PLATINUM
BUSINESS SERVICES, LLC

The Security Operations Center and Incidence Response

Platinum Business Services, LLC

Jody Venkatesan, CISA, CISM, CGEIT, CRISC, CDPSE
President & CEO

Email: jvenkatesan@weareplatinum.net
Phone: 301-651-1297
Fax: 301-483-0104
Website: weareplatinum.net

SBA Certified 8(a) HUBZone, Service-Disabled Veteran Owned Small Business (SDVOSB), Veteran-Owned Small Business (VOSB), Small Business (SB), Small Disadvantaged Business (SDB)
TIN/EIN: 26-3462811
Cage Code: 59N47
DUNS: 828491410
UEI: PCNMDK3FLJB9
CIOSP3 NIH CIOSP3 SDVO
(Contract #HHSN316201800030W)
GSA MAS Professional Services #GS00F344CA
GSA MAS IT #GS-35F-0067Y
GSA 8(a) STARS 3 #47QTCB21D0108

Preventing Incidents and Responding When They Do Happen

Introduction

Cybersecurity incidents are inevitable. Even if a system is entirely cloistered, risks from human error and individuals with malicious intent must be addressed. Platinum's primary objective is to protect the integrity of data systems, both negligent oversights and malicious attacks, while being prepared to mitigate the impact of incidents when they do occur.

Two separate teams are entrusted with executing these protective actions and providing **Computer Network Defense (CND)**. While both teams have a common committed to maintaining the confidentiality, integrity, and availability of data within the network, they have distinctly different functions.

Prevention

The Security Operations Center (SOC) personnel are tasked with protecting the system against unauthorized access or use. They stand as the frontline of protection, using an array of tools to prevent unauthorized use, detect potential attacks, and provide immediate response when an incident does occur.

Platinum employs a diverse range of tools on a regular basis to furnish comprehensive system protection, including:

- **Security Information and Event Management (SIEM)** – to automate status monitoring and detection of any anomalous activity, a typical indicator of a security event (e.g., SolarWinds SEM, Exabeam Fusion, Fortinet FortiSIEM, Splunk Enterprise Security).
- **Network Monitoring Tool**s – to analyze network data to detect network-based threats such as denial of service attacks (e.g., Nagios, Pof, Splunk).
- **Encryption** – for both in-transit and at-rest encryption, per FIPS 140-2 standards.
- **System Vulnerability Scanning Tools** – to scan for typical system/network vulnerabilities, such as missing data encryption, OS command injection, SQL injection, buffer overflow, and missing authentication for critical functions (ACAS/Tenable Nessus).
- **Web Vulnerability Scanning Tools** – to scan websites for security vulnerabilities such as cross-site scripting, SQL injection, and path traversal (e.g., Burp Suite, SQL Map).
- **Penetration Testing** – to support Red Team (offensive attack simulation) and Blue Team (defensive response simulation) using tools such as Metasploit, Netsparker, and Wireshark.
- **Intrusion Detection Systems/Intrusion Prevention Systems (IDS/IPS)** – to detect network intrusions and initiate a pre-scripted response (e.g., blocking incoming traffic, quarantining a file, shutting down malicious code) to minimize the impact of the intrusion (e.g., Cisco, Fidelis, Palo Alto, SolarWinds).
- **Antivirus Software** – to scan incoming files to detect viruses and other harmful malware, including ransomware, worms, Trojans, spyware, and adware, using a database of malware signature codes. (e.g., Norton, McAfee).

Preventing Incidents and Responding When They Do Happen

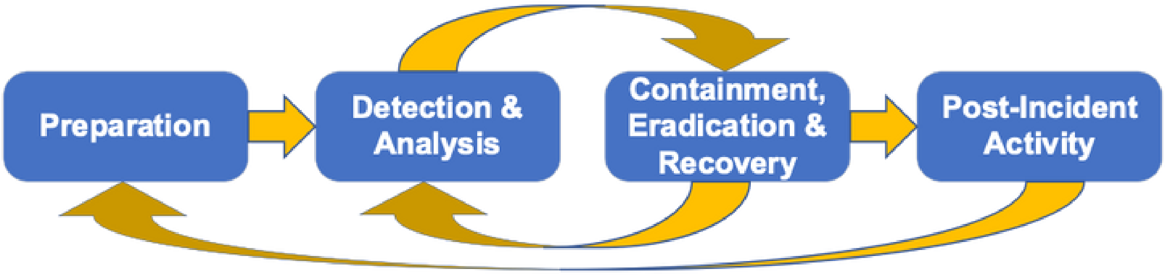
These are just some of the tools used to manage specific elements of cybersecurity to prevent cybersecurity incidents from happening.

Two tools are essential to monitoring situation awareness and enabling rapid response to events when they occur – SIEM and Security Orchestration, Automation, and Response (SOAR). We have been using SIEM tools for many years to consolidate information and provide alerts whenever an anomaly is detected at any level.

In recent years, an advance has been made on the SIEM concept. While the SIEM draws information from multiple sources and triggers alerts, SOAR tools gather information from various sources, conduct analysis per predetermined algorithms, and start immediate response scripts. Top-rated SOAR systems include Fortinet, Splunk, Swimlane, Palo Alto, and others. They provide built-in alerts, triage and investigation, risk management, intelligence management, pre-built and customized playbooks to automate incident response, dashboards, and analytics to provide real-time situation awareness. While they are relatively complex to implement, the initial work is more than offset by the significant improvements in protection, especially in incident response times. For example, SOAR automates virtually all processes defined by the use cases and known risks, cutting the time needed to address these issues from three to five hours to less than 20 milliseconds. Through automation of these processes, using a well-implemented SOAR eventually reduces the number of staff needed to respond to incidents and minimizes the damage from assaults.

Response

Regardless of the quality of defenses, incidents will still occur. When they do occur, the Incident Response Team (IRT), led by the IRT Lead, assesses the impact, takes steps to recover full functionality to the system, and conducts post-incident analysis to determine the forensics of the event and establish a means to prevent a repeat performance.
The National Institute of Standards and Technology (NIST) and the Cybersecurity and Infrastructure Security Agency (CISA) have defined a four-phase process for addressing all cybersecurity incidents. We have further identified key activities to illustrate how the SOC team and the IRT respond quickly and effectively when an incident occurs.



Preventing Incidents and Responding When They Do Happen

The IRT is separate from the SOC team. The SOC is focused on prevention and detection; the IRT is focused, as a member of our staff once said, on "Getting the bad guys." The SOC Team conducts vulnerability assessments and analysis, vulnerability management, malware protection, and information security continuous monitoring (ISCM). At the same time, the IRT addresses cyber incident handling, user activity monitoring for insider threats, and attack sensing and warning.

When addressing a suspected cybersecurity event, time is the critical element. IRTs must operate at the speed of technology to manage today's threat actors' velocity, sophistication, and frequency. The faster the IRT can validate an incident, understand the scope, implement primary containment, collect forensic information, identify vectors, and implement response and recovery activities, the greater the potential threat magnitude and the harm it can inflict on the mission. The scarcity of qualified cybersecurity analysts further complicates the challenge of cyber-attacks.

Platinum has proven our ability to recruit and retain skilled cybersecurity analysts and has access to well-qualified staff. We support our cybersecurity analysts and maximize their effectiveness by applying automation to address the time and resource challenges in initial responses for cybersecurity incident handling.

Our efforts begin with meticulous preparation. We formulate comprehensive playbooks of familiar and novel Indicators of Compromise (IOC), which serve as instructive guides, directing analysts toward the precise data, methodologies, and sequential actions requisite for addressing suspected events. These playbooks are digitized and linked to event/incident categories and keywords within the investigation record, eliminating the need to find and refer to external sources or procedures.

The task of detecting potential threats is intelligently automated, drawing upon a fusion of machine learning, artificial intelligence, and correlation rules. This amalgamation effectively winnows through the troves of event data, discerning noteworthy IOCs and anomalies that may signify malevolent undertakings. This automation significantly heightens the pace at which identifications are made, consequently expediting the process.

This concerted fusion of well-equipped cybersecurity professionals, adept playbooks, and judicious automation aids us in achieving a swift and effective identification of potential threats, ensuring an agile and efficient response to cybersecurity incidents.

Our operational toolkit includes powerful tools such as Rapid7, ELKStack, FireEye, CommandoVM, FLARE VM, Sift, and Splunk to track and analyze the impacts of cybersecurity incidents. The analysis is supported by introducing robotic process automation (RPA) that collects log information, performs automated scans, and returns the data to the investigation record for analyst triage and forensic activities using tools such as CrowdStrike.

Preventing Incidents and Responding When They Do Happen

Predetermined containment activities are automatically activated upon threat identification or by analyst initiation as a stored procedure – minimizing the potential for further loss, disruption, or contamination. Automatic containment actions include host network isolation through software-defined networking and automated blacklisting updates. Eradication and recovery activities are also automated to the extent possible to improve response and recovery velocity by deploying patches, conducting automated remediation and mitigation, and restoring systems to their last known good image, enabling mission operations to continue with minimal impact.

Eradication and recovery endeavors are similarly underpinned by meticulous automation, designed to enhance the responsiveness and swiftness of our response efforts. This involves the deployment of patches, automated remediation and mitigation techniques, and the restoration of systems to their most recent untainted configurations. This automated approach ensures the continuity of mission-critical operations with minimal hindrance by effectively minimizing downtime and swiftly restoring systems to operational integrity.

Platinum's pragmatic approach to cybersecurity is to digitize and automate reference, collection, status, and repetitive tasks to improve analyst resource productivity and real-time notification and response, creating an agile defensive posture while improving response velocity and overall efficacy.