined and security policy enforcement consistent across all environments in a ZT enterprise for automated security to provide proactive command and control. [8]

The automation and orchestration pillar is composed of the following key capabilities:

- Policy orchestration using policy decision points
- Critical process automation
- Artificial intelligence
- Machine learning
- Security orchestration, automation, and response
- Data exchange standardization
- Security operations coordination and incident response

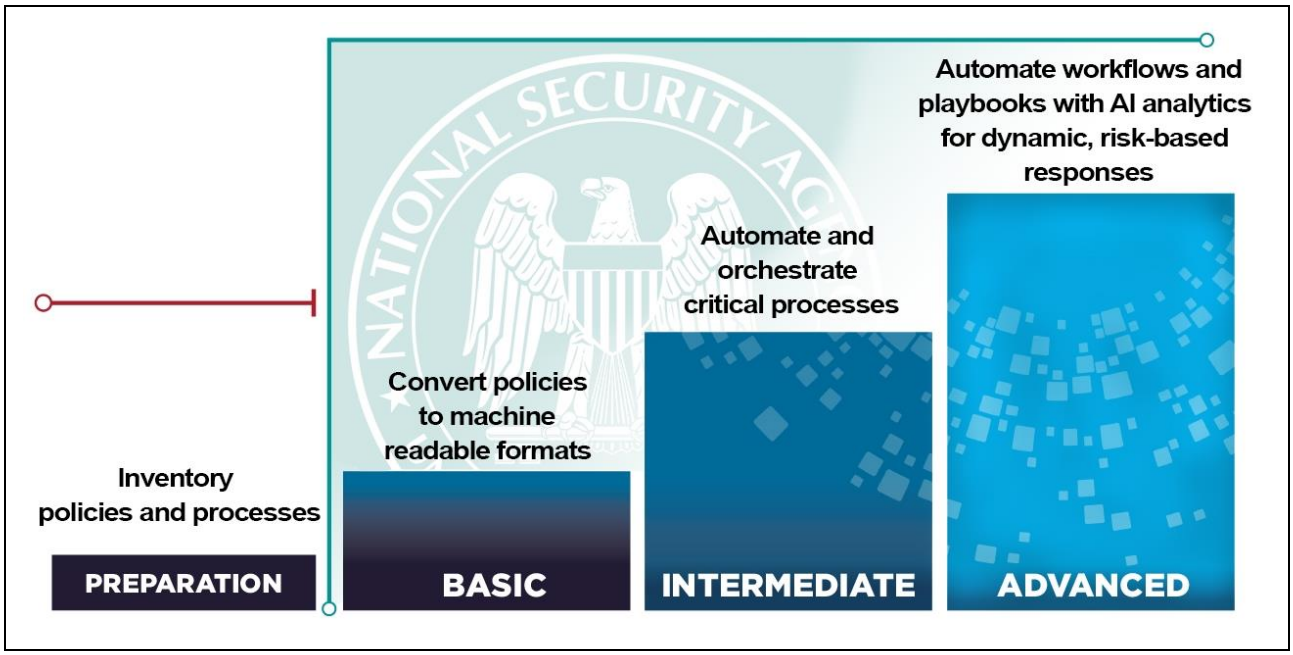

Figure 2: Zero Trust automation and orchestration pillar maturity

Policy orchestration using policy decision points

Security policies describe the ways that access decisions should be made to protect data and services. Policies and the contextual data that the policies rely on are stored in policy information points (PIPs), the policies and the contextual data are interpreted by policy decision points (PDPs) to decide whether to grant a particular access request, and those access decisions are implemented by policy enforcement point (PEPs). These are instantiated throughout the network architecture by a variety of security devices and capabilities, and are often best understood via network diagrams that depict data flows and all the security tools that implement data protections.

In traditional network environments, many security devices perform all three functions together, while in a modern ZT environment the functions are often decoupled, enabling more versatile security policies, enforcement, and response actions. For example, in a traditional network environment, a firewall may have a configuration specifying which ports and protocols to allow (i.e., the policy) and have the protocol metadata of network traffic that enters one of its network interfaces (i.e., policy-relevant information), may determine that the traffic should not be allowed (i.e., a policy decision), and then may block the traffic from traversing the device (i.e., policy enforcement).

Whereas, in an example modern ZT environment, a ZT-enabled network access capability would receive network traffic requesting access and send the access request along with network metadata to the access control engine (i.e., a PDP) to determine whether the access should be allowed. The access control engine would then request the relevant access policy (sometimes called a “conditional access policy”) from the central policy store (i.e., a PIP), request other relevant attributes and metadata (such as identity information, authentication validation, and environmental confidence levels) from other repositories (i.e., PIPs), evaluate the access policy using that contextual information to make an access decision (such as that the user associated with the network traffic is not allowed to access the requested resource), and then convey that decision back to the network access capability for enforcement (i.e., as a PEP to block the traffic). [7], [13]

Having policies in machine readable and enforceable formats enables the policies to be interpreted by PDPs and properly enforced by PEPs. It further can enable automated changes to the policies in response to changing conditions, allowing dynamic policies to

adapt to the current risk environment. Utilizing policy as code (PaC) techniques can help implement dynamic policies. [14]

Table 1: Policy orchestration using policy decision points maturity

Preparation	Basic	Intermediate	Advanced
Organizations use threat models, existing access requests (to applications and data), data flows, and related capabilities in other ZT pillars as guidance for potential policies and policy-relevant metadata that are needed.	Organizations establish a policy inventory and enterprise-wide access and security profiles. Organizations initially collect and document all existing rule-based policies to orchestrate across the security stack for effective automation.	Organizations establish PIPs and PDPs separate from PEPs to make data and service access determinations according to predefined policies that are then enforced by the PEPs, enabling incorporation of additional contextual information from PIPs. Access policies, where applicable, are converted into a standard form for use by a PDP.	PDPs, PIPs, and PEPs ensure proper implementation of dynamic fine-grained data access policies to users and non-person entities for all access requests to resources.

Critical process automation

Critical process automation (CPA) within a ZT framework involves automating an organization's critical processes while adhering to the central principle that no entity, whether inside or outside the network, should be trusted by default. This approach aims to continuously verify and validate trust for all users and devices accessing resources.

Robotic process automation (RPA) plays a role in CPA by automating repetitive tasks and workflows, allowing organizations to streamline processes and reduce human error. RPA bots can execute tasks such as user provisioning, access request approvals, and security policy enforcement, enhancing operational efficiency within a ZT environment. Furthermore, integrating AI and other advanced analytics can enhance an

organization's ZT posture by providing continuous risk assessment, behavioral analytics, predictive threat detection, and automated response.

Implementation of CPA and advanced analytics can offer significant benefits, but does not come without risk. An organization can become overly reliant on automation, leading to complacency and reduced human oversight. Additional risks can include false positives or negatives and training data biases.

To avoid some of the risks of AI, organizations should employ a few best practices. Start small and begin by automating low-risk, repetitive tasks to build a gradual confidence and understanding of how AI processes will develop over time. Maintain human oversight and involvement in processes to make final decisions and intervene when necessary. Finally, organizations should continuously monitor and evaluate automated processes to ensure continued accuracy and effectiveness.

Table 2: Critical process automation maturity

Preparation	Basic	Intermediate	Advanced
Organizations identify critical processes. Use mapping techniques to create diagrams of processes to better understand functionality for automation. Begin automating low-risk, repetitive tasks.	Integration and workflow provisioning is applied at small scales, targeting critical processes of most importance first with simple, well-defined automation rules.	Organizations expand automation by employing tools and methods such as robotic process automation (RPA), to address repetitive and predictable tasks across more critical functions. These can include data enrichment, security controls, and incident response (IR) workflows according to system security engineering principles. Existing processes are optimized, response times and accuracy are improved through advancement of rules and models.	Response time and capability is improved with orchestrated workflows and risk management processes. Automation nominates new processes and improvements to ensure continually more efficient outcomes.

Artificial intelligence

Artificial intelligence (AI) is concerned with building computers and machines "that can reason, learn, and act in such a way that would normally require human intelligence or that involves data whose scale exceeds what humans can analyze." [15] AI is the resultant conglomerate of multiple leveraged fields, including computer science, data analytics and statistics, hardware and software engineering, linguistics, neuroscience, and others. AI functions as a set of technologies based on machine learning, deep learning, robotics, expert systems, and algorithms. [16] As a broader concept, AI is about building machines that seem to perceive and reason like humans do.

AI can provide several benefits to ZT architectures. The ability for AI to analyze vast amounts of data and identify potential security threats more rapidly enables earlier threat detection and response, likely reducing the negative impacts of a breach and containing the damage. AI-powered systems can monitor user and device behavior continuously to establish baselines and detect deviations. Additionally, responses can be automated to speed up incident response times.

Consider the risks when implementing AI-powered services. Continuous human engagement and auditing is important to ensure that models behave as expected over time to reduce error and avoid complacency. Regular training is important, as are awareness programs for employees to educate themselves on the capabilities and limitations of AI within ZT architectures.

Table 3: Artificial intelligence maturity

Preparation	Basic	Intermediate	Advanced
Organizations define clear goals and use cases for AI implementation in their networks. Existing data for AI models is assessed for accuracy, completeness,	AI tools are obtained or developed based on predetermined use cases. AI models are tested and evaluated for performance and accuracy. AI tools are implemented in limited scopes to	Organizations implement AI/ML tools driven by analytics and recommend automation and orchestration modifications. AI tools are expanded across the network according to risk tolerances and AI risk principles.	Response times and capabilities are improved with AI orchestrated workflows and greater automation of risk management processes. Advanced AI models automate greater implementation of ZT capabilities

consistency, and relevance.	affect critical functions, such as risk assessment determinations and environment analysis, but in a way that AI errors would not negatively impact critical operations.		across ZT pillars, especially for prediction, anomaly detection, and recommending, or in some cases, orchestrating appropriate response actions.

Machine learning

Machine learning (ML) is a rapidly evolving branch of the AI field that focuses on the use of training data to develop statistical models that enable computers to make reliable predictions, decisions, and categorizations for new, previously unseen, data inputs.

Models can be trained through both supervised and unsupervised learning methods to process large datasets and arrive at meaningful conclusions much faster than would otherwise be possible with manual analysis. A supervised approach uses labeled data to help ML tools learn inputs and outputs, and identify known relationships and patterns. An unsupervised approach is used to discover hidden patterns or categorize patterns by having the ML tools explore unlabeled data sets. Within ZT, each method could be used to meet different security objectives or be combined in a semi-supervised learning model to leverage the benefits of each.

A ZT environment makes vigorous use of data tagging based on sensitivity and allowed access. Altogether, large quantities of data are produced from access logs, network traffic, user behavior, device attributes, security events, etc. This large volume of data can potentially train ML models with baselines of activity for users and system components. Data gathering is a foundational step in seeding the analytical information base used by statistical analyses to generate predictions and insights. [17]

When properly trained and implemented, ML solutions can be used to establish baselines and detect previously seen and potentially unforeseen anomalous activities. ML models, among other things, inform UEBA solutions in determining unusual user behavior, perform root cause analysis for faster investigative processes using large

language models (LLMs), and be integrated into network access controls and endpoint protection platform (EPP) solutions to mitigate known and possibly unforeseen threats.

Data gathering with ML modeling can be a powerful capability, but regular testing and human review should be conducted to improve model accuracy and validate suggested actions. AI and ML capabilities should also carefully adhere to any applicable legal, regulatory, privacy, or other requirements. [18], [19], [20]

Table 4: Machine learning maturity

Preparation	Basic	Intermediate	Advanced
Organizations identify data sources and ensure data tags are properly standardized for machine readability.	Organizations implement data tagging and classification ML tools. Organizations employ ML tools to execute and enhance execution of critical functions such as incident response, anomaly detection, user baselining, and data tagging. Organizations analyze models for biases and address them carefully as broader implementation is planned.	ML tools are expanded to operate across the entirety of the network. Model performance is evaluated as the dataset is increased to ensure accuracy, precision, and recall. Hyperparameter tuning is done to optimize model performance.	Models self-evaluate with new data to improve performance and address new or evolving threats.

Security orchestration, automation, and response

Security orchestration, automation, and response (SOAR) refers to technologies that enable organizations to collect and react to inputs monitored by the security operations team. SOAR can gather and enrich data, provide decision logic, and proceed through actions and tasks that support security policies. AI/ML augmentation could advance

autonomous adaptive cyber defense. This allows organizations to respond to cybersecurity compromise attempts and observe, understand, and prevent future incidents faster and at a larger scale to improve the organization's security posture.

A comprehensive SOAR product is designed to operate under three primary software capabilities: threat and vulnerability management, security IR, and security operations automation. Within the ZT framework, SOAR functionality facilitates automation and orchestration by ingesting alert data and triggering playbooks for automated response and remediation. SOAR can gather data, implement decision logic, and proceed through actions and tasks that support security policies. SOAR enables organizations to strengthen their cybersecurity defenses by focusing on incident detection and response, security team collaboration, and mitigation of security threats with speed and scale. [21]

Table 5: Security orchestration, automation, and response maturity

Preparation	Basic	Intermediate	Advanced
A logging and audit policy is developed to allow a SOAR to make decisions, and verify that the decisions and actions were taken. Organizations acquire SOAR tools to meet the needs of their use cases.	Policies and SOAR tools are implemented. Predefined playbooks from collection to IR and triage are utilized to enable initial process automation. Organizations achieve initial operating capability of security technologies to orchestrate and automate policies (e.g., through PEPs and PDPs) and rulesets to improve security operations.	SOAR tools are refined to improve security operations, threat and vulnerability management, and security responses using ingested alert data and threshold alerting which triggers playbooks for automated response and remediation. SOAR tools ingest data from UEBA solutions to create additional baselines and enhance threat hunting playbooks.	Process automations are tested and improved, and performance accelerated to suit the needs of the organization. Complex decision logic is implemented as appropriate for determining response actions. AI/ML are integrated into SOAR capabilities.

Data exchange standardization

Standardization of data formats, protocols, and application programming interfaces (APIs) can provide the ability for services and applications to communicate in the same manner, further enabling orchestration and enhancing interoperability. Organizations rely on services and applications that are composed of multiple elements that are often tightly integrated with each other. Standardized methods of exchanging data and triggering functionality help developers regulate information interchange patterns and avoid developing incompatible applications. Similarly, the growing reliance on cloud services for everything from security to networking infrastructure, has brought additional attention to the need for standards to enable interoperability.

However, achieving standardization and interoperability in practice can be challenging. Organizations should strive to have products that utilize the same standards and APIs in the same ways to orchestrate tasks across capabilities and products. Acquisition requirements may help, but some standards and APIs can be implemented in different ways that may affect actual interoperability.

Table 6: Data exchange standardization maturity

Preparation	Basic	Intermediate	Advanced
Organizations take inventory of processes, applications, workloads, and systems, especially the current and anticipated integration points, to better understand the landscape for standardization. Organizations research industry-adopted APIs	Organizations choose standards to use and create a comprehensive catalog and unified style guide for APIs. Noncompliant APIs, data formats, and protocols are altered or replaced per adopted standards. Product acquisitions include requirements to adhere to the chosen standards. Remaining APIs are standardized across	Documentation and style guides are enhanced. Feedback is solicited from developers on previous implementations and ways forward. Standardization practices are expanded across entire data landscape. Additional function testing is conducted to determine if	Organizations implement automated monitoring solutions to track performance, errors, and usage patterns, and to detect anomalies in API, protocols, and formats.

Preparation	Basic	Intermediate	Advanced
and other standards.	small projects or datasets first, checking for unintended conflicts.	products and services behave as expected using the APIs and other standards.	

Security operations coordination and incident response

Coordination of security operations and incident response are crucial for an organization's security operation. Their function is to detect, respond, and mitigate security risks, threats, and intrusions. Security operations centers (SOCs) provide security management visibility for status and tactical implementation. Workflows within the SOC are automated using automation tooling and enrichment provided jointly by service providers and technologies.

SOCs can improve response times though rapid analysis; automated collection of logs, PCAPs, and data; and automated responses to mitigate threats detected. The amount of data piping into a SOC is often far more than human analysts can process; therefore, a SOAR is needed to increase response time and coverage rate.

SOCs should also prepare for incident responses activities by developing incident response plans, testing them through table top exercises and actual simulations of potential scenarios, and updating the plans regularly. Having and following robust incident response plans can reduce the potential damage from intrusions and enable the continuity of mission.

Table 7: Security operations coordination and incident response maturity

Preparation	Basic	Intermediate	Advanced
Organizations determine a clear scope and objectives for a SOC and/or IR team. Initial incident response plan	If an organization SOC or computer network defense service provider SOC does not already exist, the organization defines and stands up a SOC to deploy,	IR plans are thoroughly developed, tested, and updated regularly. Identified data sources have fully	The SOAR solution provides advanced incident response workflow automation leveraging threat intelligence data, user activity monitoring (UAM), AI-based anomaly

(IRP) is developed. Applicable policies, data sources, and other requirements are identified. Solutions are procured to meet requirements.	operate, and maintain security monitoring. A SIEM solution begins integrating data sources (i.e., endpoint protection, detection, and response data) and initial monitoring and alerting begins. Playbook and workflow requirements are beginning development and integration for response activities.	integrated with the SIEM solution. A SOAR solution is integrated to provide basic playbook automation. Manual playbooks are identified for automation or decommission.	detection, and UEBA to determine potential issues. Automated responses (scripts and tools) leverage ML and AI. Playbooks are fully automated. Historical data is leveraged in decision making.

Summary of guidance

For ZT automation and orchestration, there are three key areas that span across the capabilities in this pillar. Organizations should employ automation methods to address repetitive, labor intensive, and predictable tasks for critical functions, such as data enrichment, security controls, and IR workflows according to system security engineering principles. Those tasks should be orchestrated across interoperable capabilities to make them even more efficient and reduce the manual burden on defenders.

Second, they should also employ advanced algorithms and analytics, especially AI/ML, to execute (and enhance execution of) critical functions, such as risk and access determinations, environmental analysis, IR, anomaly detection, user baselining, and data tagging.

Third, an organization's ability to coordinate security operations and incident response via a SOC is vital to its security and should be aided by AI/ML and other automation efforts to more quickly and effectively detect, respond to, and mitigate threats.

Further guidance

NSA is assisting NSS owners that are piloting ZT capabilities, coordinating ZT activities with NIST, CISA, the National Manager, and DoD, and developing additional ZT guidance to support system developers through the challenges of integrating ZT within NSS, DoD, and DIB environments. Upcoming additional guidance will help organize, guide, and simplify incorporating ZT principles and designs into enterprise networks.

Works cited

[1] National Institute of Standards and Technology. Special Publication 800-207: Zero Trust Architecture. 2020. https://csrc.nist.gov/publications/detail/sp/800-207/final

[2] A. Oseni. N. Moustafa, et al. Security and Privacy for Artificial Intelligence: Opportunities and Challenges. Journal of Association for Computing Machinery. 2021. https://arxiv.org/pdf/2102.04661

[3] Deloitte. 91% of All Cyber Attacks Begin with a Phishing Email to an Unexpected Victim. 2020. https://www2.deloitte.com/my/en/pages/risk/articles/91-percent-of-all-cyber-attacks-begin-with-a-phishing-email-to-an-unexpected-victim.html

[4] S. Aliello. Zero Trust: A Governance Perspective. 2022. http://dx.doi.org/10.2139/ssrn.4146521

[5] The White House. National Cybersecurity Strategy. 2023. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

[6] Cybersecurity and Infrastructure Security Agency. Zero Trust Maturity Model. 2023. https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf

[7] Department of Defense. DoD Cybersecurity Reference Architecture (CSRA) Version 5.0. 2023. https://dodcio.defense.gov/Portals/0/Documents/Library/CS-Ref-Architecture.pdf

[8] Department of Defense. Department of Defense (DoD) Zero Trust Reference Architecture v. 2.0. 2022. https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf

[9] Department of Defense. DoD Zero Trust Strategy. 2022. https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf

[10] The White House. Executive Order 14028: Improving the Nation's Cybersecurity. 2021. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[11] The White House. National Security Memorandum 8: Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems. 2022. https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/

[12] National Security Agency. Embracing a Zero Trust Security Model. 2021. https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF

[13] National Institute of Standards and Technology. Guide to Attribute Based Access Control (ABAC) Definition and Considerations. 2014. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-162.pdf

[14] National Security Agency. Enforce Secure Automated Deployment Practices through Infrastructure as Code. 2024. https://media.defense.gov/2024/Mar/07/2003407857/-1/-1/0/CSI-CloudTop10-Infrastructure-as-Code.PDF
[15] Google. What is Artificial Intelligence? n.d. https://cloud.google.com/learn/what-is-artificial-intelligence
[16] Google. Artificial Intelligence (AI) vs. Machine Learning (ML). n.d. https://cloud.google.com/learn/artificial-intelligence-vs-machine-learning
[17] IBM. What is machine learning? n.d. https://www.ibm.com/topics/machine-learning
[18] United Kingdom National Cyber Security Centre et al. Guidelines for secure AI system development. 2023. https://media.defense.gov/2023/Nov/27/2003346994/-1/-1/0/GUIDELINES-FOR-SECURE-AI-SYSTEM-DEVELOPMENT.PDF
[19] Australian Signals Directorate et al. Engaging with Artificial Intelligence (AI). 2024. https://media.defense.gov/2024/Jan/23/2003380135/-1/-1/0/CSI-ENGAGING-WITH-ARTIFICIAL-INTELLIGENCE.PDF
[20] National Security Agency et al. Deploying AI Systems Securely: Best Practices for Deploying Secure and Resilient AI Systems. 2024. https://media.defense.gov/2024/Apr/15/2003439257/-1/-1/0/CSI-DEPLOYING-AI-SYSTEMS-SECURELY.PDF
[21] Gartner. Security Orchestration, Automation and Response (SOAR). https://www.gartner.com/en/information-technology/glossary/security-orchestration-automation-response-soar

Disclaimer of endorsement

Purpose

This document was developed in furtherance of NSA's cybersecurity missions, including its responsibilities to identify and disseminate threats to National Security Systems, Department of Defense, and Defense Industrial Base information systems, and to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

Contact

Cybersecurity Report Feedback: CybersecurityReports@nsa.gov
General Cybersecurity Inquiries or Customer Requests: Cybersecurity_Requests@nsa.gov
Defense Industrial Base Inquiries and Cybersecurity Services: DIB_Defense@cyber.nsa.gov
Media Inquiries / Press Desk: NSA Media Relations: 443-634-0721, MediaRelations@nsa.gov