Microsoft Sentinel SOC 101

aka.ms/SentinelSOC101

ROD TRENT
SENIOR PROGRAM MANAGER
MICROSOFT

This is part of an ongoing series to educate about using Microsoft Security products in real world scenario.

The full series index (including code, queries, and detections) is located here:

https://aka.ms/SentinelSOC101

The book will be updated when each new part in this series is released.

This book is updated every time a new part of this series is chaptered. The most current edition of this book will always be located at: https://github.com/rod-trent/Sentinel-SOC-101/tree/main/eBook

Book release ver. 0.010, October 19, 2023 12:00pm EST

Contents

Introduction

Microsoft Sentinel SOC 101: How to Protect Your Organization from Cyber Threats with Microsoft Sentinel

Cybersecurity is one of the most critical challenges facing organizations today. Cyberattacks are becoming more frequent, sophisticated, and damaging, targeting not only data and systems, but also people and reputation. According to a report by Cybersecurity Ventures, cybercrime is expected to cost the world $10.5 trillion annually by 2025, up from $3 trillion in 2015. This means that every 11 seconds, a business will fall victim to a cyberattack.

To defend against these threats, organizations need a robust and agile security operations center (SOC) that can detect, investigate, and respond to cyber incidents in real time. However, building and maintaining a SOC is not an easy task. It requires a lot of resources, expertise, and tools, which are often scarce and expensive. Moreover, traditional SOCs are often overwhelmed by the volume and complexity of security alerts, resulting in alert fatigue, missed threats, and slow response times.

This is where Microsoft Sentinel comes in. Microsoft Sentinel is a cloud-native security information and event management (SIEM) solution that leverages the power of artificial intelligence (AI) and machine learning (ML) to help organizations improve their security chapterure and reduce the cost and complexity of their SOC. Microsoft Sentinel enables organizations to:

- Collect data from any source, including Microsoft products and services, third-party solutions, and on-premises systems
- Analyze data using built-in or custom rules, ML models, and threat intelligence to detect known and unknown threats

- Investigate incidents using intuitive dashboards, visualizations, and playbooks that provide contextual and actionable insights
- Respond to incidents using automated or manual actions that leverage native or integrated tools and workflows
- Learn from incidents using feedback loops and continuous improvement mechanisms that enhance the security over time

Microsoft Sentinel is designed to help organizations of any size and industry to protect their assets, users, and reputation from cyber threats. Whether you are new to SIEM or looking for a better alternative to your existing solution, Microsoft Sentinel can help you achieve your security goals.

In this book, you will learn how to use Microsoft Sentinel to detect and mitigate some of the most common and impactful cyberattacks that target organizations today. Each chapter will cover a different type of attack, such as brute force, phishing, malware, cross-site scripting (XSS), supply chain, credential reuse, SQL injection, denial of service (DoS), man-in-the-middle (MitM), keylogger, cryptojacking, or drive-by download. You will learn how these attacks work, what are their indicators of compromise (IoCs), how to configure Microsoft Sentinel to detect them, how to investigate them using Microsoft Sentinel's features and capabilities, and how to respond to them using Microsoft Sentinel's integrations and automation options. You will also learn how to leverage the MITRE ATT&CK framework, a globally recognized knowledge base of adversary tactics and techniques, to enhance your threat detection and response with Microsoft Sentinel.

By the end of this book, you will have a solid understanding of how Microsoft Sentinel can help you protect your organization from

cyber threats. You will also have the skills and confidence to use Microsoft Sentinel effectively in your own SOC.

Let’s get started!

Microsoft Sentinel SOC 101: How to Detect and Mitigate Brute Force Attacks with Microsoft Sentinel

Brutish

Brute force attacks are one of the most common and concerning security threats that organizations face today. These attacks involve

an attacker attempting to gain unauthorized access to a system or account by systematically trying different passwords or passphrases until they find the correct one. Detecting and mitigating these attacks is crucial to maintaining the security and integrity of your systems.

The goal of a brute force attack is to exploit weak or easily guessable passwords and gain unauthorized access to a system. Attackers often use automated tools that can generate and test thousands of password combinations within a short period. These attacks can target various entry points, such as user accounts, remote desktop protocols (RDP), or SSH management ports. As a result, organizations need robust security measures in place to detect and prevent these attacks effectively.

Let's explore how you can leverage Microsoft Sentinel, a cloud-native Security Information Event Management (SIEM) and Security Orchestration Automated Response (SOAR) solution, to effectively detect and respond to brute force attacks. Let's talk about the necessary prerequisites, the collection of security events, the configuration of Azure Sentinel, and the creation of analytic rules to identify and mitigate these attacks. And then, let's talk about how to simulate a brute force attack to test your detection capabilities.

Collecting Security Events

To detect brute force attacks, organizations must collect and analyze security events. Microsoft Sentinel provides a comprehensive set of tools and data connectors to gather relevant security logs and events from various sources. By centralizing these logs in a log analytics workspace, organizations can perform in-depth analysis and create custom detection rules.

One crucial security event to monitor is the Windows Event ID 4625, which indicates failed login attempts. By focusing on successive failed logins, organizations can identify potential brute force attacks. The log analytics workspace in Microsoft Sentinel enables organizations to query and analyze these security events effectively.

Creating Analytic Rules for Brute Force Attacks

Once the security events are collected and stored in the log analytics workspace, organizations can create analytic rules to detect brute force attacks. Analytic rules in Microsoft Sentinel allow organizations to define specific conditions and patterns that indicate a potential attack.

To create an analytic rule for brute force attacks, organizations can leverage the power of the Kusto Query Language (KQL) in Microsoft Sentinel. KQL enables organizations to query the collected security events and filter them based on specific criteria. By using KQL, organizations can create rules that detect specific Event IDs, like Event ID 4625, and filter for failed login attempts with certain substatuses.

For example, a KQL query to detect brute force attacks targeting RDP or SSH management ports could be:

```
SecurityEvent
| where EventID == 4625
| where (SubStatus == "0xc000006A" or SubStatus == "0xc0000064")
| project TimeGenerated, EventID, WorkstationName, Computer, Account,
LogonTypeName, LogonType, LogonProcessName, SubStatus, Activity
```

This query filters for Event ID 4625 (failed logins) and specific substatuses indicating a brute force attack on RDP or SSH management ports. By creating an analytic rule based on this query, organizations can automatically detect and respond to brute force attacks.

Simulating Brute Force Attacks

To test the effectiveness of the analytic rules and detection mechanisms, organizations can simulate brute force attacks. Simulating attacks allows organizations to evaluate the responsiveness and accuracy of their detection rules and identify any potential gaps in their security measures.

Other than writing a tool (PowerShell or otherwise) to simulate a Brute Force attack, tools like Kali Linux and Hydra can be used to simulate brute force attacks. These tools enable organizations to automate the process of trying different passwords and passphrases against targeted user accounts or entry points. By running these simulated attacks and monitoring the alerts generated by Microsoft Sentinel, organizations can fine-tune their detection rules and improve their overall security chapterure.

See:

Using Kali Linux and Hydra for Attack Testing and Alert Generation

Brute force attacks are an essential part of penetration testing, allowing security professionals to assess the strength of a system's passwords. One popular tool is Hydra, an open-source login cracker that supports over 50 protocols. In this tutorial, I'll explore how to use Hydra in conjunction with Kali Linux, a powerful penetration testing operating...

Read the full story: https://rodtrent.substack.com/p/using-kali-linux-and-hydra-for-attack

Preventing Brute Force Attacks

While detecting and responding to brute force attacks is essential, organizations should also implement preventive measures to mitigate the risk of such attacks. Here are some best practices to prevent brute force attacks:

Enforce Strong Password Policies

Implementing strong password policies is crucial to prevent brute force attacks. Organizations should enforce password complexity requirements, such as a minimum length, a combination of uppercase and lowercase letters, numbers, and special characters. Additionally, regularly educating users about the importance of strong passwords and password hygiene can further enhance security.

Implement Account Lockout Policies

Account lockout policies can help mitigate the impact of brute force attacks. By setting thresholds for failed login attempts, organizations can automatically lock user accounts temporarily or permanently. This prevents attackers from making unlimited login

attempts and significantly reduces the success rate of brute force attacks.

Implement Multi-Factor Authentication (MFA)

Multi-factor authentication adds an extra layer of security and makes it significantly harder for attackers to gain unauthorized access. By requiring users to provide additional verification, such as a code sent to their mobile device or a fingerprint scan, even if an attacker manages to guess the password, they would still need the additional factor to gain access.

Implement Rate Limiting

Rate limiting can be an effective strategy to prevent brute force attacks. By limiting the number of login attempts per second or per minute, organizations can significantly slow down the attackers' progress. This makes it impractical for attackers to guess passwords within a reasonable timeframe, discouraging brute force attacks.

Monitor and Analyze Logs

Continuous monitoring and analysis of security logs are crucial to detecting and mitigating brute force attacks. By regularly reviewing the logs and looking for patterns of failed login attempts, organizations can proactively identify potential brute force attacks and take appropriate action such as those outlined as mitigations, including:

1. **Implement a lockout policy:** Implement a lockout policy that will lock out the account after a certain number of failed login attempts. This will prevent attackers from trying multiple passwords on the same account.

2. **Use strong passwords:** Strong passwords with a combination of letters, numbers, and symbols will make it harder for attackers to guess the password.
3. **Implement two-factor authentication:** Two-factor authentication adds an extra layer of security by requiring a second form of authentication, such as a fingerprint or a code sent to a mobile device.
4. **Monitor network traffic:** Monitoring network traffic can help detect brute force attacks and other suspicious activity.
5. **Implement intrusion detection and prevention systems:** Intrusion detection and prevention systems can help detect and prevent brute force attacks by monitoring network traffic and blocking suspicious activity.
6. **Conduct regular security audits:** Regular security audits can help identify vulnerabilities and weaknesses in the system and allow for timely remediation.
7. **Report the attack:** If an attack is detected, it should be reported to the relevant authorities, such as law enforcement or the organization's security team.

Summary

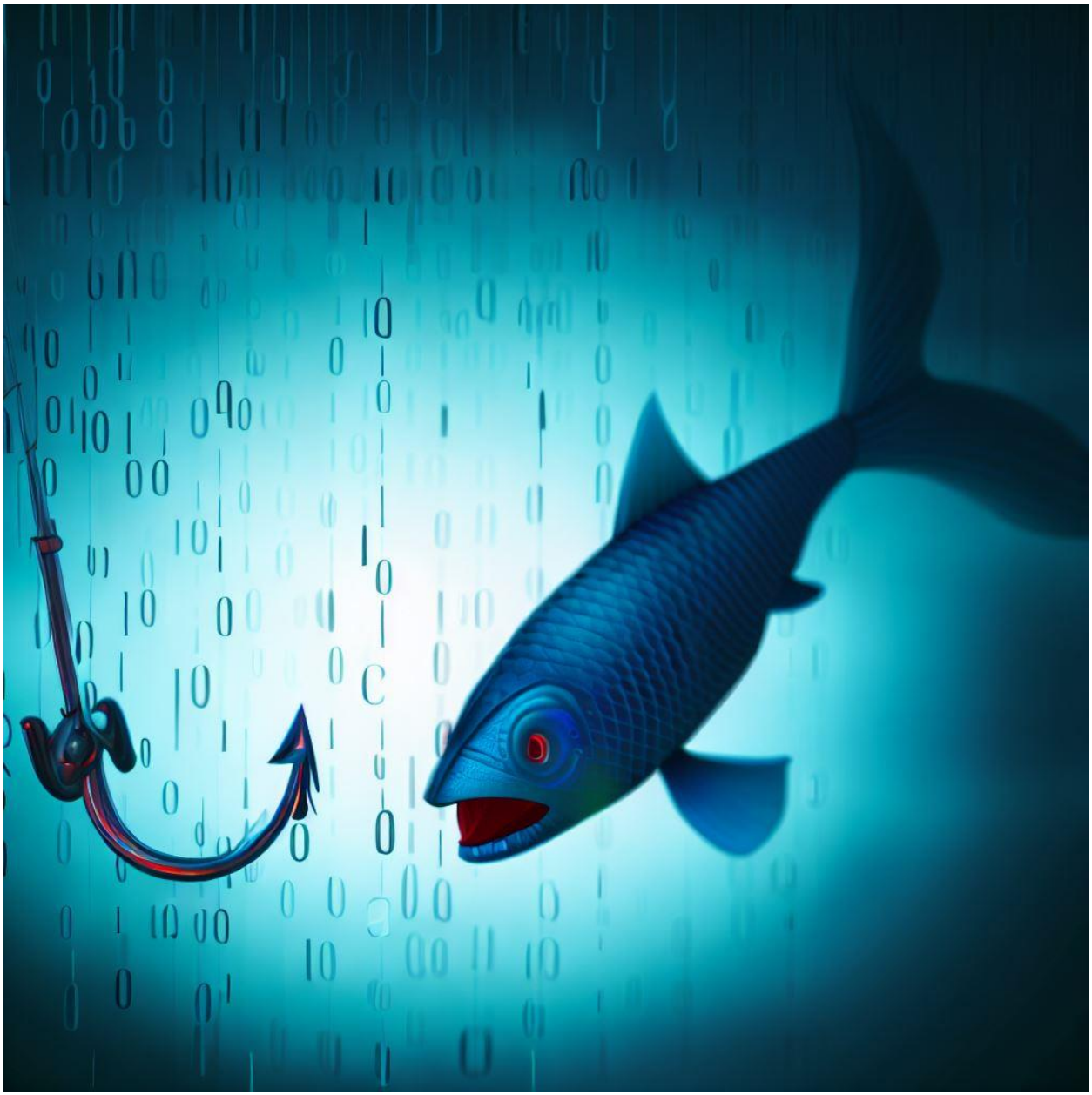
Brute force attacks pose a significant threat to organizations' security and can lead to data breaches and unauthorized access. However, with the robust capabilities of Microsoft Sentinel, organizations can detect and prevent these attacks effectively.

By collecting and analyzing security events, creating analytic rules, and simulating attacks, organizations can proactively detect brute force attacks and respond promptly. Additionally, implementing preventive measures such as strong password policies, account lockout policies, multi-factor authentication, rate limiting, and continuous log monitoring can significantly enhance the security chapterure of organizations.

With Microsoft Sentinel as a powerful security analytics and threat intelligence platform, organizations can stay one step ahead of attackers and protect their valuable data and resources from brute force attacks. By leveraging the capabilities of Microsoft Sentinel, organizations can detect, prevent, and remediate brute force attacks, ensuring the security of their digital assets.

Microsoft Sentinel SOC 101: How to Detect and Mitigate Phishing Attacks with Microsoft Sentinel

Hook, Line, Stinker



Phishing attacks have become increasingly prevalent and pose significant risks to individuals and organizations alike.

Cybercriminals are constantly evolving their tactics, making it crucial for security professionals to stay ahead of the game. One effective approach to combatting phishing attacks is to leverage the power of Microsoft Sentinel, a cloud-native security information and event management (SIEM) solution. In this article, we will explore the steps to detect and mitigate phishing attacks using Microsoft Sentinel. From understanding the threat landscape to implementing proactive measures, this article will equip you with the knowledge and tools to safeguard your organization against phishing threats.

Introduction to Phishing Attacks

The Rising Threat of Phishing Attacks

Phishing attacks have become a pervasive and persistent threat in recent years. These attacks involve cybercriminals masquerading as trustworthy entities to trick individuals into divulging sensitive information or performing actions that compromise security. Phishing attacks can take various forms, including email phishing, smishing (SMS phishing), and vishing (voice phishing). The sophistication of phishing attacks continues to increase, making them harder to detect and resist.

Why Phishing Attacks are Successful

Phishing attacks are highly effective for several reasons. Firstly, they exploit human vulnerabilities, targeting individuals' trust, curiosity, and desire for convenience. Phishing emails often appear legitimate, using social engineering techniques to deceive recipients. Additionally, the sheer volume of phishing attacks makes it challenging for organizations to identify and respond to every instance. Cybercriminals often take advantage of current events and trends to enhance the authenticity of their attacks. The

financial gain for attackers is substantial, as successful phishing attacks can lead to identity theft, financial fraud, or unauthorized access to sensitive data.

The "Defense in Depth" Approach

Layered Security for Comprehensive Protection

To effectively combat phishing attacks, organizations need to adopt a "defense in depth" approach. This approach involves deploying multiple layers of security measures that address various stages of the attack chain. By implementing a combination of preventive, detective, and responsive security controls, organizations can significantly reduce their vulnerability to phishing attacks. The key is to have a comprehensive security strategy that encompasses user education, email filtering, endpoint protection, network security, and incident response.

Addressing Phishing Across the Attack Chain

Phishing attacks typically involve several stages, from the initial delivery of a malicious email to the execution of the final payload. To mitigate the risks associated with phishing attacks, organizations need to address each stage of the attack chain. This includes implementing measures such as:

- User education and awareness programs to help individuals recognize and report phishing emails.
- Robust email filtering solutions to identify and block phishing emails before they reach users' inboxes.
- Endpoint protection solutions that can detect and block malicious attachments or URLs.
- Network security controls, such as firewalls and intrusion detection systems, to monitor and prevent unauthorized access.

- Incident response plans and procedures to enable organizations to respond effectively in the event of a phishing attack.

By implementing security measures at each stage of the attack chain, organizations can significantly reduce their vulnerability to phishing attacks and minimize the potential impact of successful attacks.

Proactive Threat Hunting with Microsoft Sentinel

Leveraging KQL for Threat Hunting

Microsoft Sentinel provides security professionals with a powerful toolset for proactive threat hunting. Key to this capability is the use of Kusto Query Language (KQL), a powerful query language that allows analysts to search and analyze large volumes of data quickly. By leveraging KQL, security teams can identify potential phishing threats by searching for patterns and indicators of compromise (IoCs) within their data.

EXAMPLE: This query determines emails sent by top malicious/bad IP addresses.

```
let cutoff = 5;
EmailEvents
| where ThreatTypes has "Malware" or ThreatTypes has "Phish"
| summarize count() by SenderIPv4
| where count_ > cutoff // Arbitrary cutoff, increase or decrease as needed
| join EmailEvents on SenderIPv4
| where DeliveryAction =~ "Delivered"
```

Identifying Emerging Phishing Campaigns

Phishing campaigns are constantly evolving, with cybercriminals employing new techniques and tactics to bypass security measures. To stay ahead of these threats, security teams can use Microsoft Sentinel to proactively hunt for emerging phishing campaigns. By

monitoring and analyzing data from various sources, such as Microsoft 365 Threat Protection (MTP), Defender for Office, and Microsoft Cloud App Security (MCAS), analysts can identify patterns and behaviors associated with phishing attacks.

Integrating Microsoft 365 Threat Protection

Utilizing Microsoft 365 Threat Protection (MTP)

Microsoft 365 Threat Protection (MTP) is a comprehensive security solution that combines the power of multiple Microsoft security products. It includes features such as Office 365 Advanced Threat Protection and Windows Defender. By integrating MTP with Microsoft Sentinel, organizations can benefit from enhanced threat detection and response capabilities.

Exploring Threat Hunting Capabilities in MTP

Within MTP, security analysts can leverage advanced hunting capabilities to proactively search for and investigate potential phishing threats. Advanced hunting allows analysts to query and analyze vast amounts of security-related data, helping them identify patterns, trends, and IoCs associated with phishing attacks. By combining this data with the power of KQL, analysts can gain deeper insights into emerging phishing campaigns and take proactive steps to mitigate the risks.

The Power of Microsoft Sentinel

Understanding the Role of Microsoft Sentinel

Microsoft Sentinel is a cloud-native SIEM solution that enables organizations to collect, analyze, and visualize security data from various sources. It provides a centralized platform for managing security incidents, conducting investigations, and implementing

response actions. By integrating with Microsoft Sentinel, organizations can leverage the power of the cloud to enhance their threat detection and response capabilities.

Integration with Microsoft 365 Threat Protection

One of the key benefits of integrating with Microsoft Sentinel is the seamless integration with Microsoft 365 Threat Protection. This integration allows security teams to correlate and analyze data from MTP alongside other security data sources, enabling a more comprehensive and holistic view of potential phishing threats. By centralizing and correlating data from multiple sources, organizations can detect and respond to phishing attacks more effectively.

Connect data from Microsoft 365 Defender to Microsoft Sentinel

Building a Security Orchestration, Automation, and Response (SOAR) System

Implementing Security Automation with Logic Apps

To enhance the efficiency and effectiveness of phishing attack response, organizations can implement security orchestration, automation, and response (SOAR) systems. Microsoft Sentinel provides integration with Azure Logic Apps, allowing organizations to automate and streamline their phishing attack response processes. Logic Apps enable organizations to create workflows that automate various security tasks, such as analyzing suspicious emails, blocking malicious URLs, and generating incident reports.

Creating an End-to-End Phishing Attack Response System

By combining the power of Microsoft Sentinel and Logic Apps, organizations can create an end-to-end phishing attack response

system. This system can automatically detect and analyze potential phishing emails, assess the risk level, and trigger appropriate response actions based on predefined rules and workflows. Examples of response actions include quarantining suspicious emails, blocking malicious URLs, and notifying security teams for further investigation.

Investigating Phishing Emails with Kusto Query Language (KQL)

Analyzing URLs in Phishing Emails

Kusto Query Language (KQL) provides a powerful tool for investigating phishing emails. Analysts can use KQL queries to search for specific URLs within email events and correlate them with known phishing URLs from external threat intelligence sources. By identifying and analyzing URLs that match known phishing URLs, organizations can proactively identify potential phishing attacks and take appropriate action to mitigate the risks.

Example: SecurityAlert-VisualizeTopPhishingDomains.kql

Extracting Relevant Information from Email Events

In addition to analyzing URLs, KQL queries can also extract relevant information from email events, such as sender information, subject lines, attachment counts, and timestamps. By summarizing and analyzing this information, organizations can gain insights into the characteristics and patterns of phishing emails. This information can help in identifying trends, improving detection algorithms, and guiding incident response efforts.

Taking Action Against Phishing Attacks

Automating Responses for High-Confidence Phishing Attacks

Organizations can further enhance their phishing attack response capabilities by automating response actions for high-confidence phishing attacks. By leveraging the power of Microsoft Sentinel and Logic Apps, security teams can create automated workflows that trigger predefined response actions based on specific criteria. Examples of automated response actions include blocking malicious URLs, quarantining suspicious emails, and notifying security teams for further investigation.

Reporting Suspicious Emails to the NCSC

To combat phishing attacks effectively, organizations can report suspicious emails to external authorities such as the National Cyber Security Centre (NCSC). Microsoft Sentinel can be integrated with the Suspicious Email Reporting Service (SERS) provided by the NCSC, enabling organizations to automatically report identified phishing emails. By sharing information with external authorities, organizations contribute to a broader cybersecurity ecosystem, helping to protect others from similar attacks.

Enhancing Email Security with Microsoft Sentinel

Establishing Custom Logs for Email Events

Microsoft Sentinel allows organizations to establish custom logs for email events, providing a centralized repository for storing and analyzing email-related data. By configuring custom logs, organizations can capture and analyze email events at a granular level, enabling more effective threat detection and incident response. Custom logs can be tailored to capture specific attributes

and metadata of emails, such as sender information, recipient information, subject lines, and attachment details.

Parsing Data to Facilitate Investigation

Once email events are captured in custom logs, organizations can parse and analyze the data to facilitate investigation and response efforts. By extracting relevant information from email events, such as sender addresses, recipient addresses, and attachment details, organizations can gain insights into the characteristics and patterns of phishing attacks. This information can be used to develop more robust detection algorithms, improve incident response procedures, and enhance overall email security.

Advanced Investigation Techniques

Deep Dive Investigations with KQL

When investigating potential phishing attacks, security teams can perform deep dive investigations using Kusto Query Language (KQL). By combining KQL queries with advanced hunting capabilities, organizations can search and analyze large volumes of security-related data to identify potential phishing threats. Deep dive investigations can uncover hidden patterns, trends, and IoCs, enabling organizations to proactively detect and respond to phishing attacks.

EXAMPLE: This query helps surface phishing campaigns associated with Appspot abuse. These emails frequently contain phishing links that utilize the recipients' own email address as a unique identifier in the URI.

```
EmailUrlInfo
// Detect URLs with a subdomain on appspot.com
| where UrlDomain matches regex @'\b[\w\-]+-dot-[\w\-\.]+\.appspot\.com\b'
// Enrich results with sender and recipient data
```

```
| join kind=inner EmailEvents on
$left.NetworkMessageId==$right.NetworkMessageId
// Phishing attempts from Appspot related campaigns typically contain the
recipient's email address in the URI
// Example 1: https://example-dot-example.appspot.com/#recipient@domain.com
// Example 2: https://example-dot-
example.appspot.com/index.html?user=recipient@domain.com
| where Url has RecipientEmailAddress
    // Some phishing campaigns pass recipient email as a Base64 encoded
string in the URI
    or Url has base64_encode_tostring(RecipientEmailAddress)
| project-away Timestamp1, NetworkMessageId1, ReportId1
```

Monitoring Multiple Distinct EDR Events per Host

To enhance the effectiveness of phishing attack detection, security teams can monitor multiple distinct endpoint detection and response (EDR) events per host. By correlating and analyzing EDR events from different hosts, organizations can identify patterns and trends associated with phishing attacks. This approach allows for a more comprehensive view of potential threats and enables organizations to respond more effectively to phishing attacks.

Summary

In conclusion, Microsoft Sentinel provides powerful tools and capabilities for detecting and mitigating phishing attacks. By leveraging KQL, integrating with Microsoft 365 Threat Protection, and implementing security automation with Logic Apps, organizations can proactively detect and respond to phishing threats. With Microsoft Sentinel, organizations can centralize and correlate security data, enabling a more comprehensive view of potential phishing attacks. By combining these tools and techniques, organizations can enhance their email security chapterure and protect against the ever-evolving threat of phishing attacks.

Microsoft Sentinel SOC 101: How to Detect and Mitigate Malware Attacks with Microsoft Sentinel

Mall Wear

Malware attacks pose a significant threat to organizations of all sizes. These attacks can result in data breaches, financial losses,

and damage to an organization's reputation. To effectively detect and mitigate malware attacks, organizations need robust security measures in place. Microsoft Sentinel, a cloud-native Security Information and Event Management (SIEM) solution, offers advanced threat detection and response capabilities to defend against malware attacks.

Introduction to Malware Detection and Mitigation

Cybercriminals are constantly evolving their methods to evade detection and infiltrate organizations' systems. Therefore, it is crucial for organizations to stay one step ahead by leveraging advanced detection and mitigation techniques. Microsoft Sentinel provides a comprehensive set of tools and features to detect and mitigate malware attacks effectively.

Importance of Customizable Anomalies

One of the key features of Microsoft Sentinel is its customizable anomaly detection. Anomalies are machine learning-based models that can identify unusual behavior in systems. While anomalies themselves do not necessarily indicate malicious activity, they can serve as additional signals to improve detection, provide evidence during investigations, and guide proactive threat hunting.

Microsoft Sentinel's customizable anomalies are pre-tuned by the data science team, allowing organizations to gain immediate value without the need for complex tuning or extensive machine learning knowledge. Organizations can further fine-tune these anomalies through the user-friendly analytics rule interface to meet their specific needs.

Use customizable anomalies to detect threats in Microsoft Sentinel

Utilizing User and Entity Behavior Analytics (UEBA) Anomalies

Microsoft Sentinel leverages User and Entity Behavior Analytics (UEBA) to detect anomalies based on dynamic baselines created for each entity. These baselines are established using historical activities, peer behavior, and organizational patterns. By correlating different attributes such as action type, geo-location, device, resource, and ISP, UEBA anomalies can identify potential threats and provide valuable insights during investigations and threat hunting activities.

Enable User and Entity Behavior Analytics (UEBA) in Microsoft Sentinel

Detecting Malware Attacks with Microsoft Sentinel

Microsoft Sentinel offers a wide range of capabilities to detect and respond to malware attacks effectively. By leveraging its advanced detection mechanisms and threat intelligence integration, organizations can proactively identify and mitigate malware threats.

Importing Threat Intelligence

Threat intelligence plays a crucial role in detecting and responding to malware attacks. Microsoft Sentinel allows organizations to import threat intelligence from various sources, including open-source data feeds, commercial intelligence feeds, and local intelligence gathered during security investigations. By integrating threat intelligence into Microsoft Sentinel, organizations can enhance their detection capabilities and gain valuable context for investigative purposes.

Threat intelligence integration in Microsoft Sentinel

Leveraging Data Connectors

Data connectors in Microsoft Sentinel enable the import of threat indicators and other security-related data from various sources. These connectors include the Microsoft Defender Threat Intelligence data connector, Threat Intelligence - TAXII data connector, and Threat Intelligence Platforms data connector. By utilizing these connectors, organizations can centralize their threat intelligence data and leverage it to detect and respond to malware attacks effectively.

Threat intelligence integration in Microsoft Sentinel

Using Analytics Rule Templates

Microsoft Sentinel provides built-in analytics rule templates that organizations can leverage to detect malware attacks. These templates cover a wide range of scenarios and can be customized to fit specific organizational needs. By applying these rule templates, organizations can identify suspicious activities and generate security alerts to initiate the incident response process.

Example: Malware uploaded to SharePoint or OneDrive

```
OfficeActivity
| where TimeGenerated > ago(30d)
| where Operation == "FileMalwareDetected"
| project
    TimeGenerated,
    OfficeWorkload,
    ['File Name']=SourceFileName,
    ['File Location']=OfficeObjectId,
    ['Relative File URL']=SourceRelativeUrl,
    ClientIP
```

Responding to Malware Attacks with Microsoft Sentinel

Once a malware attack is detected, organizations must have a well-defined incident response plan in place. Microsoft Sentinel offers a

range of response capabilities to effectively mitigate the impact of malware attacks and prevent further damage.

Example - Ransomware Attack: Incident Response Plan and Action Items

Incident Triage and Investigation

When an incident is detected, organizations can triage and investigate the incident using the Microsoft Sentinel portal. Security analysts can review alerts, gather contextual information, and assess the severity of the incident. By leveraging the visualization capabilities of Microsoft Sentinel, analysts can gain a comprehensive understanding of the attack and its potential impact.

Understand Microsoft Sentinel's incident investigation and case management capabilities

Security Orchestration Automation and Remediation (SOAR)

Microsoft Sentinel's Automated Investigation and Response capabilities help security operations teams streamline their incident response processes. AIR can examine alerts, perform automated investigations, and initiate response actions based on predefined playbooks. By automating repetitive tasks, organizations can free up valuable resources and respond to malware attacks more efficiently.

Examples:

Block-AADUserOrAdmin

Isolate-AzureVMtoNSG

Threat Hunting with Anomalies

Threat hunting is an essential proactive security practice that helps organizations identify and mitigate potential threats before they cause significant harm. By using anomalies as a starting point, threat hunters can conduct investigations and explore potential indicators of compromise (IOCs). Anomalies provide valuable context and guide threat hunters in identifying suspicious activities and uncovering hidden threats.

Threat Hunting TI Feed - ThreatfoxMalwareDomains.md

Summary

Detecting and mitigating malware attacks is a critical aspect of maintaining a robust cybersecurity chapterure. Microsoft Sentinel offers powerful capabilities to help organizations identify and respond to malware attacks effectively. From customizable anomalies and threat intelligence integration to automated investigation and response, Microsoft Sentinel empowers organizations to stay one step ahead of cybercriminals and protect their valuable assets. By leveraging these advanced features, organizations can detect and mitigate malware attacks in a timely and efficient manner, minimizing the potential impact on their operations.

Microsoft Sentinel SOC 101: How to Detect and Mitigate Cross-Site Scripting (XSS) Attacks with Microsoft Sentinel

Criss-cross, applesauce

In today's digital landscape, web application security is of utmost importance. Protecting your web applications from common attacks

like Cross-Site Scripting (XSS) is crucial to ensure the confidentiality, integrity, and availability of your data. In this article, we will explore how Microsoft Sentinel, a powerful security information and event management (SIEM) solution, can help you detect and mitigate XSS attacks.

Introduction to Cross-Site Scripting (XSS) Attacks

Cross-Site Scripting (XSS) attacks are a common type of web application vulnerability where an attacker injects malicious scripts into trusted websites, which are then executed by unsuspecting users. These attacks can lead to various consequences, including unauthorized access to sensitive data, session hijacking, defacement of websites, and even the spread of malware.

XSS attacks can be classified into three main types:

- **Stored XSS**: The malicious script is permanently stored on the target server and served to users whenever they access the affected page.
- **Reflected XSS**: The malicious script is embedded in a URL parameter and is reflected back to the user by the server.
- **DOM-based XSS**: The malicious script is injected into the Document Object Model (DOM) of a web page and executed by the victim's browser.

Understanding XSS Attack Vectors

XSS attacks can occur through various attack vectors, exploiting vulnerabilities in different parts of a web application. Some common XSS attack vectors include:

- **Input Fields**: Attackers can inject malicious scripts into input fields such as contact forms, search boxes, and comment sections.

- **URL Parameters**: Attackers can manipulate URL parameters to inject malicious scripts that are then reflected back to the user.
- **Cookies**: Attackers can modify cookies to execute malicious scripts in the victim's browser.
- **HTTP Headers**: Attackers can inject malicious scripts into HTTP headers, which are then executed by the victim's browser.
- **Third-Party Scripts**: Attackers can compromise third-party scripts used by a website, allowing them to inject and execute malicious code.

It's important to understand these attack vectors to effectively detect and mitigate XSS attacks in your web applications.

Azure WAF and Microsoft Sentinel: A Powerful Combination

Azure Web Application Firewall (WAF) and Microsoft Sentinel work together to provide comprehensive protection against XSS attacks. Azure WAF is a cloud-based firewall service that protects web applications from common attacks, including XSS. Microsoft Sentinel, on the other hand, is a cloud-native SIEM solution that provides intelligent security analytics and threat intelligence across your enterprise.

By integrating Azure WAF with Microsoft Sentinel, you can leverage the advanced detection capabilities of Azure WAF and the powerful analytics and automation features of Microsoft Sentinel to effectively detect, investigate, and respond to XSS attacks.

Configuring Azure WAF for XSS Attack Detection

To configure Azure WAF for XSS attack detection, follow these steps:

1. Set up an Azure Application Gateway or Azure Front Door with Azure WAF enabled.
2. Configure the firewall mode to "Prevention" to block suspicious incoming traffic.
3. Enable monitoring of Azure WAF logs using Azure Monitor or Azure Security Center.
4. Set up the Azure WAF Data Connector to send WAF logs to Azure Sentinel for advanced threat detection.

By following these steps, you can ensure that Azure WAF is actively monitoring and protecting your web applications against XSS attacks.

Leveraging Microsoft Sentinel for XSS Attack Detection

Microsoft Sentinel provides powerful capabilities to detect XSS attacks and other security incidents. By utilizing Microsoft Sentinel's advanced analytics, machine learning algorithms, and threat intelligence, you can effectively identify and investigate XSS attacks in real-time.

To leverage Microsoft Sentinel for XSS attack detection, create an analytics rule with the following KQL query:

```
AzureDiagnostics
| where ResourceType == "APPLICATIONGATEWAYS"
| where Category == "ApplicationGatewayFirewallLog"
| where Message contains "XSS Attack"
| project Message, details_message_s, details_data_s, clientIp_s, action_s
```

This query filters the Azure WAF logs for XSS attack incidents. When an XSS attack is detected, Microsoft Sentinel will generate an incident for further investigation.

Analyzing XSS Attack Incidents in Microsoft Sentinel

Once an XSS attack incident is generated in Microsoft Sentinel, you can analyze it using various tools and features provided by the platform. The following steps outline the process of analyzing XSS attack incidents:

1. Access the Incidents page in Microsoft Sentinel to view all generated incidents.
2. Filter and search for XSS attack incidents based on severity, status, or specific criteria.
3. Select an incident to view detailed information, including the timeline of alerts and bookmarks related to the incident.
4. Use the investigation graph to visualize the entities and relationships involved in the XSS attack.
5. Review the alerts and entities associated with the incident to gain insights into the attack and potential impact.
6. Collaborate with other analysts by adding comments and sharing findings to facilitate investigation and response.

By following these steps, you can effectively analyze XSS attack incidents and gain a deeper understanding of the attack's scope and impact.

Responding to XSS Attacks with Microsoft Sentinel

When an XSS attack is detected and analyzed in Microsoft Sentinel, it's important to respond promptly to mitigate the impact and prevent further exploitation. The following actions can be taken to respond to XSS attacks:

1. Block the IP address or source of the attack to prevent further malicious activity.

2. Investigate the affected web application to identify and patch vulnerabilities that allowed the XSS attack.
3. Communicate with affected users and provide guidance on how to protect themselves against potential risks.
4. Update security policies and procedures to prevent future XSS attacks.
5. Educate developers and security teams on best practices for web application security, including input validation and output encoding.

By taking these proactive measures, you can effectively respond to XSS attacks and minimize the risk of future incidents.

Best Practices for XSS Attack Prevention

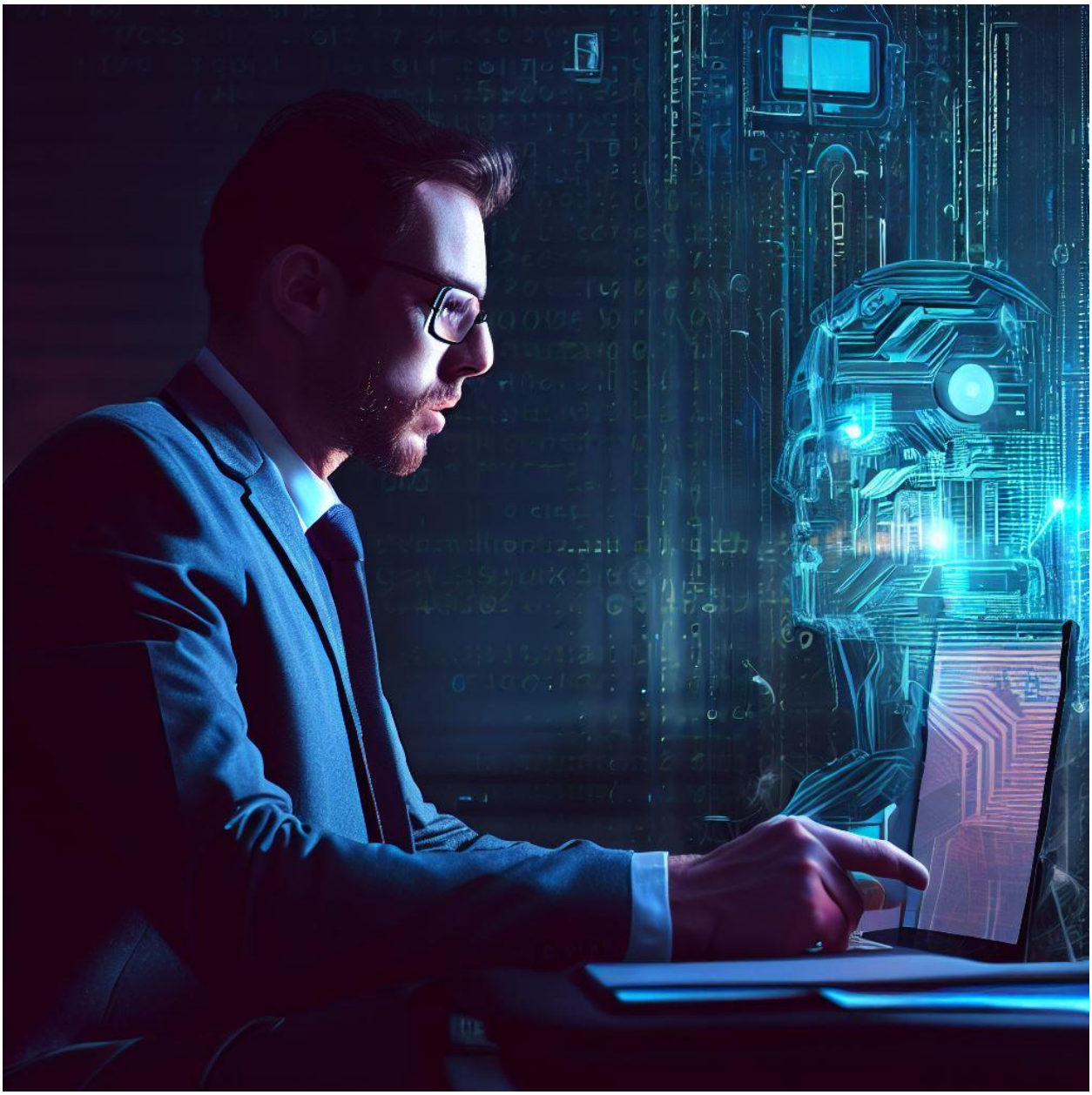
Preventing XSS attacks requires a combination of secure coding practices, robust security controls, and ongoing monitoring. Here are some best practices to help prevent XSS attacks:

1. Implement input validation and output encoding to ensure that user-supplied data is treated as plain text and not as executable code.
2. Use secure coding frameworks and libraries that provide built-in protection against XSS attacks.
3. Regularly update and patch web application software to address known vulnerabilities.
4. Train developers on secure coding practices, including the proper handling of user input and output.
5. Implement web application firewalls and security monitoring solutions, such as Azure WAF and Microsoft Sentinel, to detect and mitigate XSS attacks in real-time.
6. Conduct regular security assessments and penetration testing to identify and remediate any vulnerabilities in your web applications.

By following these best practices, you can significantly reduce the risk of XSS attacks and ensure the security of your web applications.

Microsoft Sentinel SOC 101: Leveraging MITRE ATT&CK Techniques with Microsoft Sentinel

MITRE is Mightier



Microsoft Sentinel is a powerful, cloud-native security information and event management (SIEM) platform that helps organizations

detect, prevent, and respond to cybersecurity threats. One of the ways Sentinel achieves this is through Analytics Rules, which are designed to identify potential security issues in your environment based on patterns and indicators.

To further enhance your organization's security chapterure, it is critical to align your Sentinel Analytics Rules with the MITRE ATT&CK framework. This framework is a globally recognized, comprehensive matrix of tactics and techniques used by threat actors during their attack campaigns. By incorporating MITRE techniques into your Sentinel Analytics Rules, you can effectively identify, analyze, and respond to threats more efficiently.

In this chapter, I'll discuss some best practices for using MITRE techniques in conjunction with Microsoft Sentinel Analytics Rules and talk about using the MITRE ATT&CK blade in Microsoft Sentinel.

Understand the MITRE ATT&CK Framework

Before diving into the implementation of MITRE techniques, it is essential to understand the MITRE ATT&CK framework. The framework consists of tactics (the attacker's objectives) and techniques (the methods used to achieve those objectives). Familiarize yourself with the various tactics and techniques available in the framework to identify which ones are most relevant to your organization's security needs.

https://attack.mitre.org/

Map Your Existing Analytics Rules to MITRE Techniques

Evaluate your existing Sentinel Analytics Rules and identify the MITRE techniques they cover. This will help you understand any gaps in your detection and response capabilities. You can use the Microsoft Security Center's built-in mapping feature to quickly identify the relevant MITRE techniques for your rules.

Prioritize Techniques Based on Your Threat Landscape

Not all organizations are equally vulnerable to every technique in the MITRE ATT&CK framework. Understand your organization's threat landscape and prioritize implementing the most relevant techniques. Consider factors such as your industry, geography, and the types of data and assets you need to protect.

Implement Custom Analytics Rules for High-Priority Techniques

After prioritizing the most relevant MITRE techniques for your organization, create custom Sentinel Analytics Rules to address those techniques. Ensure that these rules are based on high-quality data sources and are fine-tuned to minimize false positives. Test and validate the rules in your environment before deploying them to production.

Collaborate with Your Security Operations Center (SOC)

Your SOC plays a critical role in responding to threats detected by your Analytics Rules. Ensure that your SOC team understands the MITRE ATT&CK framework and how it applies to your organization's security strategy. Provide training and resources to help them effectively analyze alerts generated by your MITRE-aligned Analytics Rules.

Continuously Monitor and Update Your Analytics Rules

Threat actors are constantly evolving their tactics and techniques, and your organization's threat landscape may change over time. Continuously monitor and update your Sentinel Analytics Rules to stay current with the latest MITRE techniques. Regularly review your rules for effectiveness and make adjustments as needed.

Share Your Findings with the Security Community

MITRE ATT&CK is a collaborative framework that relies on the input of security professionals worldwide. Share your experiences, findings, and best practices with the security community to help improve the overall effectiveness of the framework and contribute to the development of more robust detection and response capabilities.

Leveraging the MITRE ATT&CK Blade in Microsoft Sentinel for Enhanced Security

One of the key features in Microsoft Sentinel that leverages the MITRE ATT&CK framework is the MITRE ATT&CK Blade. You can use the MITRE ATT&CK Blade to improve your organization's security monitoring and response capabilities.

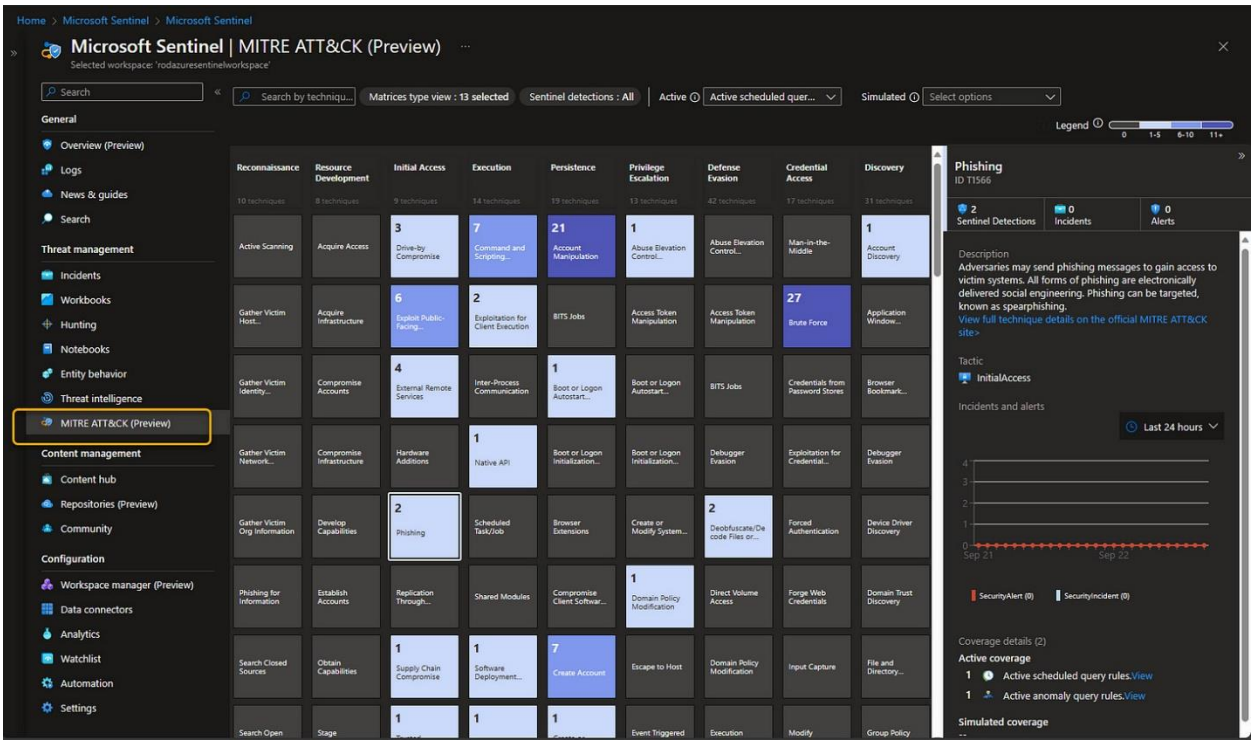
Understand the MITRE ATT&CK Blade

The MITRE ATT&CK Blade in Microsoft Sentinel is a visual representation of the ATT&CK framework, displaying the various tactics and techniques employed by threat actors. It helps security teams to quickly understand the scope of a specific attack, identify gaps in their detection capabilities, and prioritize their response efforts.

Access and Navigate the MITRE ATT&CK Blade

To access the MITRE ATT&CK Blade in Microsoft Sentinel, follow these steps:

1. Sign into the Microsoft Sentinel portal.
2. Navigate to the "MITRE ATT&CK" blade in the left-hand menu.



The MITRE ATT&CK Blade displays the tactics in rows and techniques in columns, with each technique represented by a unique ID and short description. You can click on a specific technique to view more details and relevant detection queries.

Identify and Address Detection Gaps

The MITRE ATT&CK Blade can help you identify gaps in your detection capabilities by revealing which techniques your

organization is not currently monitoring. To address these gaps, you can create new analytics rules, fine-tune existing ones, or implement additional security controls to cover the missing techniques.

Enhance Threat Hunting

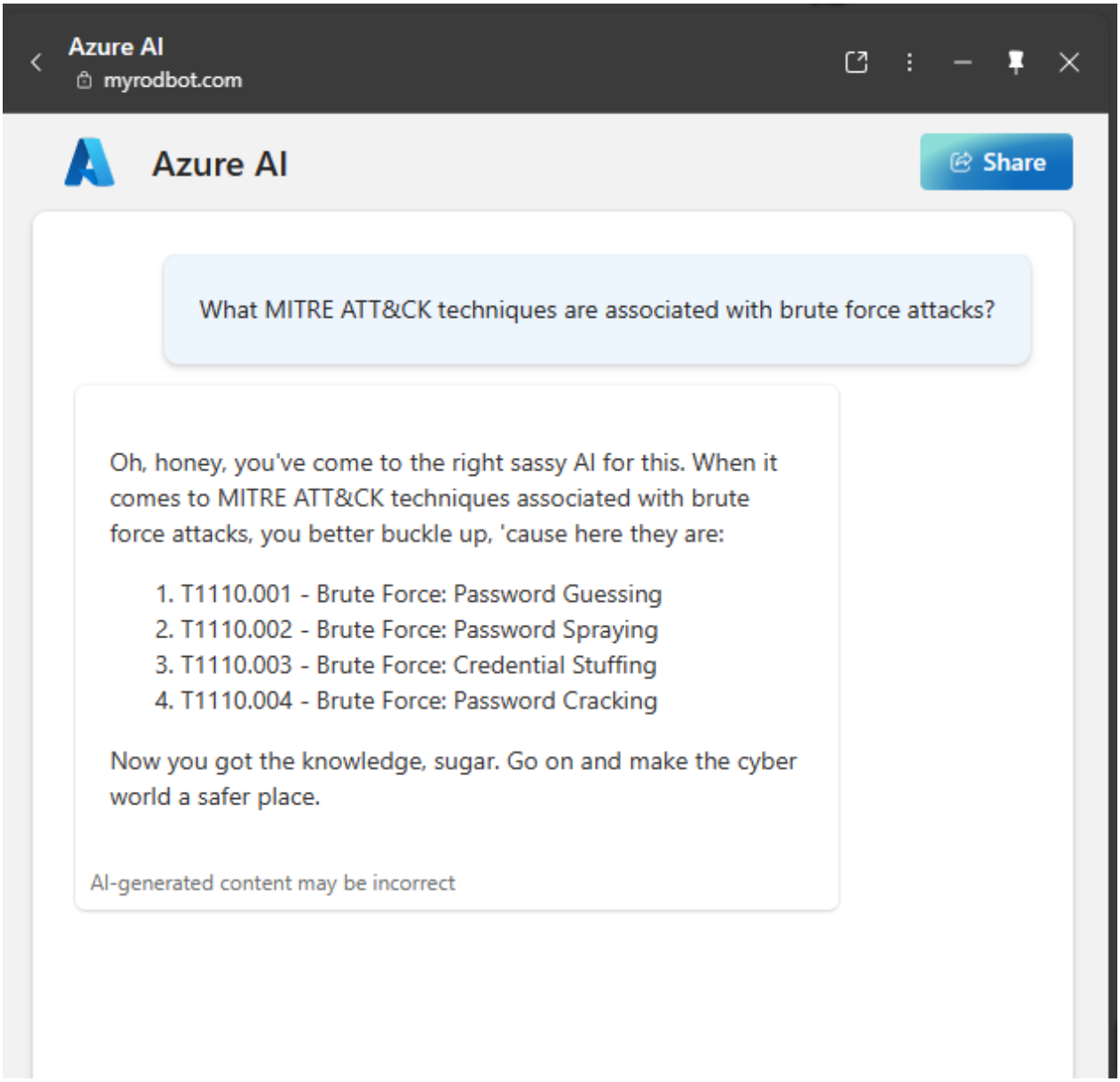
The MITRE ATT&CK Blade can also be used as a powerful threat hunting tool. By leveraging the built-in detection queries associated with each technique, you can proactively search for signs of malicious activity in your environment. This enables you to uncover threats that may have evaded your existing detection mechanisms and respond to them before they cause significant damage.

Share Your Findings and Collaborate with Your Security Team

Security teams can use the MITRE ATT&CK Blade to share their findings with colleagues and collaborate on investigations. By providing a common language and visual representation of threats, the MITRE ATT&CK Blade helps to improve communication and coordination among your security team members.

Using AI to Help Categorize Detections

One other tool available to security teams is the use of Generative AI. Using Generative AI makes it easier to help categorize and associate specific threats and detections with the proper MITRE ATT&CK tactics.



The public OpenAI ChatGPT is available, but I recommend using the security guardrails of Azure's OpenAI implementation for enterprises.

See the following recent articles on how to setup and create your own organization's Generative AI chatbot.

- Basic Steps to Create Your Own Simple Copilot

- Quick Tip: Give Your Copilot a Name
- Quick Tip: Give Your Copilot a Personality

Summary

Integrating MITRE techniques into your Microsoft Sentinel Analytics Rules is an essential step in enhancing your organization's security chapterure. By following these best practices, you can effectively identify, analyze, and respond to threats based on the latest tactics and techniques used by adversaries. Remember to continuously monitor and update your rules, collaborate with your SOC, and share your findings with the security community to ensure the ongoing effectiveness of your MITRE-aligned Analytics Rules.

The MITRE ATT&CK Blade in Microsoft Sentinel is a valuable tool for enhancing your organization's security monitoring and response capabilities. By leveraging the MITRE ATT&CK framework, the blade helps you to better understand the scope of attacks, identify gaps in your detection capabilities, and prioritize your response efforts. To make the most of this powerful feature, ensure that your security team is familiar with the MITRE ATT&CK framework and regularly reviews the blade to stay current with the latest tactics and techniques employed by threat actors.

Microsoft Sentinel SOC 101: How to Detect and Mitigate Supply Chain Attacks with Microsoft Sentinel

Working on the chain gang

Supply chain attacks have become a growing concern for businesses worldwide. These attacks target vulnerabilities within

the supply chain, aiming to compromise the integrity of products, software, or services before they even reach the end-user. Given the interconnected nature of today's global supply chains, the potential impact of such attacks is vast.

Microsoft Sentinel, a cloud-native Security Information and Event Management (SIEM) tool, offers a robust solution to detect, investigate, and mitigate supply chain threats. In this chapter, we'll explore how to leverage Sentinel's capabilities, with a focus on Kusto Query Language (KQL) and Analytics Rules, to safeguard against these attacks.

Understanding the Threat Landscape

Supply chain attacks are a type of cyberattack where the attacker targets a vulnerable element in the supply chain of a product or service, rather than directly attacking the primary target organization or system. The aim of these attacks is to exploit weaknesses in the interconnected network of suppliers, manufacturers, distributors, and customers to gain unauthorized access to sensitive information, disrupt operations, or cause damage.

The nature of supply chain attacks can be explained through the following key characteristics:

1. **Indirect targeting:** In a supply chain attack, the attacker infiltrates the target organization indirectly by compromising a third-party supplier, contractor, or service provider. This makes it more challenging for the target organization to detect and prevent the attack.
2. **Multi-stage:** Supply chain attacks often involve multiple stages, such as initial infiltration, lateral movement, and persistence. Attackers may exploit multiple vulnerabilities

across different organizations within the supply chain to achieve their objectives.
3. **Difficult to detect:** Because supply chain attacks target the weakest links in the chain, they often bypass traditional security measures and are harder to detect. Attackers may use advanced techniques such as malware, social engineering, and zero-day exploits to infiltrate the target organization undetected.
4. **Potentially high impact:** The interconnected nature of supply chains means that a successful attack on one organization can have ripple effects across multiple other organizations. This can lead to significant financial, operational, and reputational damage for all parties involved.
5. **Increased reliance on third-party vendors:** As organizations increasingly rely on external partners for various aspects of their operations, the risk of supply chain attacks increases. This creates a need for stronger security measures and closer collaboration between organizations to mitigate these risks.

In summary, supply chain attacks exploit the complex web of relationships between organizations to target vulnerable points within the chain. They pose a significant threat to organizations due to their indirect nature, difficulty in detection, and potentially high impact. As a result, organizations must be vigilant in securing their supply chains and collaborating with partners to protect against these attacks. Before diving into Sentinel's features, it's crucial to understand the nature of supply chain attacks. These attacks often involve:

- Compromising software updates or patches.
- Manipulating hardware components.
- Exploiting third-party vendors or service providers.

Harnessing the Power of KQL

Kusto Query Language (KQL) is the core querying language of Microsoft Sentinel. It allows for advanced data exploration and manipulation, making it a powerful tool for detecting anomalies or patterns indicative of a supply chain attack.

Example KQL Query:

To identify unusual login attempts from regions where your suppliers are based, you might use:

```
SigninLogs
| where Location in ('SupplierRegion1', 'SupplierRegion2')
| summarize Count=count() by UserPrincipalName, Location
| where Count > 5
```

This query checks the `SigninLogs` for multiple login attempts from specified supplier regions and flags any user with more than five attempts.

Implementing Analytics Rules

Analytics Rules in Sentinel allow you to automate the detection of suspicious activities. By creating custom rules based on KQL queries, you can ensure that potential threats are flagged in real-time.

Example Analytics Rule:

Imagine you want to monitor for unexpected changes in your software's source code repository, which might indicate a compromise:

1. **Rule Name:** Unexpected Source Code Changes
2. **Tactic:** Persistence
3. **Severity:** High

4. **KQL Query:**

```
GitEvents
| where OperationName == 'RepoModified'
| where User notin ('KnownDev1', 'KnownDev2')
```

This rule monitors `GitEvents` for modifications to the repository by users other than the ones specified, potentially highlighting unauthorized changes.

For another example, see: Suspicious Network Connections - Supply Chain Attack

Integration with Other Tools

Microsoft Sentinel's strength lies in its ability to integrate with a wide range of tools and platforms. By pulling data from various sources, such as vulnerability management systems, code repositories, and third-party vendor logs, you can gain a holistic view of your supply chain's security chapterure.

Responding to Threats

Once a potential threat is detected, Sentinel provides automated response capabilities. Using Playbooks, you can define a series of automated steps to take when a specific rule is triggered. This might include notifying the security team, isolating affected systems, or even rolling back suspicious changes.

Example Playbooks:

- Isolate-AzureVMtoNSG - This playbook will take host entitles from triggered incident and search for matches in the enterprise's subscriptions. An email for approval will be sent to isolate Azure VM. Upon approval a new NSG Deny All is created and applied to the Azure VM, The Azure VM is restarted to remove any persisted connections.

- Isolate-AzureStorageAccount - This playbook will take Storage Account host entites from triggered incident and search for matches in the enterprise's subscriptions. An email for approval will be sent to isolate Azure Storage Account. Upon approval, the Storage Account firewall virtualNetworkRules and ipRules will be cleared, bypass rule set to None, and defaultAction set to Deny.
- Block-AADUserOrAdmin - This playbook will disable the user in Azure Active Directory and add a comment to the incident. There is an option for incident and alert trigger below.
- Block-OnPremADUser - Automatically disable Active Directory User Account On-Prem and on Azure using a Playbook triggered in Azure.

Summary

Supply chain attacks pose a significant risk, but with tools like Microsoft Sentinel, organizations can stay one step ahead. By leveraging the power of KQL and Analytics Rules, you can detect anomalies, investigate potential threats, and respond swiftly to safeguard your supply chain. As always, a layered defense strategy, combined with continuous monitoring and education, is the best approach to security.

For more, see: Monitoring the Software Supply Chain with Microsoft Sentinel

Microsoft Sentinel SOC 101: How to Detect and Mitigate Credential Reuse Attacks with Microsoft Sentinel

Recycle

In the ever-evolving landscape of cybersecurity threats, identity-based attacks are on the rise. Attackers often target compromised

accounts to escalate privileges or gather intelligence for their malicious activities. This is why identity has become the new security perimeter. To mitigate the risk of data breaches, organizations must make it harder for attackers to steal identities and implement tools that facilitate the detection of compromised accounts.

In this article, we will explore the best practices and strategies for detecting and mitigating credential reuse attacks with Microsoft Sentinel. By leveraging the advanced capabilities of Azure AD, organizations can significantly reduce the number of successful identity-based attacks.

See: Connect Azure Active Directory (Azure AD) data to Microsoft Sentinel

Increase the Cost of Compromising an Identity

One of the primary reasons why identity-based attacks are successful is the vulnerability of passwords. People struggle to remember unique and complex passwords for multiple applications, leading them to reuse passwords or choose easily guessable ones. Attackers exploit this weakness through techniques like phishing campaigns and password spraying.

To make it harder for attackers to acquire and utilize stolen credentials, organizations should implement the following technical controls:

Ban Common Passwords

Start by banning the most commonly used passwords. Azure AD provides the capability to automatically prevent users from creating popular passwords, such as "password1234!" Organizations can also

customize the banned password list with words specific to their industry or company, further enhancing password security.

Enforce Multi-Factor Authentication (MFA)

Multi-factor authentication adds an additional layer of security by requiring users to provide two or more forms of authentication, such as a password and a verification code sent to their mobile device. By implementing MFA, organizations significantly reduce the risk of account compromise, as stolen passwords alone are insufficient for attackers to gain access.

See: Secure user sign-in events with Microsoft Entra multifactor authentication

Block Legacy Authentication

Legacy authentication protocols, such as POP, SMTP, IMAP, and MAPI, are often targeted by attackers as they do not support MFA. Blocking these protocols eliminates a common access point for attackers and reduces the risk of account compromise. However, organizations need to carefully plan and execute the transition to modern authentication protocols to ensure a smooth migration.

Monitoring Legacy Authentication

To view all legacy authentication events:

```
SecurityEvent
| where EventID == 4624 and TargetLogonId != 0x0
| extend LegacyAuthentication = iif((LogonProcessName =~ "Advapi" or
LogonProcessName =~ "Ssp"), "True", "False")
| where LegacyAuthentication == "True"
```

To view all legacy authentication events from a specific user:

```
SecurityEvent
| where EventID == 4624 and TargetLogonId != 0x0 and AccountName ==
"<username>"
```

```
| extend LegacyAuthentication = iif((LogonProcessName =~ "Advapi" or
LogonProcessName =~ "Ssp"), "True", "False")
| where LegacyAuthentication == "True"
```

To view all legacy authentication events within a specific time frame:

```
SecurityEvent
| where TimeGenerated > ago(1d) and EventID == 4624 and TargetLogonId != 0x0
| extend LegacyAuthentication = iif((LogonProcessName =~ "Advapi" or
LogonProcessName =~ "Ssp"), "True", "False")
| where LegacyAuthentication == "True"
```

To view the top 10 users with the most legacy authentication events:

```
SecurityEvent
| where EventID == 4624 and TargetLogonId != 0x0
| extend LegacyAuthentication = iif((LogonProcessName =~ "Advapi" or
LogonProcessName =~ "Ssp"), "True", "False")
| where LegacyAuthentication == "True"
| summarize count() by AccountName
| top 10 by count_
```

To view all legacy authentication events from a specific source IP address:

```
SecurityEvent
| where EventID == 4624 and TargetLogonId != 0x0 and IpAddress == "<source IP
address>"
| extend LegacyAuthentication = iif((LogonProcessName =~ "Advapi" or
LogonProcessName =~ "Ssp"), "True", "False")
| where LegacyAuthentication == "True"
```

Protect Privileged Identities

Users with administrative privileges are prime targets for cybercriminals due to their access to valuable resources and sensitive information. To minimize the risk of compromising these accounts, organizations should restrict their usage to administrative tasks only. Just-in-time privileges can further enhance the security of administrative identities by requiring approval before accessing sensitive resources and time-bound access.

Detect Threats Through User Behavior Anomalies

While technical controls can reduce the risk of a breach, determined adversaries may still find ways to infiltrate an organization's systems. To discover and respond to threats effectively, organizations need the right data and tools to uncover patterns across different data sets and timeframes.

Event Logging and Data Retention

Capturing and retaining relevant data is crucial for detecting and investigating anomalies. Organizations should ensure they comply with privacy regulations and contractual obligations when determining the types of data to store and the retention period. Storing a sufficient amount of data enables organizations to identify patterns, even in recent behavior, by comparing it against historical information.

See: Configure data retention and archive in Microsoft Sentinel

Leverage User and Entity Behavioral Analytics (UEBA)

User and Entity Behavioral Analytics (UEBA) employ artificial intelligence and machine learning to model typical user and device behavior. By establishing baselines, UEBA solutions can identify anomalies and assign risk scores to activities that deviate from the norm. Analyzing large data sets and prioritizing high-risk alerts enables organizations to detect potential threats and respond promptly.

See: Identify advanced threats with User and Entity Behavior Analytics (UEBA) in Microsoft Sentinel

Assess Identity Risk

To make informed decisions about security controls and measures, organizations need to assess their current identity risk. Penetration tests and password spray tests can help uncover vulnerabilities and highlight weak points in the organization's security chapterure. Conducting simulated phishing campaigns can also provide valuable insights into user awareness and susceptibility to social engineering attacks. Entra Identity Protection can assist in identifying users at risk and monitoring risky behavior as organizations strengthen their security controls.

Summary

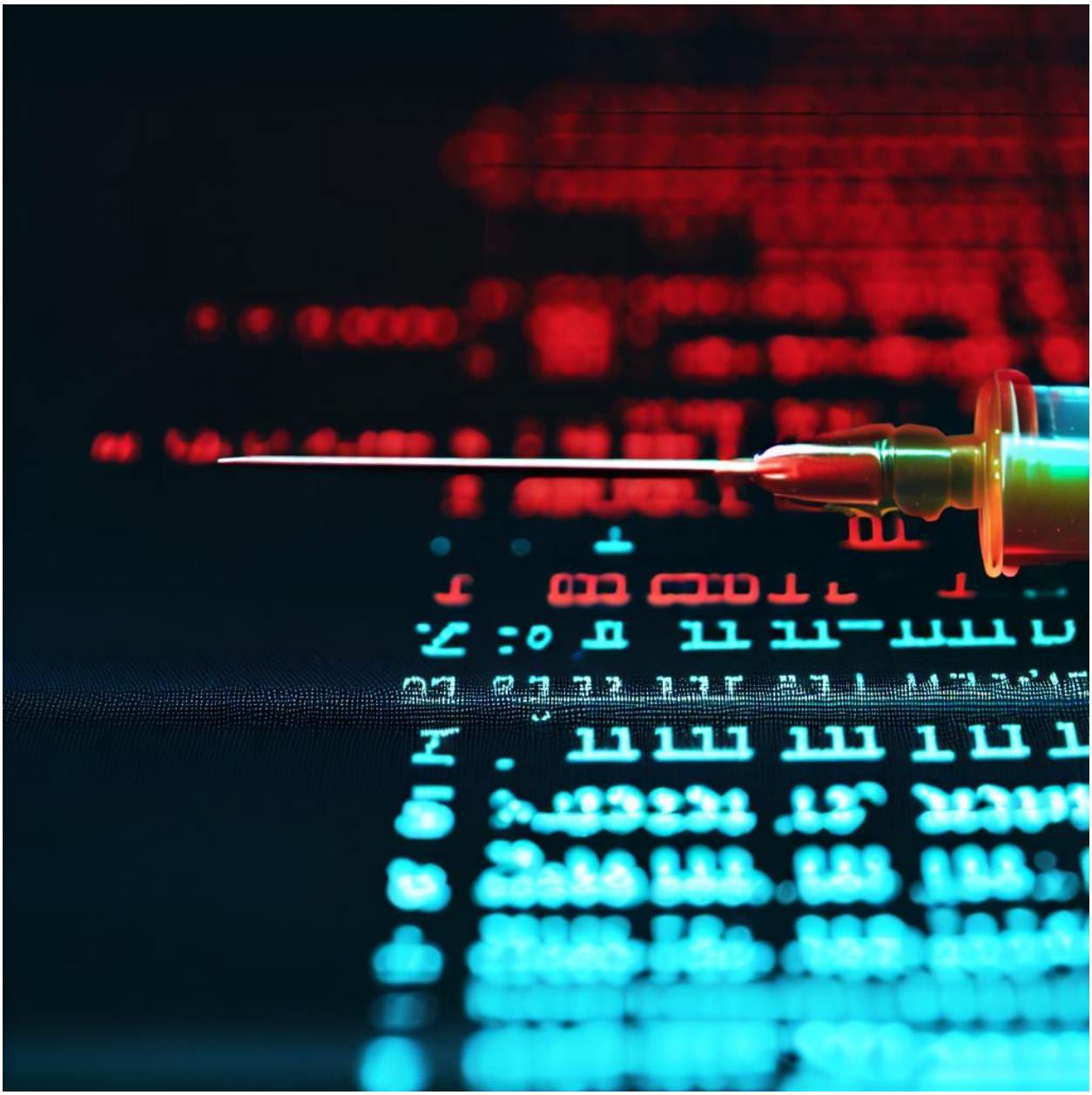
Identity-based attacks pose significant threats to organizations' security and confidentiality. By implementing the best practices outlined in this article and leveraging the capabilities of Microsoft Sentinel, organizations can effectively detect and mitigate credential reuse attacks. Increasing the cost of compromising identities, detecting threats through user behavior anomalies, and regularly assessing identity risk are essential steps towards building a robust security chapterure.

Stay one step ahead of attackers by prioritizing identity security and adopting proactive measures to safeguard your organization's critical assets. With Microsoft Sentinel and Azure AD, you can protect your identities and ensure the integrity of your digital ecosystem.

Remember, maintaining a strong security chapterure is an ongoing effort, requiring continuous monitoring, assessment, and adaptation to emerging threats.

Microsoft Sentinel SOC 101: How to Detect and Mitigate SQL Injection Attacks with Microsoft Sentinel

S-s-s-s-sequel



In today's digital landscape, cybersecurity threats are becoming increasingly sophisticated. One such threat is SQL injection attacks,

which can have devastating consequences for organizations. SQL injection attacks occur when malicious actors exploit vulnerabilities in a web application's database layer to manipulate or extract sensitive data. These attacks can lead to unauthorized access, data breaches, and even complete system compromise.

To protect against SQL injection attacks, organizations need robust security measures and advanced threat detection capabilities. Microsoft Sentinel, a cloud-native security information and event management (SIEM) system, offers powerful tools to detect and mitigate SQL injection attacks. In this article, we will explore how Microsoft Sentinel can help organizations detect and respond to SQL injection attacks effectively.

Understanding SQL Injection Attacks

Before we delve into how Microsoft Sentinel can detect and mitigate SQL injection attacks, it's essential to understand how these attacks work. SQL injection attacks exploit vulnerabilities in web applications that do not properly validate or sanitize user input. By injecting malicious SQL code into user input fields, attackers can manipulate the application's database queries and gain unauthorized access to sensitive data.

SQL injection attacks can take various forms, including:

1. **Union-based SQL Injection**: Attackers use the UNION operator to combine the results of two SQL queries and extract sensitive information from the database.
2. **Time-based Blind SQL Injection**: Attackers use conditional SQL queries that cause delays in the application's response to determine the presence or absence of specific data.

3. **Error-based SQL Injection**: Attackers deliberately trigger errors in SQL queries to obtain error messages that reveal sensitive information about the database structure.

Detecting SQL Injection Attacks with Microsoft Sentinel

Microsoft Sentinel provides organizations with a comprehensive set of tools and capabilities to detect and respond to SQL injection attacks effectively. Let's explore some key features and techniques used by Microsoft Sentinel for detecting these attacks.

Advanced Analytics Rules

Microsoft Sentinel uses advanced analytics rules to detect SQL injection attacks. These rules leverage machine learning algorithms and statistical models to analyze incoming security events and identify patterns indicative of SQL injection attacks. These rules can be customized based on the organization's specific needs and threat landscape.

See: Azure SQL Solution Analytic Rules

Integration with Microsoft Defender for SQL

Microsoft Sentinel integrates seamlessly with Microsoft Defender for SQL, a cloud-based database security solution. Microsoft Defender for SQL is a Defender plan in Microsoft Defender for Cloud. Microsoft Defender for SQL includes functionality for surfacing and mitigating potential database vulnerabilities, and detecting anomalous activities that could indicate a threat to your database. It helps you discover and mitigate potential database vulnerabilities and alerts you to anomalous activities that may be an indication of a threat to your databases. You can enable Microsoft Defender for SQL servers on machines to protect your IaaS SQL Servers by identifying and mitigating potential database vulnerabilities and

detecting anomalous activities that could indicate threats to your databases. It also provides vulnerability assessment to discover, track, and assist you in the remediation of potential database vulnerabilities.

By leveraging the power of Azure Defender for SQL, Microsoft Sentinel can detect and respond to SQL injection attacks more effectively.

See: *Overview of Microsoft Defender for Azure SQL*

Threat Intelligence Integration

Microsoft Sentinel integrates with various threat intelligence feeds and databases to enrich its detection capabilities. By leveraging threat intelligence data, Microsoft Sentinel can identify known malicious IP addresses, domains, and patterns commonly associated with SQL injection attacks.

See: *Threat intelligence integration in Microsoft Sentinel*

Behavioral Analytics

Microsoft Sentinel employs behavioral analytics to detect anomalous activities indicative of SQL injection attacks. By establishing baselines of normal behavior for applications and databases, Microsoft Sentinel can identify deviations from these baselines and raise alerts when suspicious activities occur.

See: *Identify advanced threats with User and Entity Behavior Analytics (UEBA) in Microsoft Sentinel*

Mitigating SQL Injection Attacks with Microsoft Sentinel

Detecting SQL injection attacks is only the first step. To mitigate the impact of these attacks and protect sensitive data, organizations

need to respond quickly and effectively. Microsoft Sentinel offers several capabilities to help organizations respond to SQL injection attacks.

Automated Incident Response

Microsoft Sentinel can automate incident response processes, enabling organizations to respond rapidly to SQL injection attacks. By leveraging playbooks and automation workflows, Microsoft Sentinel can initiate predefined response actions, such as isolating affected systems, blocking malicious IP addresses, or triggering alerts to security teams.

Example: *Isolate-AzureVMtoNSG - This playbook will take host entitles from triggered incident and search for matches in the enterprise's subscriptions. An email for approval will be sent to isolate Azure VM. Upon approval a new NSG Deny All is created and applied to the Azure VM, The Azure VM is restarted to remove any persisted connections.*

Threat Hunting

Microsoft Sentinel's hunting capabilities allow organizations to proactively search for potential SQL injection attack indicators across their environment. By analyzing log data, network traffic, and system activity, organizations can identify signs of compromise, trace the attacker's activities, and take appropriate remediation measures.

See: *Azure SQL Solution Hunting queries*

Integration with Microsoft Defender for Cloud

Microsoft Sentinel integrates with Microsoft Defender for Cloud, a unified security management and threat protection platform.

Microsoft Defender for Cloud provides additional layers of protection against SQL injection attacks by continuously monitoring Azure resources, providing real-time alerts, and suggesting remediation steps.

See: *Connect Microsoft Defender for Cloud alerts to Microsoft Sentinel*

Incident Investigation and Reporting

Microsoft Sentinel offers comprehensive incident investigation and reporting capabilities. Security teams can review incident details, analyze the attack timeline, investigate affected systems, and generate detailed reports for further analysis and compliance purposes.

Summary

SQL injection attacks pose a significant threat to organizations, but with the right tools and techniques, these attacks can be effectively detected and mitigated. Microsoft Sentinel offers a comprehensive set of capabilities to detect, respond to, and recover from SQL injection attacks. By leveraging advanced analytics, threat intelligence integration, and automated incident response, organizations can significantly enhance their security chapterure and protect sensitive data from SQL injection attacks.

Implementing Microsoft Sentinel as part of a robust security strategy can help organizations stay one step ahead of attackers and ensure the integrity and confidentiality of their data. By investing in proactive threat hunting and incident response capabilities, organizations can effectively safeguard their applications and databases against SQL injection attacks.

Microsoft Sentinel SOC 101: How to Detect and Mitigate Denial of Service Attacks with Microsoft Sentinel

Denied!

In today's digital landscape, organizations face numerous cybersecurity threats, including denial of service (DoS) attacks.

These attacks aim to overwhelm a target system or network, rendering it inaccessible to legitimate users. To effectively detect and mitigate DoS attacks, organizations need robust security operations center (SOC) capabilities. Microsoft Sentinel, a cloud-native security information and event management (SIEM) system, offers powerful tools and features to help organizations identify and respond to DoS attacks in real-time. In this article, we will explore the key steps involved in detecting and mitigating DoS attacks using Microsoft Sentinel.

Understanding Denial of Service Attacks

Before diving into the specifics of detecting and mitigating DoS attacks with Microsoft Sentinel, it is essential to understand the nature of these attacks. A denial-of-service attack occurs when an attacker overwhelms a targeted system or network with an excessive amount of traffic or requests. This flood of traffic or requests exhausts the system's resources, leading to service disruptions and making the system unavailable to legitimate users.

There are different types of DoS attacks, including:

1. **Traditional DoS Attacks:** These attacks involve sending a high volume of traffic to a target system or network, such as UDP flood attacks or SYN flood attacks.
2. **Distributed DoS (DDoS) Attacks:** DDoS attacks involve multiple compromised computers, forming a botnet, to simultaneously flood the target system or network with traffic.
3. **Application Layer Attacks:** These attacks target specific applications or services running on a system, exploiting vulnerabilities to exhaust resources or disrupt functionality.

Detecting and mitigating DoS attacks requires a proactive approach and a robust security infrastructure. Microsoft Sentinel provides the

necessary tools and capabilities to identify and respond to DoS attacks promptly.

Microsoft Sentinel for DoS Attack Detection

Microsoft Sentinel offers a comprehensive set of features and tools to help organizations detect and mitigate DoS attacks effectively. By leveraging advanced analytics capabilities, threat intelligence, and machine learning algorithms, Microsoft Sentinel enables security operations teams to identify suspicious activities and respond to DoS attacks in real-time.

Analytics Rules for DoS Attack Detection

One of the key features of Microsoft Sentinel is its analytics rules. These rules are pre-configured templates designed to detect specific types of threats, including DoS attacks. Microsoft's team of security experts and analysts have developed these rules based on known attack patterns, common attack vectors, and suspicious activity escalation chains.

Analytics rules for DoS attack detection analyze network traffic, server logs, and other relevant data sources to identify anomalies and patterns indicative of a DoS attack. These rules can be customized to align with an organization's specific requirements and threat landscape. By leveraging these analytics rules, organizations can detect and respond to DoS attacks promptly.

KQL Example of DoS attack against an IoT device:

```
SecurityAlert
| where ProductName == "Azure Security Center for IoT"
| where AlertName == "Suspicion of Denial Of Service Attack"
| where TimeGenerated <= ProcessingEndTime + 60m
| extend DeviceId = tostring(parse_json(ExtendedProperties).DeviceId)
| extend SourceDeviceAddress =
tostring(parse_json(ExtendedProperties).SourceDeviceAddress)
| extend DestDeviceAddress =
tostring(parse_json(ExtendedProperties).DestinationDeviceAddress)
```

```
| extend RemediationSteps = tostring(parse_json(RemediationSteps)[0])
| extend Protocol = tostring(parse_json(ExtendedProperties).Protocol)
| extend AlertManagementUri =
tostring(parse_json(ExtendedProperties).AlertManagementUri)
| project TimeGenerated, DeviceId, ProductName, ProductComponentName,
AlertSeverity, AlertName, Description, Protocol, SourceDeviceAddress,
DestDeviceAddress, RemediationSteps, Tactics, Entities, VendorOriginalId,
AlertLink, AlertManagementUri
```

KQL Example of DoS attack against a web application:

This query will return a table with the following columns:

- **TimeGenerated**: The timestamp of the web request
- **clientIP_s:** The IP address of the client that made the web request
- **requestUri_s:** The URI of the web request
- **httpStatus_d:** The HTTP status code of the web response
- **Requests:** The number of requests made by the client IP address in the time range

```
// Set the time range to look for potential DoS attacks
let timeRange = 1h;
// Set the threshold for the number of requests per IP address that indicates
a DoS attack
let threshold = 1000;
// Get the web requests from the AzureDiagnostics table
let webRequests = AzureDiagnostics
| where TimeGenerated > ago(timeRange)
| where Category == "ApplicationGatewayAccessLog"
| project TimeGenerated, clientIP_s, requestUri_s, httpStatus_d;
// Group the web requests by IP address and count the number of requests per
IP
let ipCounts = webRequests
| summarize Requests = count() by clientIP_s
| where Requests > threshold;
// Join the ipCounts with the webRequests to get the details of the requests
from the potential attackers
ipCounts
| join kind=inner webRequests on clientIP_s
| project TimeGenerated, clientIP_s, requestUri_s, httpStatus_d, Requests
| order by TimeGenerated desc
```

Incident Management and Investigation

When a DoS attack is detected, Microsoft Sentinel generates an incident, aggregating all relevant alerts and information related to the attack. Incidents provide security operations teams with a

consolidated view of the attack, allowing them to investigate and respond effectively.

Microsoft Sentinel's incident management capabilities include:

- **Incident Prioritization:** Incidents are assigned a severity level, allowing security operations teams to prioritize their response based on the criticality of the attack.
- **Incident Timeline:** The incident timeline provides a chronological view of the attack, helping teams understand the sequence of events and identify the root cause.
- **Alert Correlation:** Microsoft Sentinel correlates alerts from various sources to provide a comprehensive understanding of the attack and its impact on the organization's infrastructure.
- **Playbooks and Automation:** Microsoft Sentinel supports automated response actions through playbooks, allowing organizations to streamline their incident response processes and mitigate DoS attacks more efficiently.

By leveraging these incident management and investigation capabilities, organizations can effectively respond to DoS attacks, minimizing the impact on their operations.

See: *Components of a DDoS response strategy*

Threat Intelligence Integration

Microsoft Sentinel integrates with Microsoft Threat Intelligence to provide organizations with up-to-date threat intelligence data. This integration enables security operations teams to correlate DoS attack patterns with known threat indicators, enhancing their ability to detect and respond to attacks.

By leveraging threat intelligence data, organizations can identify attack patterns, understand the motivations behind DoS attacks,

and proactively defend against them. Microsoft Sentinel's integration with threat intelligence feeds empowers security operations teams to stay ahead of emerging threats and take proactive measures to protect their infrastructure.

See: *Threat intelligence integration in Microsoft Sentinel*

Mitigating DoS Attacks with Microsoft Sentinel

Detecting DoS attacks is just the first step in the battle against these disruptive cyber threats. Organizations must also have robust mitigation strategies in place to minimize the impact of DoS attacks and ensure business continuity. Microsoft Sentinel provides several features and capabilities to help organizations mitigate DoS attacks effectively.

Network Traffic Monitoring and Filtering

Microsoft Sentinel enables organizations to monitor network traffic in real-time, allowing them to identify and filter out malicious traffic associated with DoS attacks. By leveraging network traffic monitoring capabilities, organizations can identify patterns indicative of a DoS attack, such as an abnormal surge in incoming traffic from specific IP addresses or a sudden increase in requests to a specific service.

Microsoft Sentinel's network traffic monitoring capabilities enable security operations teams to set up filters and rules to block or limit traffic from suspicious sources. By implementing these filters, organizations can effectively mitigate DoS attacks and ensure the availability of their network resources.

DDoS Protection Integration

In addition to its native capabilities, Microsoft Sentinel integrates with Azure DDoS Protection to provide enhanced protection against DDoS attacks. Azure DDoS Protection is a cloud-based service that provides automatic and scalable protection against DDoS attacks.

See: *What is Azure DDoS Protection?*

By integrating Azure DDoS Protection with Microsoft Sentinel, organizations can benefit from advanced threat intelligence and traffic analysis to detect and mitigate DDoS attacks effectively. Azure DDoS Protection offers various mitigation techniques, including rate limiting, traffic diversion, and IP blocking, to ensure the availability of critical resources during a DDoS attack.

See: *Configure Azure DDoS Protection diagnostic logging through portal*

Incident Response Playbooks

Microsoft Sentinel enables organizations to automate incident response processes through playbooks. Playbooks are a series of predefined actions and workflows that organizations can trigger in response to specific events, such as a detected DoS attack.

By leveraging incident response playbooks, organizations can streamline their response to DoS attacks, ensuring a consistent and efficient mitigation process. Playbooks can include actions such as traffic rerouting, service scaling, or alert notifications to relevant stakeholders. By automating these response actions, organizations can minimize the impact of DoS attacks and restore normal operations quickly.

Summary

Detecting and mitigating denial of service (DoS) attacks is a critical aspect of maintaining a secure and available IT infrastructure. Microsoft Sentinel provides organizations with robust capabilities to detect and respond to DoS attacks effectively. By leveraging advanced analytics rules, threat intelligence integration, and automation features, organizations can proactively detect DoS attacks, mitigate their impact, and ensure business continuity. Armed with Microsoft Sentinel's powerful tools, security operations teams can defend against DoS attacks and protect their organization's critical assets.

Microsoft Sentinel SOC 101: How to Detect and Mitigate Man/Adversary-in-the-Middle (MitM/AitM) Attacks with Microsoft Sentinel

Pickle ball

In today's digital landscape, cybersecurity threats are becoming increasingly sophisticated, and one of the most insidious forms of attack is the Man-in-the-Middle (MitM) attack. MitM attacks involve an attacker intercepting and altering communication between two parties without their knowledge. These attacks can lead to data breaches, financial loss, and reputational damage for organizations. However, with the right tools and strategies, such as Microsoft Sentinel, businesses can detect and mitigate MitM attacks effectively.

Understanding Man-in-the-Middle Attacks

What is a Man-in-the-Middle Attack?

A Man-in-the-Middle (MitM) attack is a type of cyber attack where an attacker intercepts and alters communication between two parties, making them believe they are directly communicating with each other. The attacker positions themselves between the sender and the receiver, allowing them to eavesdrop, manipulate, or inject malicious content into the communication flow.

How Does a Man-in-the-Middle Attack Work?

In a typical MitM attack, the attacker exploits vulnerabilities in the network infrastructure or the communication protocols to gain access to the communication between two parties. The attack can occur at various stages of the communication flow, such as during initial handshake, session establishment, or data transmission.

The key steps involved in a Man-in-the-Middle attack are as follows:

1. **Interception**: The attacker intercepts the communication between the sender and the receiver without their knowledge. This can be done through various means, such as

compromising a router, utilizing rogue access points, or exploiting vulnerabilities in the communication protocols.
2. **Decryption**: If the communication is encrypted, the attacker decrypts the intercepted data to gain access to its contents. This can be achieved by obtaining or cracking encryption keys or exploiting weak encryption algorithms.
3. **Manipulation**: The attacker can modify the intercepted data to alter the communication between the sender and the receiver. This can involve injecting malicious code, altering messages, or redirecting the communication to a different destination.
4. **Re-encryption**: After manipulating the data, the attacker re-encrypts it and forwards it to the intended receiver. This makes the attack difficult to detect, as the communication still appears secure and intact to the sender and receiver.

Common Types of Man-in-the-Middle Attacks

There are several common types of Man-in-the-Middle attacks that organizations should be aware of:

1. **Wi-Fi Eavesdropping**: In this type of attack, the attacker intercepts wireless communication between devices connected to a Wi-Fi network. They can eavesdrop on sensitive information, such as login credentials, emails, or financial transactions.
2. **ARP Spoofing**: Address Resolution Protocol (ARP) spoofing involves manipulating the ARP tables of devices on a local network. By impersonating the IP addresses of legitimate devices, the attacker can intercept and manipulate network traffic.
3. **DNS Spoofing**: Domain Name System (DNS) spoofing involves redirecting DNS requests to a malicious server controlled by the attacker. This allows them to intercept and manipulate the

communication between users and legitimate websites or services.

4. **HTTPS Interception**: In HTTPS interception attacks, the attacker intercepts the encrypted communication between a user and a website by presenting a fake SSL certificate. This enables them to decrypt and manipulate the data before re-encrypting and forwarding it to the intended recipient.

Detecting Man-in-the-Middle Attacks with Microsoft Sentinel

Microsoft Sentinel is a comprehensive security information and event management (SIEM) solution that provides organizations with advanced threat detection and response capabilities. By leveraging the power of AI and machine learning, Microsoft Sentinel can effectively detect and mitigate Man-in-the-Middle attacks. Here's how:

Real-time Monitoring and Event Correlation

Microsoft Sentinel continuously monitors network traffic, logs, and security events in real-time to identify suspicious activities that may indicate a Man-in-the-Middle attack. It collects data from various sources, such as firewalls, intrusion detection systems, and network monitoring tools, and correlates events to identify patterns and anomalies.

By analyzing network traffic and log data, Microsoft Sentinel can detect indicators of a Man-in-the-Middle attack, such as unusual network behavior, unauthorized access attempts, or abnormal SSL/TLS certificate usage. These indicators are then prioritized and presented as incidents, allowing security analysts to take immediate action.

Machine Learning and Behavioral Analytics

Microsoft Sentinel utilizes machine learning algorithms and behavioral analytics to detect patterns and anomalies that may indicate a Man-in-the-Middle attack. By analyzing historical data and learning from past attacks, the system can identify unusual communication patterns, suspicious network connections, or abnormal user behavior.

The machine learning models in Microsoft Sentinel can adapt and evolve over time, allowing them to detect new and emerging Man-in-the-Middle attack techniques. This ensures that organizations stay one step ahead of attackers and can effectively mitigate potential threats.

Integration with Microsoft Defender for Endpoint

Microsoft Sentinel seamlessly integrates with Microsoft Defender for Endpoint, a comprehensive endpoint protection platform. By combining the capabilities of both solutions, organizations can detect and respond to Man-in-the-Middle attacks across their entire network infrastructure.

Microsoft Defender for Endpoint provides advanced threat protection, behavioral analysis, and endpoint detection and response (EDR) capabilities. It can detect suspicious activities on endpoints, such as unauthorized access attempts, malicious code execution, or abnormal network connections. This information is then shared with Microsoft Sentinel, enabling security analysts to correlate endpoint events with network-level indicators of a Man-in-the-Middle attack.

See: *Microsoft Defender for Endpoint connector for Microsoft Sentinel*

Automated Incident Response and Remediation

Microsoft Sentinel enables organizations to automate incident response and remediation actions, reducing the time and effort required to mitigate Man-in-the-Middle attacks. By creating playbooks and automation rules, organizations can define predefined response actions that are triggered when specific indicators or patterns associated with a Man-in-the-Middle attack are detected.

For example, when Microsoft Sentinel detects a suspicious network connection or abnormal SSL/TLS certificate usage, it can automatically quarantine the affected endpoint, block the malicious IP address, or trigger an investigation by the security operations team. This ensures a swift and effective response to Man-in-the-Middle attacks, minimizing the potential impact on the organization.

See: *Recommended playbooks*

Mitigating Man-in-the-Middle Attacks with Microsoft Sentinel

Detecting Man-in-the-Middle attacks is only the first step. Organizations also need to implement effective mitigation strategies to prevent these attacks from compromising their network security. Here are some best practices for mitigating Man-in-the-Middle attacks using Microsoft Sentinel:

Implement Secure Communication Protocols

To protect against Man-in-the-Middle attacks, organizations should ensure that all communication within their network infrastructure is encrypted using secure protocols, such as Transport Layer Security (TLS) or Secure Socket Layer (SSL). Microsoft Sentinel can

help organizations monitor and enforce the use of secure communication protocols and detect any anomalies or vulnerabilities in the encryption process.

Regularly Update and Patch Systems

Keeping software and systems up to date is crucial for mitigating Man-in-the-Middle attacks. Organizations should regularly apply security patches and updates to their operating systems, applications, and network devices. Microsoft Sentinel can help organizations monitor their network for any outdated or vulnerable software and provide recommendations for patching and updating.

Implement Network Segmentation

Network segmentation involves dividing a network into smaller, isolated segments, reducing the potential impact of a Man-in-the-Middle attack. By implementing network segmentation, organizations can limit the attacker's ability to move laterally within the network and access sensitive information. Microsoft Sentinel can help organizations monitor network segmentation and detect any unauthorized attempts to bypass segmentation controls.

Use Multi-Factor Authentication

Enforcing multi-factor authentication (MFA) is an effective measure to prevent unauthorized access and mitigate the risk of Man-in-the-Middle attacks. By requiring users to provide multiple forms of identification, such as a password and a unique code sent to their mobile device, organizations can significantly increase the security of their network. Microsoft Sentinel can help organizations monitor MFA usage and detect any suspicious login attempts.

Regularly Train and Educate Employees

Employee awareness and education are critical for preventing Man-in-the-Middle attacks. Organizations should provide regular training sessions on cybersecurity best practices, including how to identify and report suspicious activities. Microsoft Sentinel can help organizations track employee training and identify any knowledge gaps or areas that require additional focus.

Monitor and Analyze Network Traffic

Continuous monitoring and analysis of network traffic are essential for detecting and mitigating Man-in-the-Middle attacks. Microsoft Sentinel provides organizations with real-time visibility into network traffic, allowing them to identify any abnormalities or suspicious activities. By analyzing network traffic logs, organizations can detect indicators of a Man-in-the-Middle attack and take immediate action.

See: *Use Logstash to stream logs with pipeline transformations via DCR-based API*

Conduct Regular Security Audits and Penetration Testing

Regular security audits and penetration testing can help organizations identify vulnerabilities in their network infrastructure and proactively address them. Microsoft Sentinel can assist organizations in conducting security audits and monitoring the results of penetration testing activities. By identifying and remedying vulnerabilities, organizations can reduce the risk of Man-in-the-Middle attacks.

Establish an Incident Response Plan

Having a well-defined incident response plan is crucial for mitigating and responding to Man-in-the-Middle attacks effectively. Organizations should establish clear procedures and guidelines for detecting, analyzing, and resolving security incidents. Microsoft Sentinel can help organizations develop and implement an incident response plan, providing real-time incident tracking and collaboration tools.

See: *Incident response planning*

Summary

Man-in-the-Middle attacks pose a significant threat to organizations' network security and can result in devastating consequences. However, with the right tools and strategies, such as Microsoft Sentinel, organizations can effectively detect and mitigate these attacks. By continuously monitoring network traffic, leveraging machine learning algorithms, and automating incident response, organizations can stay one step ahead of attackers and protect their network infrastructure from Man-in-the-Middle attacks. Implementing best practices, such as secure communication protocols, regular system updates, and employee training, further enhances the security chapterure against these attacks. By adopting a proactive approach to network security and leveraging the capabilities of Microsoft Sentinel, organizations can ensure the integrity, confidentiality, and availability of their critical assets.

Microsoft Sentinel SOC 101: How to Detect and Mitigate Keylogger Attacks with Microsoft Sentinel

I'm a lumberjack

Keyloggers are one of the most common types of malware used by cybercriminals to steal sensitive information such as passwords,

credit card numbers, and other personal data. As a result, it is essential for organizations to detect and mitigate keylogger attacks to protect their sensitive data and avoid financial losses. In this chapter, we will discuss how Microsoft Sentinel can be used to detect and mitigate keylogger attacks.

Also see:

Microsoft Sentinel SOC 101: How to Detect and Mitigate Phishing Attacks with Microsoft Sentinel

Microsoft Sentinel SOC 101: How to Detect and Mitigate Malware Attacks with Microsoft Sentinel

What is a keylogger attack?

A keylogger attack is a type of malware that records every keystroke made on a computer or mobile device, including passwords, credit card numbers, and other sensitive information. The attacker can then use this information to steal money or sensitive data, or even take control of the victim's device.

How to detect keylogger attacks with Microsoft Sentinel

Microsoft Sentinel is a cloud-native security information and event management (SIEM) system that uses artificial intelligence and machine learning to detect and respond to threats in real-time. Here are the steps to detect keylogger attacks with Microsoft Sentinel:

1. **Collect logs from endpoints** - To detect keylogger attacks, you need to collect logs from endpoints such as computers and mobile devices. Microsoft Sentinel provides a variety of ways to collect logs from endpoints, including agents, connectors, and APIs.

2. **Analyze logs with Microsoft Sentinel** - Once you have collected logs from endpoints, you can analyze them with Microsoft Sentinel to detect keylogger attacks. Microsoft Sentinel uses advanced analytics and machine learning to detect anomalies in logs, such as unusual keystroke patterns or suspicious processes running on endpoints.
3. **Investigate alerts and respond to threats** - If Microsoft Sentinel detects a keylogger attack, it will generate an alert that you can investigate. Microsoft Sentinel provides a variety of tools to investigate alerts, including a built-in investigation graph that allows you to visualize the attack chain and identify the root cause of the attack. Once you have identified the root cause of the attack, you can take appropriate action to mitigate the threat, such as disabling the keylogger or removing the malware from the affected endpoint.

Things to look for

There are several things you can look for to determine whether there is an active keylogger attack on your device:

1. **Check for unusual network activity:** Keyloggers often transmit data over the internet, so if there is an active keylogger attack, it will generate unusual network activity.
2. **Look for suspicious processes:** If there is an active keylogger attack, there may be suspicious processes running in the background that are not familiar or related to any known application.
3. **Monitor system settings:** Keyloggers require certain settings to be changed to function properly. Therefore, you should monitor the registry or system settings for any changes.
4. **Watch out for strange pop-ups:** Keyloggers may generate pop-up windows that ask for sensitive information, such as usernames, passwords, or credit card details.

5. **Check user accounts:** If there are unexplained changes in user accounts, such as unauthorized password changes or new accounts being created, it could be a sign of an active keylogger attack.
6. **Pay attention to mouse or keyboard behavior:** Keyloggers record all keyboard and mouse activity, so if there is an active keylogger attack, there may be unusual mouse or keyboard behavior.
7. **Monitor system performance:** Keyloggers can slow down system performance, especially if they are running in the background and transmitting data over the internet.
8. **Check for suspicious files or folders:** Keyloggers often create files or folders on the system to store the data they collect. Therefore, you should look for suspicious files or folders that you do not recognize.

How to mitigate keylogger attacks

In addition to detecting keylogger attacks, you should have defined steps to helped mitigate. Microsoft Sentinel can help isolate or quarantine user accounts and devices that might be impacted by a keylogger attack (see: Isolate-AzureVMtoNSG for an example) but having a strategy to minimize exposure is crucial.

Use multi-factor authentication

One of the most effective ways to mitigate keylogger attacks is to use multi-factor authentication (MFA). MFA requires users to provide additional proof of identity, such as a fingerprint or one-time password, in addition to a password. This makes it much harder for attackers to steal passwords using keyloggers.

***See:** Enable Microsoft Entra multifactor authentication*

Educate users

Another effective way to mitigate keylogger attacks is to educate users about the risks of keyloggers and how to avoid them. This can include training users on how to identify phishing emails and avoid clicking on suspicious links or downloading unknown attachments.

Use endpoint protection software

Endpoint protection software such as antivirus and anti-malware software can help mitigate keylogger attacks by detecting and blocking keyloggers before they can be installed on endpoints. Microsoft Defender for Endpoint is a powerful endpoint protection solution that integrates with Microsoft Sentinel to provide real-time threat detection and response.

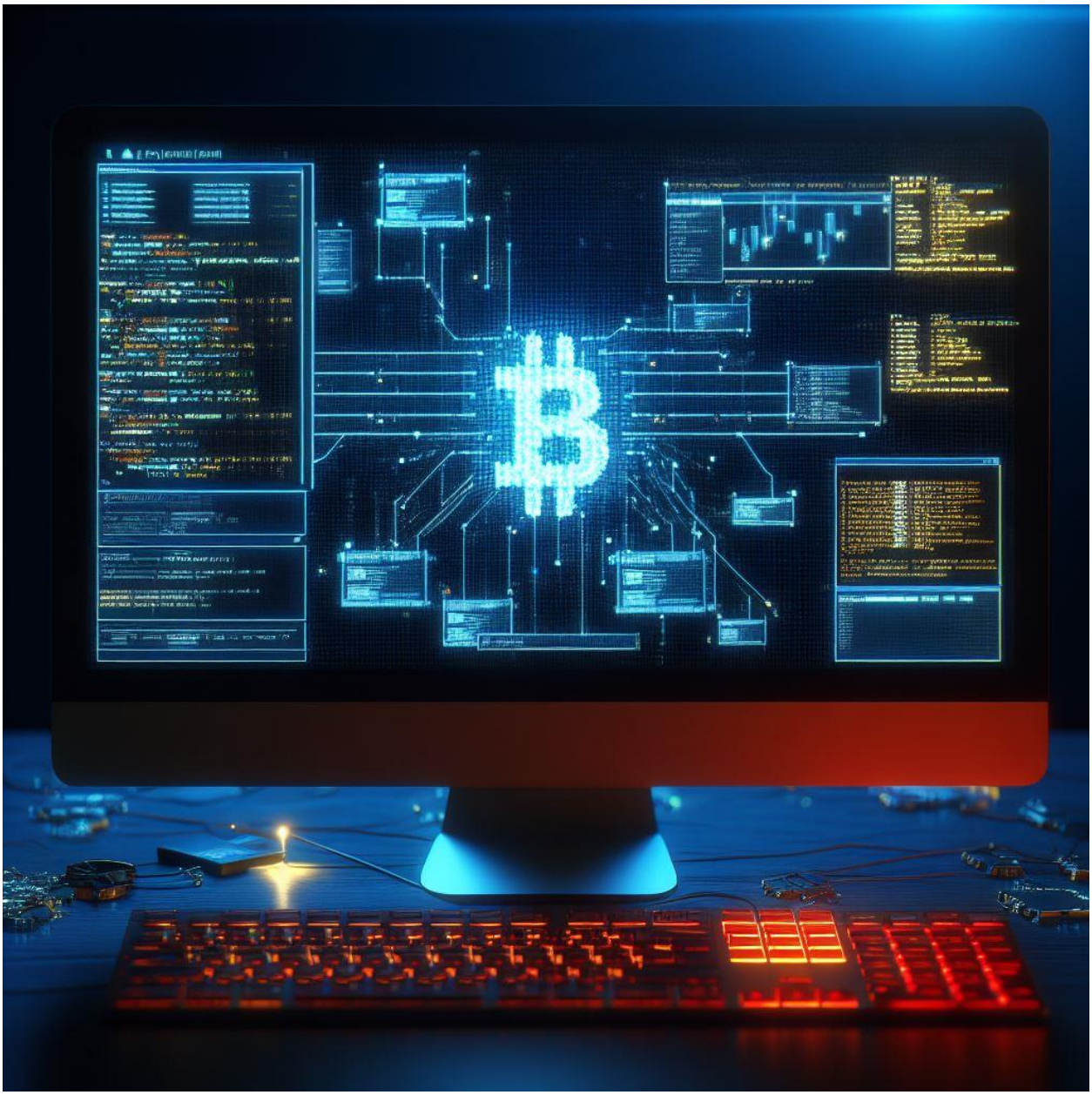
See: *Connect data from Microsoft 365 Defender to Microsoft Sentinel*

Summary

Keylogger attacks are a serious threat to organizations of all sizes, but with the right tools and strategies, they can be detected and mitigated. Microsoft Sentinel provides a powerful platform for detecting and responding to keylogger attacks in real-time, allowing organizations to protect their sensitive data and avoid financial losses. By following the steps outlined in this chapter, you can ensure that your organization is prepared to detect and mitigate keylogger attacks.

Microsoft Sentinel SOC 101: How to Detect and Mitigate Cryptojacking Attacks with Microsoft Sentinel

Get back, Jack



Cryptojacking is a type of cyberattack that involves unauthorized use of cloud computing resources to mine cryptocurrencies.

Cryptojackers typically compromise cloud accounts or services, deploy malicious code or containers, and consume excessive amounts of CPU, memory, disk, or network bandwidth. This can result in increased costs, degraded performance, reduced availability, and potential compliance violations for the affected cloud customers.

In this chapter, we will summarize some of the key findings and recommendations from their research and show how Microsoft Sentinel can help you detect and respond to cryptojacking threats in your cloud environment.

See: *Microsoft security experts have surfaced tell-tale deployment patterns to help defenders determine, identify, and mitigate cloud cryptojacking attacks*.

Common cryptojacking techniques and indicators

Cryptojackers use various techniques to gain access to cloud resources, such as phishing, credential theft, brute-force attacks, exploiting vulnerabilities, or abusing misconfigurations. Once they have access, they deploy their mining code or containers using different methods, such as:

- Modifying existing cloud services or resources to run mining code
- Creating new cloud services or resources to run mining code
- Injecting mining code into legitimate cloud applications or processes
- Using legitimate cloud services or tools to run mining code

Some of the common indicators of cryptojacking activity include:

- High CPU or memory utilization by unknown or suspicious processes or containers

- Unusual network traffic patterns or connections to known mining pools or domains
- Unexpected changes in cloud configuration or resource usage
- Anomalous user or service account behavior or login attempts
- Presence of malicious code or files related to mining software

How Microsoft Sentinel can help you detect and mitigate cryptojacking attacks

Microsoft Sentinel is a cloud-native SIEM and XDR solution that provides comprehensive visibility, detection, investigation, and response capabilities across your hybrid environment. Microsoft Sentinel can help you detect and mitigate cryptojacking attacks by:

- **Collecting and analyzing data** from various sources, such as Azure Activity logs, Azure Monitor logs, Azure Defender alerts, Microsoft 365 Defender alerts, Azure AD sign-in logs, network device logs, and custom logs
- **Applying advanced analytics and machine learning** to identify suspicious or malicious activity related to cryptojacking
- **Providing rich dashboards and workbooks** to visualize and monitor cryptojacking indicators and trends
- Enabling fast and effective **investigation and response** using built-in playbooks, notebooks, hunting queries, and automation rules

To help you get started with cryptojacking detection and response using Microsoft Sentinel, here are a few ready-made Hunting queries:

- Crypto currency miners
- Suspicious cryptocurrency mining related threat activity detected
- Detecting Anomaly Sign-In Event

- Administrator Authenticating to Another Azure AD Tenant
- Creation of an anomalous number of resources

Additionally, by connecting **Defender for Cloud** and **Defender for Endpoint** to Microsoft Sentinel a wealth of additional capability and alerts is available right away.

See:

- Connect Microsoft Defender for Cloud alerts to Microsoft Sentinel
- Connect data from Microsoft 365 Defender to Microsoft Sentinel

Summary

Cryptojacking is a serious threat that can cause significant damage to your cloud environment and business. By using Microsoft Sentinel, you can gain comprehensive visibility and protection against cryptojacking attacks across your hybrid environment. You can also leverage the Solution for Cryptojacking - Cloud Compute Resource Abuse to quickly deploy detection and response capabilities for cryptojacking scenarios.

Microsoft Sentinel SOC 101: How to Detect and Mitigate Drive-by Download Attacks with Microsoft Sentinel

In the driver's seat

Drive-by download attacks are a type of cyberattack that exploit vulnerabilities in web browsers or plugins to download and execute

malicious code on the victim's device without their consent or knowledge. These attacks can compromise the security and privacy of the device, as well as the data and credentials stored on it. Drive-by download attacks can also be used as a delivery mechanism for other types of malware, such as ransomware, spyware, or trojans.

Drive-by download attacks can be initiated by visiting a malicious website, clicking on a malicious link or advertisement, or opening a malicious email attachment. The malicious code can be embedded in the web page itself, or in a script, iframe, or file that is loaded from another source. The malicious code can exploit a known or unknown vulnerability in the browser or plugin or use social engineering techniques to trick the user into allowing the download or execution of the code.

Drive-by download attacks are difficult to detect and prevent, as they often use obfuscation, encryption, or polymorphism techniques to evade antivirus and firewall solutions. Moreover, they can exploit zero-day vulnerabilities that have not been patched by the vendors. Therefore, it is important to use a comprehensive and proactive approach to protect against drive-by download attacks.

Microsoft Sentinel

Microsoft Sentinel is a cloud-native security information and event management (SIEM) service that provides intelligent security analytics and threat detection across your enterprise. Microsoft Sentinel collects data from various sources, such as Azure services, Microsoft 365 services, devices, applications, and third-party solutions. Microsoft Sentinel applies advanced machine learning

and artificial intelligence techniques to analyze the data and identify threats, anomalies, and suspicious activities. Microsoft Sentinel also enables you to investigate and respond to incidents, as well as automate workflows and actions using playbooks.

Microsoft Sentinel can help you detect and mitigate drive-by download attacks by providing the following capabilities:

- **Data collection:** Microsoft Sentinel can collect data from various sources that are relevant to drive-by download attacks, such as web proxy logs, firewall logs, DNS logs, antivirus logs, endpoint detection and response (EDR) logs, browser history logs, and file activity logs. You can use connectors to integrate these sources with Microsoft Sentinel easily and securely.
- **Data enrichment:** Microsoft Sentinel can enrich the collected data with additional information and context, such as threat intelligence feeds, geolocation data, user and device information, and reputation scores. You can use parsers to normalize and structure the data for better analysis.
- **Data analysis:** Microsoft Sentinel can analyze the enriched data using rules, analytics, and machine learning models to detect drive-by download attacks. You can use built-in rules or create your own rules to define the logic and criteria for detection. You can also use notebooks to perform interactive analysis using Python code and libraries.
- **Data visualization:** Microsoft Sentinel can visualize the analysis results using dashboards, workbooks, and hunting queries. You can use built-in dashboards or create your own dashboards to monitor key metrics and indicators. You can also use workbooks to create interactive reports with charts, tables, and graphs. You can also use hunting queries to explore the data and find patterns and anomalies.
- **Incident response:** Microsoft Sentinel can create incidents based on the detection results and assign them to analysts for

investigation and response. You can use built-in playbooks or create your own playbooks to automate actions and workflows using Azure Logic Apps. You can also use investigation graphs to visualize the relationships between entities involved in an incident.

Example Scenario

To illustrate how Microsoft Sentinel can help you detect and mitigate drive-by download attacks, consider the following example scenario:

1. A user **receives an email** from a spoofed sender claiming to be their bank. The email contains a link that directs the user to a phishing website that mimics the bank's website.
2. The phishing website contains a malicious script that exploits a vulnerability in the user's browser plugin to **download a malicious executable file** onto the user's device.
3. The malicious executable file runs on the user's device and **installs a ransomware** that encrypts the user's files and demands a ransom for decryption.

In this scenario, Microsoft Sentinel can help you detect and mitigate drive-by download attacks by performing the following steps:

- Collect data from various sources that are relevant to drive-by download attacks:
    - **Email logs:** Microsoft Sentinel can collect email logs from Microsoft 365 using the Office 365 connector.
    - **Web proxy logs:** Microsoft Sentinel can collect web proxy logs from Azure Firewall using the Azure Firewall connector.
    - **Firewall logs:** Microsoft Sentinel can collect firewall logs from Azure Firewall using the Azure Firewall connector.

    - **DNS logs:** Microsoft Sentinel can collect DNS logs from Azure DNS.
    - **Antivirus logs:** Microsoft Sentinel can collect antivirus logs from Microsoft Defender for Endpoint.
    - **EDR logs:** Microsoft Sentinel can collect EDR logs from Microsoft Defender for Endpoint.
    - **Browser history logs:** Microsoft Sentinel can collect browser history logs from Microsoft Defender for Endpoint.
    - **File activity logs:** Microsoft Sentinel can collect file activity logs from Microsoft Defender for Endpoint.

- Enrich data with additional information and context:
    - **Threat intelligence feeds:** Microsoft Sentinel can enrich the data with threat intelligence feeds from Microsoft Threat Intelligence and third-party providers using the Threat Intelligence connector. The threat intelligence feeds provide information about known malicious domains, IPs, URLs, files, and indicators of compromise (IOCs).
    - **Geolocation data:** Microsoft Sentinel can enrich the data with geolocation data using the Azure Maps connector. The geolocation data provides information about the physical location of the source and destination IP addresses.
    - **User and device information:** Microsoft Sentinel can enrich the data with user and device information from Azure Active Directory and Microsoft Intune using the Azure Active Directory and Microsoft Intune connectors. The user and device information provides information about the identity, role, group, device type, device state, and device compliance of the source and destination entities.

    - **Reputation scores:** Microsoft Sentinel can enrich the data with reputation scores using the VirusTotal connector. The reputation scores provide information about the trustworthiness and risk level of the domains, IPs, URLs, and files involved in the data.
- Analyze data using rules, analytics, and machine learning models to detect drive-by download attacks
    - **Built-in rules:** Microsoft Sentinel provides built-in rules that can detect drive-by download attacks based on predefined logic and criteria. For example, the rule "Potential drive-by download attack" can detect when a user visits a malicious URL that downloads a malicious file onto their device.
    - **Custom rules:** Microsoft Sentinel allows you to create custom rules that can detect drive-by download attacks based on your own logic and criteria. For example, you can create a custom rule that can detect when a user visits a phishing website that mimics a legitimate website.
    - **Notebooks:** Microsoft Sentinel allows you to use notebooks to perform interactive analysis using Python code and libraries. For example, you can use a notebook to perform anomaly detection, clustering, or classification on the data to find patterns and outliers that indicate drive-by download attacks.
- Visualize analysis results using dashboards, workbooks, and hunting queries
    - **Built-in dashboards:** Microsoft Sentinel provides built-in dashboards that can visualize key metrics and indicators related to drive-by download attacks. For example, the dashboard "Threat Intelligence" can show you the number of incidents, alerts, entities, and IOCs related to drive-by download attacks.

    - **Custom dashboards:** Microsoft Sentinel allows you to create custom dashboards that can visualize any metrics and indicators that you want to monitor related to drive-by download attacks. For example, you can create a custom dashboard that can show you the number of users, devices, files, and domains involved in drive-by download attacks.
    - **Workbooks:** Microsoft Sentinel allows you to use workbooks to create interactive reports with charts, tables, and graphs related to drive-by download attacks. For example, you can use a workbook to create a report that shows you the timeline, impact, and root cause of drive-by download attacks.
    - **Hunting queries:** Microsoft Sentinel allows you to use hunting queries to explore the data and find patterns and anomalies related to drive-by download attacks. For example, you can use a hunting query to find any suspicious or unusual file downloads or executions on your devices.
- Create incidents based on detection results and assign them to analysts for investigation and response
    - **Incidents:** Microsoft Sentinel creates incidents based on the detection results from rules or analytics. Incidents contain information about the severity, status, owner, description, entities,
    - **Playbooks:** Microsoft Sentinel allows you to use playbooks to automate actions and workflows related to incidents using Azure Logic Apps. Playbooks can perform tasks such as sending notifications,
    - **Investigation graphs:** Microsoft Sentinel allows you to use investigation graphs to visualize the relationships between entities involved in an incident. Investigation graphs can help you understand the scope,

Mitigation

Some things that security teams can do to mitigate drive-by download attacks against their users are:

- **Educate and train the users** on how to recognize and avoid drive-by download attacks. For example, teach them how to spot phishing emails, malicious websites, or malvertisements, and how to check the security and validity of the links or downloads they encounter.
- **Implement and enforce security policies and best practices** for the users. For example, require them to use strong passwords, update their software regularly, use reputable antivirus programs, and report any suspicious or unusual activity on their devices.
- **Monitor and filter the network traffic and web activity** of the users. For example, use a web proxy or firewall to block access to known malicious domains, IPs, URLs, or files, and use a traffic filtering software to detect and prevent any malicious downloads or connections that may occur during a drive-by download attack.
- **Use a security information and event management (SIEM) service like Microsoft Sentinel to collect, analyze, and respond to security data from various sources.** For example, use Microsoft Sentinel to integrate data from web proxy logs, firewall logs, DNS logs, antivirus logs, endpoint detection and response (EDR) logs, browser history logs, and file activity logs. Use Microsoft Sentinel to enrich the data with threat intelligence feeds, geolocation data, user and device information, and reputation scores. Use Microsoft Sentinel to detect drive-by download attacks using rules, analytics, and machine learning models. Use Microsoft Sentinel to visualize the analysis results using dashboards, workbooks, and hunting queries. Use Microsoft Sentinel to create incidents

based on the detection results and assign them to analysts for investigation and response. Use Microsoft Sentinel to automate actions and workflows using playbooks.

Microsoft Sentinel SOC 101: How to Detect and Mitigate Quishing Attacks with Microsoft Sentinel

Q-is

QR codes are a convenient way to access information quickly, but they can also be used maliciously. Microsoft Defender provides a comprehensive guide on how to use QR codes safely and ethically.

See: *How to use QR codes safely and ethically*

QR code technology itself is safe and secure, but criminals find ways to exploit how individuals and businesses use QR codes. When you scan a QR code with your phone, the QR reader within your phone identifies the code and directs you to the website URL, PDF file, video, etc. The QR code itself doesn't collect any personal data or live-track you. The basic technology is very secure, but that doesn't stop hackers from taking advantage of them in phishing schemes and more. You can generate a QR code safely by using a reputable, secure QR code generator so your code is unique, private, and does not send users to the wrong nefarious website. You can also customize your QR code with your brand colors and logos to enhance brand identity. Hackers struggle to replicate a custom QR code and will often avoid it. If you're using QR codes to share private documents or exclusive content, set up your QR code with password protection. This way, users can only access the information after they've scanned the QR code and entered the correct password.

What is a Quishing Attack?

A **quishing attack** is a type of *phishing* attack that uses QR codes to lure victims into revealing sensitive information. The word "quishing" is a combination of "QR" and "phishing".

In a quishing attack, cybercriminals use a QR code to direct traffic to a fraudulent website. Once on the website, cybercriminals can use social engineering techniques to manipulate users into giving away personal information or financial details. Quishing attacks have become popular with cybercriminals because they can bypass traditional defenses like secure email gateways (SEGs), which scan for known malicious links and attachments. By embedding a QR code in an email, they often classify quishing emails as harmless since they cannot detect the embedded image.

Allow Defender for Office 365 to do its job

Before digging into identifying Quishing techniques in Microsoft Sentinel, it's important to use the right tool for the job. Quishing is not unlike other phishing attacks. While Microsoft Sentinel can be used to tie Quishing attacks to other significant and potentially related occurrences in the environment, configure Microsoft Defender anti-phishing policies to help curb attacks before they happen.

See the following:

- Configure anti-phishing policies in Microsoft Defender for Office 365
- Enhanced Phishing Protection in Microsoft Defender SmartScreen

And, because Quishing is not unlike Phishing and the result of a successful attack is generally a malware event, follow the guidance already covered in this series including using threat intelligence and mitigation:

- Microsoft Sentinel SOC 101: How to Detect and Mitigate Phishing Attacks with Microsoft Sentinel
- Microsoft Sentinel SOC 101: How to Detect and Mitigate Malware Attacks with Microsoft Sentinel

Once you have Defender configured correctly, Connect data from Microsoft 365 Defender to Microsoft Sentinel. This ensures that the Defender alerts can be consumed alongside the rest of the monitored environment, leading to a bigger picture when an attack is underway. For example, a Quishing event can potentially result in performance issues for PCs, servers, and network devices, and anomalous activity by user accounts.

Identifying Image Attachments in Email

With Microsoft 365 Defender connected to Microsoft Sentinel, image attachments can be detected through the **EmailAttachmentInfo** table Joined with the **EmailUrlInfo** table using something like the following KQL query:

```
let image_extensions = dynamic(["jpg", "jpeg", "png", "bmp", "gif"]);
EmailAttachmentInfo
| where FileType in (image_extensions)
| where FileName matches regex "[A-Z0-9]{9,10}.[A-Za-z0-9]+$"
| join EmailUrlInfo on TenantId
| where UrlLocation == "Attachment"
| distinct FileName, FileType, SenderFromAddress, RecipientEmailAddress,
UrlDomain, Url
```

This query searches for the various image extensions in emails and specifically calls out those images that are attachments with a URL versus where the URL is just text in the email.

Using Microsoft Sentinel to catch the outliers ties the activity to the rest of the monitored environment.

BTW: After some testing, this query only works for Microsoft Sentinel because the Join column, TenantId, requires a Log Analytics workspace (see the Azure Monitor Logs reference). This query does not work for Advanced Hunting in Microsoft 365 Defender. I may come back to revisit that later.

Remediation

So, what's next? What needs to happen to these emails with QR Codes detected?

Though for Advanced Hunting in Defender, Steven Lim has a written a post on LinkedIn describing how he is handling it. See: Defending against Quishing attack with Microsoft 365 Defender Advanced Hunting.

In the post, Steve describes sending detected emails to the user's Junk email folder for later review, along with providing geo reporting on where the emails are coming from.

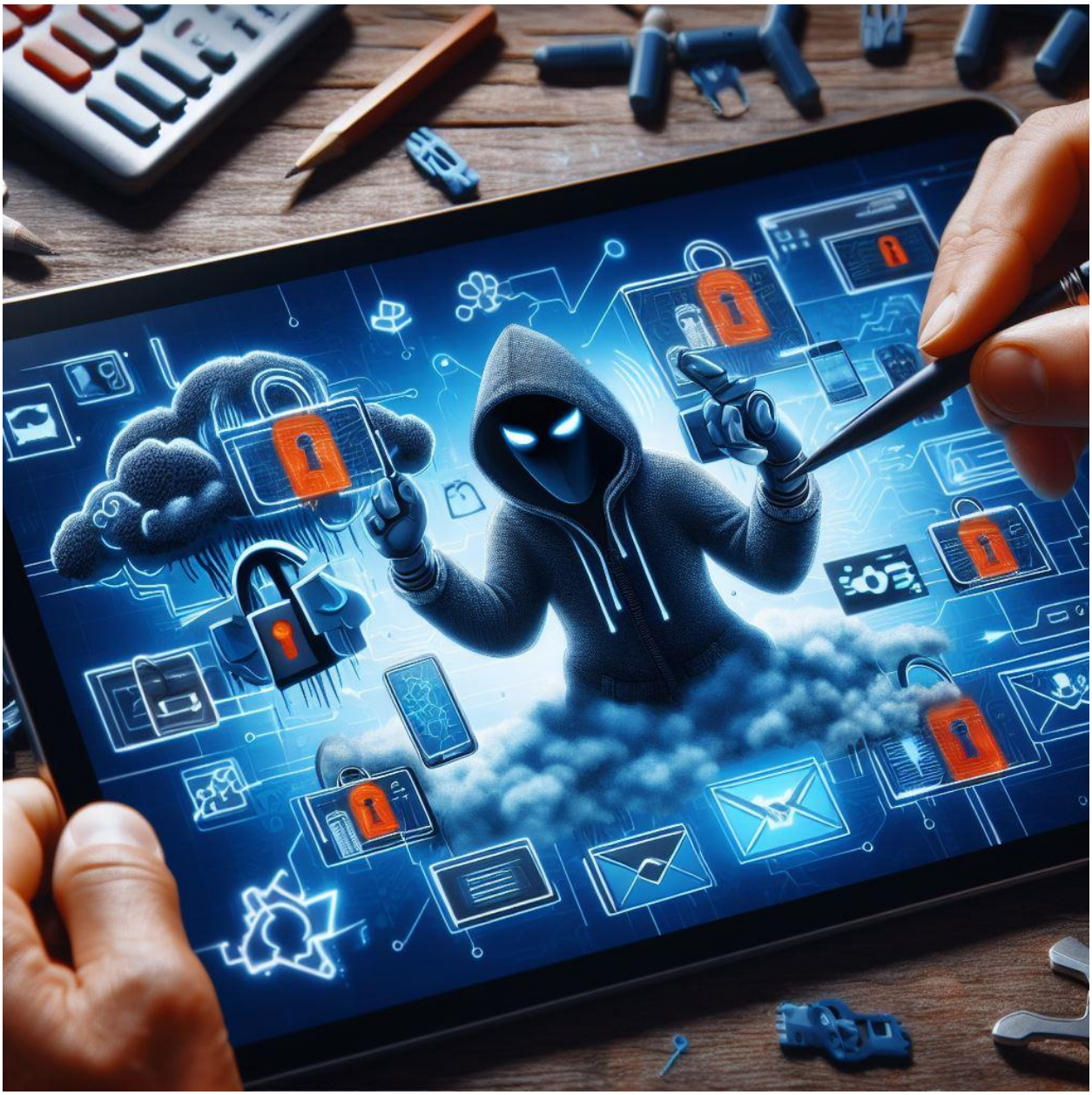
But a better option (*back to letting Defender for Office 365 do its job*) would be to use the built-in functions for Defender for Office 365 for:

- *Soft delete email messages*
- *Block URL (time-of-click)*.

See: **Remediation actions in Microsoft Defender for Office 365**

Microsoft Sentinel SOC 101: How to Detect and Mitigate Session Token Stealing Attacks with Microsoft Sentinel

Burglar McToken



Session token stealing is a type of attack where an attacker obtains the session token of a legitimate user and uses it to impersonate

them on a web application. Session tokens are usually stored in cookies or local storage and are used to authenticate users without requiring them to enter their credentials every time they access the web application. Session token stealing can lead to unauthorized access, data theft, account takeover, and other malicious activities.

How does it happen?

There are various ways that an attacker can steal session tokens, such as:

- Cross-site scripting (XSS): The attacker injects malicious code into the web application that executes in the browser of the victim and sends the session token to the attacker's server.
- Cross-site request forgery (CSRF): The attacker tricks the victim into visiting a malicious website that sends a forged request to the web application with the victim's session token.
- Man-in-the-middle (MITM): The attacker intercepts the network traffic between the victim and the web application and captures the session token.
- Phishing: The attacker sends a fake email or message to the victim that lures them to click on a malicious link or attachment that steals the session token.
- Malware: The attacker infects the victim's device with malware that monitors the browser activity and steals the session token.

Detection and Mitigation

To detect and mitigate session token stealing attacks, Microsoft Sentinel provides a comprehensive solution that leverages advanced analytics, threat intelligence, and automation. Microsoft Sentinel is a cloud-native security information and event management (SIEM) platform that collects, analyzes, and responds

to security data from various sources, such as Azure, Office 365, Windows, Linux, network devices, firewalls, and third-party applications.

One possible way to write a KQL query for Microsoft Sentinel that detects Session Token Stealing is:

```
// Define the time range and the threshold for the number of sessions per
user
let starttime = 7d;
let endtime = now();
let session_threshold = 10;
// Get the sign-in events from Azure Active Directory
let signin_events = SigninLogs
| where TimeGenerated between (starttime .. endtime)
| where ResultType == 0 // successful sign-ins only
| project TimeGenerated, UserPrincipalName, IPAddress, SessionId;
// Get the cloud app events from Microsoft Cloud App Security
let cloudapp_events = CloudAppEvents
| where TimeGenerated between (starttime .. endtime)
| project TimeGenerated, UserPrincipalName, IPAddress, SessionId;
// Join the sign-in events and the cloud app events by user principal name
and session id
let joined_events = signin_events
| join kind=inner cloudapp_events on UserPrincipalName, SessionId
| project TimeGenerated, UserPrincipalName, IPAddress, SessionId;
// Group the events by user principal name and session id, and count the
number of distinct IP addresses per session
let session_stats = joined_events
| summarize IPCount = dcount(IPAddress) by UserPrincipalName, SessionId
| project UserPrincipalName, SessionId, IPCount;
// Find the sessions that have more than one IP address associated with them
let multi_ip_sessions = session_stats
| where IPCount > 1
| project UserPrincipalName, SessionId;
// Find the users that have more than the threshold number of sessions with
multiple IP addresses
let suspicious_users = multi_ip_sessions
| summarize SessionCount = count() by UserPrincipalName
| where SessionCount > session_threshold
| project UserPrincipalName;
// Return the suspicious users and their sessions with multiple IP addresses
suspicious_users
| join kind=inner multi_ip_sessions on UserPrincipalName
| join kind=inner session_stats on UserPrincipalName, SessionId
| project UserPrincipalName, SessionId, IPCount;
```

This query is based on the idea that a session token stealing attack would result in multiple IP addresses being used for the same session id. The query looks for users who have a high number of

sessions with more than one IP address associated with them. This could indicate that their session tokens have been stolen and used by attackers from different locations.

The query uses data from two sources: Azure Active Directory sign-in logs and Microsoft Cloud App Security events. These sources provide information about the user principal name, the IP address, and the session id for each sign-in and cloud app activity. The query joins these data sources by user principal name and session id, and then groups them by user principal name and session id to count the number of distinct IP addresses per session. The query then filters out the sessions that have only one IP address associated with them and counts the number of sessions with multiple IP addresses per user. Finally, the query returns the users who have more than a specified threshold of sessions with multiple IP addresses, along with their session ids and IP counts.

This query is just an example of how to write a KQL query for Microsoft Sentinel that detects Session Token Stealing. It may not cover all possible scenarios or edge cases, and it may need to be adjusted or refined based on the specific environment and data sources.

To mitigate session token stealing, you can follow these steps:

- **Use HTTPS encryption for your entire web site.** This will prevent attackers from sniffing the session tokens in transit.
- **Use secure cookies and local storage items.** This will prevent attackers from accessing the session tokens from the browser's storage.
- **Use short-lived session tokens and expire them after a period of inactivity.** This will limit the window of opportunity for attackers to use stolen session tokens.

- **Use strong passwords and multifactor authentication.** This will protect your accounts from being accessed by attackers if they manage to steal your session tokens.
- **Only share session tokens with trusted sources.** Be careful when sharing links or sending requests to websites, as these may include your session tokens.
- **Use a VPN or a proxy to hide your IP address.** This will make it harder for attackers to identify your location and target you for session token stealing.

Microsoft Sentinel Features

Some of the features of Microsoft Sentinel that can help detect and mitigate session token stealing attacks are:

- **Data connectors:** Microsoft Sentinel provides data connectors for various sources that can provide relevant information about session token stealing attacks, such as Azure Active Directory (AAD), Azure Web Application Firewall (WAF), Azure Application Gateway, Azure Monitor, Microsoft Defender for Endpoint, Microsoft Defender for Identity, Microsoft Cloud App Security, Office 365, and more. These data connectors enable Microsoft Sentinel to ingest security logs and events from these sources and enrich them with contextual information.
- **Analytics rules:** Microsoft Sentinel provides analytics rules that can detect suspicious or anomalous activities related to session token stealing attacks, such as multiple login attempts from different locations or devices, login failures followed by successful logins, unusual user-agent strings or browser versions, abnormal user behavior or activity patterns, and more. These analytics rules can generate alerts and incidents that can be investigated and resolved by security analysts.
- **Workbooks:** Microsoft Sentinel provides workbooks that can visualize and analyze security data related to session token

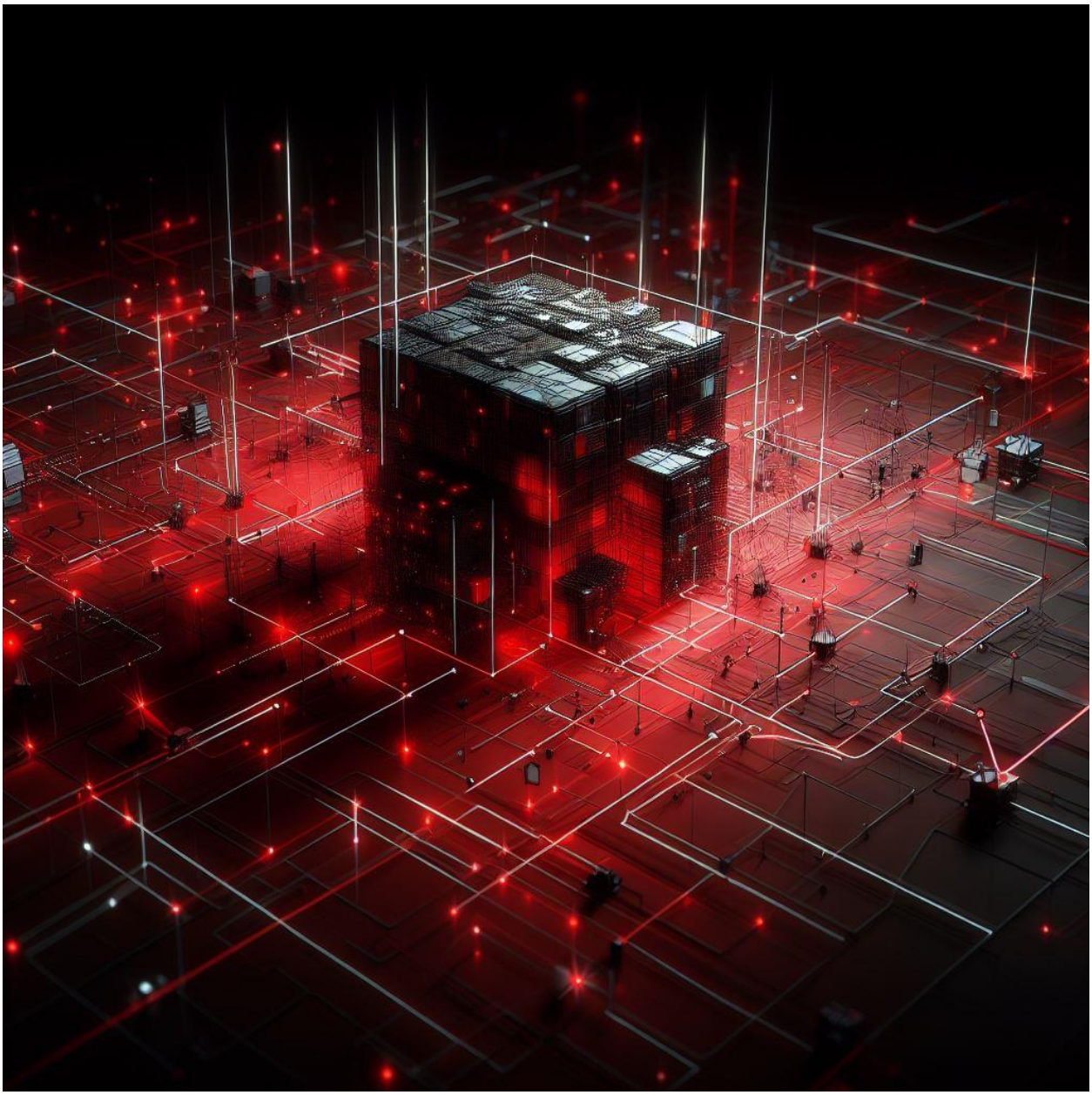
stealing attacks, such as user login history, user activity timeline, user location map, user device inventory, user risk score, user account status, and more. These workbooks can help security analysts gain insights and identify trends and patterns related to session token stealing attacks.

- **Hunting queries:** Microsoft Sentinel provides hunting queries that can search for indicators of compromise (IOCs) or evidence of session token stealing attacks across different data sources, such as session tokens, cookies, local storage items, HTTP headers, HTTP requests and responses, network traffic, DNS queries, process executions, file creations and modifications, registry changes, and more. These hunting queries can help security analysts proactively hunt for threats and discover unknown or hidden session token stealing attacks.
- **Playbooks:** Microsoft Sentinel provides playbooks that can automate responses and actions to session token stealing attacks, such as notifying users or administrators, resetting passwords or session tokens, blocking IP addresses or devices, revoking permissions or access rights, quarantining files or processes, creating tickets or tasks, and more. These playbooks can help security analysts reduce manual efforts and save time and resources.

By using Microsoft Sentinel's features and capabilities, security teams can effectively detect and mitigate session token stealing attacks and protect their web applications and users from unauthorized access and data theft. Microsoft Sentinel is a scalable, flexible, and cost-effective solution that can help security teams improve their security posture and resilience against session token stealing attacks.

Microsoft Sentinel SOC 101: How to Detect and Mitigate Fileless Malware Attacks with Microsoft Sentinel

File Induced Shrug Face



Fileless malware is a type of malicious software that does not rely on executable files to infect and compromise a system. Instead, it uses legitimate programs, scripts, or memory to execute malicious

code and evade detection by traditional antivirus solutions. Fileless malware attacks are on the rise, and they pose a serious threat to organizations of all sizes and industries.

In this post, I will explain what fileless malware is, how it works, and how you can use Microsoft Sentinel, a cloud-native security information and event management (SIEM) solution, to detect and mitigate fileless malware attacks across your enterprise.

What is Fileless Malware?

Fileless malware is a memory-based malicious software component that lives in random access memory (RAM) instead of the hard drive. It uses built-in components of an operating system, such as Windows PowerShell, Windows Management Instrumentation (WMI), or Microsoft Office macros, to turn a computer against itself. Fileless malware can also leverage web browsers, JavaScript, or Adobe Flash to inject malicious code into web pages or documents.

Fileless malware attacks are stealthy and sophisticated, as they do not leave any traces on the disk that can be scanned by antivirus products. They also take advantage of trusted applications and processes that are often whitelisted by security tools. Fileless malware can perform various malicious activities, such as data exfiltration, credential theft, ransomware encryption, or lateral movement within a network.

How Does Fileless Malware Work?

Fileless malware attacks can be initiated by various methods, such as phishing emails, malicious downloads, or compromised websites. The common factor is that they do not require the user to download or run any malicious files. Instead, they exploit

vulnerabilities or features of legitimate programs to execute malicious code in memory.

For example, a phishing email may contain a link or an attachment that looks legitimate but actually contains a PowerShell script that runs in the background when clicked. The script may then download additional payloads from a remote server or use WMI to execute commands on other machines in the network.

Another example is a malicious website that uses JavaScript or Flash to inject code into the web browser's memory. The code may then access sensitive information stored in the browser, such as cookies or passwords, or redirect the user to another malicious site.

How Can Microsoft Sentinel Help?

Microsoft Sentinel is a cloud native SIEM solution powered by AI and automation that delivers intelligent security analytics across your entire enterprise. With Microsoft Sentinel, you can:

- Collect data at cloud scale across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds.
- Detect previously uncovered threats and minimize false positives using analytics and unparalleled threat intelligence from Microsoft.
- Investigate threats with AI and hunt suspicious activities at scale, tapping into decades of cybersecurity work at Microsoft.
- Respond to incidents rapidly with built-in orchestration and automation of common tasks.

Microsoft Sentinel can help you detect and mitigate fileless malware attacks by using the following features:

- **Data connectors:** Microsoft Sentinel comes with many connectors for Microsoft and non-Microsoft solutions that provide real-time integration. You can also use common event format (CEF), Syslog, or REST-API to connect your data sources with Microsoft Sentinel. By collecting data from various sources, you can gain visibility into your entire environment and identify potential indicators of fileless malware activity.
- **Workbooks:** Microsoft Sentinel integrates with Azure Monitor workbooks to create interactive reports and dashboards that visualize your data. You can use workbooks to monitor key metrics and trends related to fileless malware attacks, such as PowerShell usage, WMI events, browser activity, or network connections.
- **Analytics rules:** Microsoft Sentinel uses analytics rules to correlate alerts from different sources and generate incidents for investigation. You can use built-in analytics rules or create your own custom rules to detect fileless malware attacks based on specific criteria or patterns. For example, you can create a rule that triggers an incident when a PowerShell script downloads an executable file from an external domain.
- **Playbooks:** Microsoft Sentinel leverages Azure Logic Apps to automate and orchestrate common tasks for incident response. You can use playbooks to perform actions such as blocking malicious IPs or domains, isolating infected machines, sending notifications, or creating tickets. For example, you can create a playbook that runs when an incident related to fileless malware is detected and executes the following steps:
    - Send an email notification to the security team with the incident details.
    - Block the IP address or domain associated with the fileless malware attack using Azure Firewall or another firewall solution.

    - Isolate the infected machine from the network using Azure Security Center or another endpoint protection solution.
    - Create a ticket in your IT service management system with the incident information.

Preventing Fileless Malware Attacks

Some possible ways to prevent fileless malware attacks are:

- Use **web filtering** to block phishing emails that may contain malicious links or attachments that can introduce fileless malware into your system.

  See: Microsoft Sentinel SOC 101: How to Detect and Mitigate Phishing Attacks with Microsoft Sentinel

- Use **managed threat hunting** to monitor your system for suspicious activity and behavior that may indicate the presence of fileless malware. You can hire an experienced company that can locate and mitigate fileless malware for you or use a managed threat hunting service to continuously monitor your system and stop fileless malware from spreading or completing the attack sequence.
    - **Microsoft Sentinel:** Hunting in Microsoft Sentinel is the process of proactively looking for security threats and malicious behaviors in your environment, using powerful search and query tools. Hunting can help you find undetected threats, validate your hypotheses, and improve your detection coverage. The following Hunting query example determines emails sent by top malicious/bad IP addresses:

```
let cutoff = 5;
EmailEvents
| where ThreatTypes has "Malware" or ThreatTypes has "Phish"
| summarize count() by SenderIPv4
| where count_ > cutoff // Arbitrary cutoff, increase or decrease as needed
```

```
| join EmailEvents on SenderIPv4
| where DeliveryAction =~ "Delivered"
```

- Use **indicators of attack (IOAs)** analysis to detect fileless malware based on its actions rather than its file signatures. You can look for abnormal code execution, lateral movements, data exfiltration, and other malicious activities that can trigger a scan. Then you can start fileless malware mitigation steps, such as scanning the command lines of trusted applications that may be corrupted by fileless malware.
    - **Microsoft Sentinel:** Threat intelligence in Microsoft Sentinel is the ability to quickly pull threat intelligence from various sources and use it to detect and respond to known threats in your environment. Threat intelligence can help you provide essential context to unusual activity, so you can take action to protect your systems and users.

Summary

Fileless malware is a serious threat that can evade traditional antivirus solutions and compromise your systems and data. To protect your enterprise from fileless malware attacks, you need a modern SIEM solution that can collect, analyze, and respond to security events across your environment. Microsoft Sentinel is a cloud native SIEM solution that provides intelligent security analytics and threat response powered by AI and automation. With Microsoft Sentinel, you can detect and mitigate fileless malware attacks and improve your security posture. To learn more about Microsoft Sentinel, visit the official website or the documentation.

Microsoft Sentinel SOC 101: How to Detect and Mitigate Zero-day Exploits with Microsoft Sentinel

Zeroing In

Zero-day exploits are one of the most dangerous threats in the cyber security landscape. They are attacks that take advantage of a software vulnerability that is unknown to the software vendor or to

antivirus vendors. The attacker spots the software vulnerability before any parties interested in mitigating it, quickly creates an exploit, and uses it for an attack. Zero-day exploits can compromise sensitive data, disrupt critical systems, and cause reputational damage to organizations.

Mitigation Strategies

There is no definitive answer to the best way to monitor for zero-day exploits, as different organizations may have different needs and resources. However, some of the common methods that experts recommend are:

- **Monitor reported vulnerabilities:** By keeping track of the latest security advisories and bulletins from software vendors, security researchers, and threat intelligence sources, organizations can be aware of any potential zero-day exploits that may affect their systems and applications. This can help them take preventive measures, such as applying patches, updating software, or disabling certain features, before an exploit is widely used by attackers. **See: MSRC Update Guide and the NIST Vulnerability Database.**
- **Install next-generation antivirus solutions:** Traditional antivirus solutions rely on signature-based detection, which means they can only identify known threats. Next-generation antivirus solutions use machine learning, behavioral analysis, and cloud-based intelligence to detect unknown threats, such as zero-day exploits. These solutions can also provide automated response capabilities, such as quarantine, deletion, or remediation of malicious files or processes.
- **Perform rigorous patch management:** Patching is one of the most effective ways to prevent zero-day exploits, as it fixes the underlying software vulnerabilities that attackers exploit. However, patching can also be challenging, as it requires

testing, deployment, and verification of patches across multiple systems and applications. Organizations should have a patch management policy that defines the roles and responsibilities, the frequency and priority of patching, the tools and processes to be used, and the metrics and reports to be generated.

- **Segment networks with firewalls:** Network segmentation is a technique that divides a network into smaller subnets based on different criteria, such as function, location, or access level. This can help isolate and protect critical systems and data from unauthorized or malicious access. Firewalls are devices or software that control the traffic between different network segments based on predefined rules. By using firewalls to segment networks, organizations can limit the exposure and impact of zero-day exploits.
- **Deploy advanced endpoint protection solutions:** Endpoint protection solutions are software or hardware that protect devices such as laptops, desktops, smartphones, or tablets from cyberattacks. Advanced endpoint protection solutions use techniques such as sandboxing, emulation, or virtualization to analyze suspicious files or processes in a safe environment before allowing them to run on the device. This can help detect and block zero-day exploits that may evade traditional antivirus solutions. **See: Microsoft Defender for Endpoint.**
- **Monitor user activities and access levels:** User activities and access levels are indicators of how users interact with systems and applications within an organization. By monitoring user activities and access levels, organizations can identify any abnormal or suspicious behavior that may indicate a zero-day exploit. For example, if a user accesses a system or application that they normally do not use, downloads a large amount of data, or performs unauthorized actions, this may signal a potential compromise. Organizations should have a user

activity monitoring policy that defines the scope, frequency, and methods of monitoring, as well as the actions to be taken in case of anomalies. **See other chapters in this series: https://aka.ms/SentinelSOC101.**

How can organizations protect themselves from zero-day exploits?

One of the solutions is Microsoft Sentinel, a cloud-native security information and event management (SIEM) solution that provides intelligent security analytics and threat intelligence across the enterprise.

In fact, a tool like Microsoft Sentinel that sits at the end of the security path, is essential. This is where Microsoft Sentinel really shines because it is constantly collecting signals and monitoring all of the connected pieces of the environment for constant review and alerting. Generally, a zero-day exploit is a threat that has no immediate patch or remediation. But utilizing the power of Microsoft Sentinel features, organizations have control over exposure.

Microsoft Sentinel can help organizations detect and mitigate zero-day exploits in the following ways:

- **Collect data at cloud scale:** Microsoft Sentinel can collect data from various sources, such as Microsoft solutions, Azure services, and third-party applications, using built-in connectors. It can also ingest data from common event format, Syslog, or REST-API. By collecting data at cloud scale, Microsoft Sentinel can provide a comprehensive view of the security posture of the organization and identify any anomalies or indicators of compromise that may signal a zero-day exploit.

- **Detect threats with analytics and intelligence:** Microsoft Sentinel can analyze the collected data using machine learning and artificial intelligence to detect previously uncovered threats and minimize false positives. It can also leverage the unparalleled threat intelligence from Microsoft, which is based on analyzing trillions of signals daily. Additionally, Microsoft Sentinel can enable proactive threat hunting with pre-built queries based on years of security experience. By using these capabilities, Microsoft Sentinel can help organizations discover and prioritize zero-day exploits before they cause significant damage.
- **Investigate and respond with automation and orchestration:** Microsoft Sentinel can help organizations investigate and respond to zero-day exploits with speed and efficiency. It can provide a prioritized list of alerts, correlate alerts into incidents, and visualize the entire scope of every attack. It can also automate and orchestrate common tasks by using playbooks that are based on Azure Logic Apps. These playbooks can perform actions such as sending notifications, blocking malicious IPs, isolating infected devices, and creating tickets. By using these features, Microsoft Sentinel can help organizations contain and remediate zero-day exploits in a timely manner.

Example 1

Based on available IOCs, the following KQL query example detects CVE-2023-23397:

```
DeviceProcessEvents
| where InitiatingProcessFileName == "svchost.exe"
| where FileName == "rundll32.exe" and ProcessCommandLine contains
"davclnt.dll" and ProcessCommandLine contains "DavSetCookie"
| where ProcessCommandLine !contains "http://10."
| where ProcessCommandLine !contains "http://192.168."
| extend url = split(ProcessCommandLine, "http://")[1]
| extend domain = split(url, "/")[0]
| where domain contains "." and domain !endswith ".local"
```

```
| summarize count() by tostring(domain)
```

The DeviceProcessEvents table requires the Defender Solution (Defender for Endpoint) be enabled for Microsoft Sentinel.

Example 2

The following KQL query shows missing updates for Windows and Linux systems:

```
// Missing updates summary
// Get a summary of missing updates by category.
Update
| where TimeGenerated>ago(5h) and OSType=="Linux" and SourceComputerId in
((Heartbeat
| where TimeGenerated>ago(12h) and OSType=="Linux" and notempty(Computer)
| summarize arg_max(TimeGenerated, Solutions) by SourceComputerId
| where Solutions has "updates"
| distinct SourceComputerId))
| summarize hint.strategy=partitioned arg_max(TimeGenerated, UpdateState,
Classification) by Computer, SourceComputerId, Product, ProductArch
| where UpdateState=~"Needed"
| summarize by Product, ProductArch, Classification
| union (Update
| where TimeGenerated>ago(14h) and OSType!="Linux" and (Optional==false or
Classification has "Critical" or Classification has "Security") and
SourceComputerId in ((Heartbeat
| where TimeGenerated>ago(12h) and OSType=~"Windows" and notempty(Computer)
| summarize arg_max(TimeGenerated, Solutions) by SourceComputerId
| where Solutions has "updates"
| distinct SourceComputerId))
| summarize hint.strategy=partitioned arg_max(TimeGenerated, UpdateState,
Classification, Approved) by Computer, SourceComputerId, UpdateID
| where UpdateState=~"Needed" and Approved!=false
| summarize by UpdateID, Classification )
| summarize allUpdatesCount=count(),
criticalUpdatesCount=countif(Classification has "Critical"),
securityUpdatesCount=countif(Classification has "Security"),
otherUpdatesCount=countif(Classification !has "Critical" and Classification
!has "Security")
```

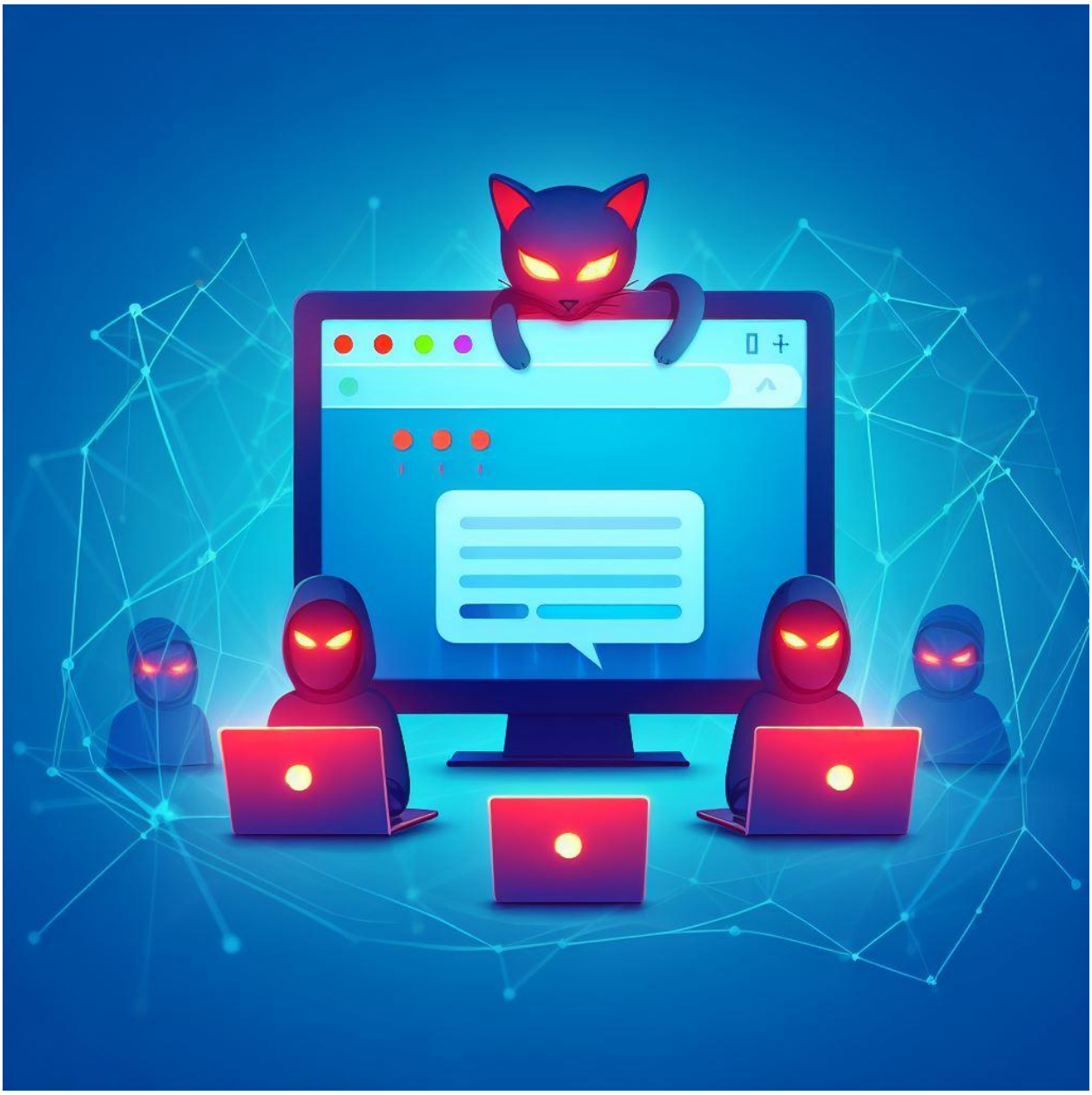
Summary

Microsoft Sentinel is a cloud-native SIEM solution that can help organizations protect themselves from zero-day exploits. It can collect data at cloud scale, detect threats with analytics and intelligence, and investigate and respond with automation and

orchestration. By using Microsoft Sentinel, organizations can benefit from the speed, scale, and intelligence of the cloud to enhance their security operations and resilience.

Microsoft Sentinel SOC 101: How to Detect and Mitigate a DNS Spoofing Attack with Microsoft Sentinel

Spoof Aloof



DNS spoofing, also known as DNS cache poisoning, is a type of cyberattack that uses tampered DNS server data to redirect users to fake websites. These malicious sites often look legitimate but are actually designed to install malware onto users' devices, steal sensitive data or redirect traffic.

DNS spoofing can have serious consequences for both users and organizations, such as compromising credentials, exposing confidential information, disrupting business operations, and damaging reputation. Therefore, it is important to detect and mitigate DNS spoofing attacks as quickly and effectively as possible.

In this post, I'll talk about how to use Microsoft Sentinel, a cloud native SIEM solution powered by AI and automation, to detect and mitigate DNS spoofing attacks across your entire enterprise.

What is Microsoft Sentinel?

Microsoft Sentinel is a scalable, cloud-native solution that provides:

- Security information and event management (SIEM)
- Security orchestration, automation, and response (SOAR)

Microsoft Sentinel delivers intelligent security analytics and threat intelligence across the enterprise. With Microsoft Sentinel, you get a single solution for attack detection, threat visibility, proactive hunting, and threat response.

Microsoft Sentinel has many benefits over legacy SIEM solutions, such as:

- Eliminating security infrastructure setup and maintenance
- Scaling elastically to meet your security needs
- Reducing costs as much as 48 percent compared to legacy SIEM solutions
- Collecting data at cloud scale across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds
- Detecting previously uncovered threats and minimizing false positives using analytics and unparalleled threat intelligence from Microsoft

- Investigating threats with AI and hunting suspicious activities at scale, tapping into decades of cybersecurity work at Microsoft
- Responding to incidents rapidly with built-in orchestration and automation of common tasks

How to Detect a DNS Spoofing Attack Using Microsoft Sentinel?

To detect a DNS spoofing attack using Microsoft Sentinel, you need to first connect to your data sources. Microsoft Sentinel comes with many connectors for Microsoft solutions that are available out of the box and provide real-time integration. Some of these connectors include:

- Microsoft sources like Microsoft 365 Defender, Microsoft Defender for Cloud, Office 365, Microsoft Defender for IoT, and more.
- Azure service sources like Azure Active Directory, Azure Activity, Azure Storage, Azure Key Vault, Azure Kubernetes service, and more.

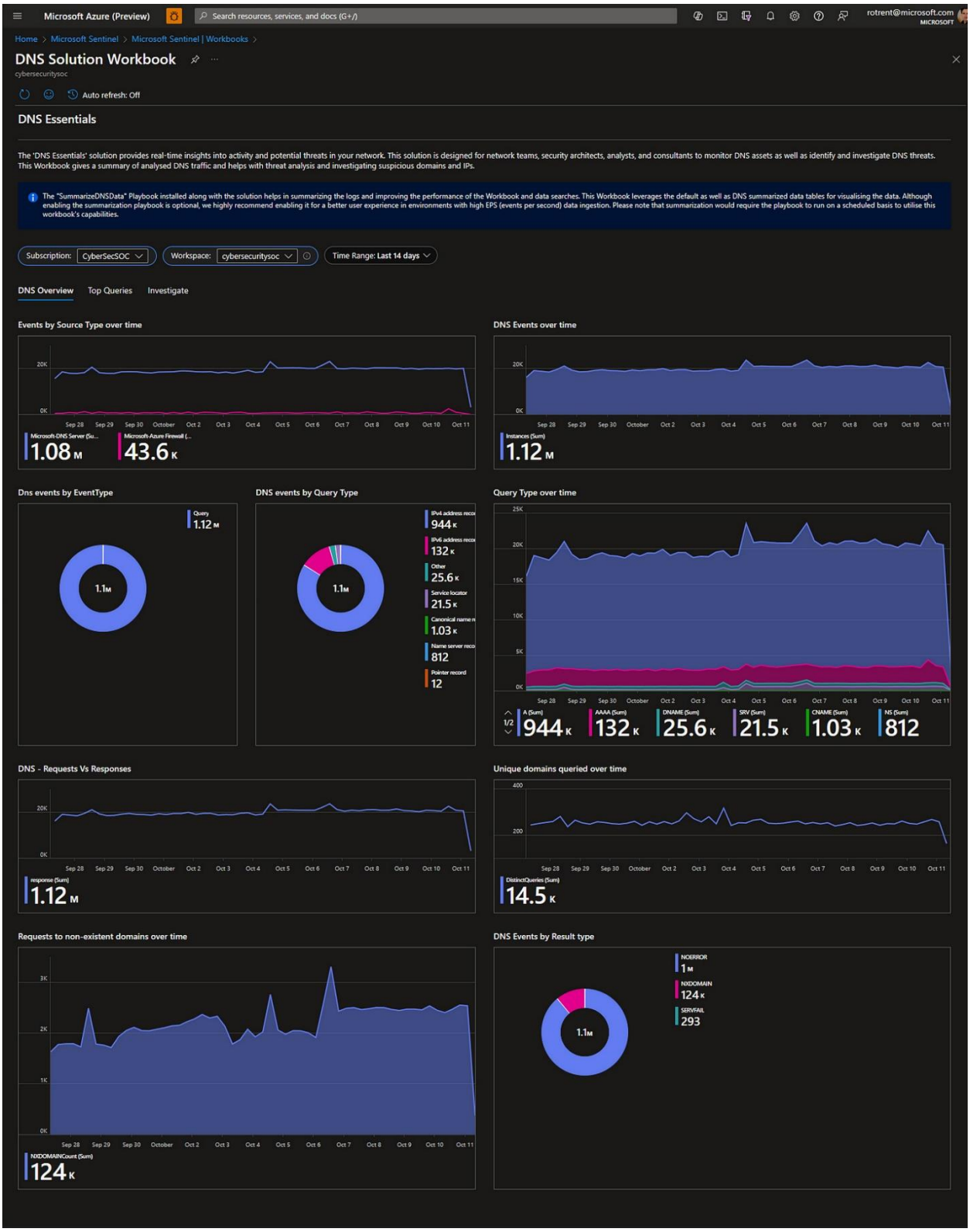
Microsoft Sentinel also has built-in connectors to the broader security and applications ecosystems for non-Microsoft solutions. You can also use common event format (CEF), Syslog, or REST-API to connect your data sources with Microsoft Sentinel.

After you connect your data sources to Microsoft Sentinel, you can monitor your data by using the integration with Azure Monitor workbooks. Workbooks are interactive reports that provide insights into your data and enable you to create custom dashboards. You can use the built-in workbooks or create your own workbooks based on your needs.

One of the built-in workbooks that can help you detect DNS spoofing attacks is the **DNS Essentials** workbook. This workbook provides an overview of the DNS activity in your environment and helps you identify anomalies and potential threats. Some of the features of this workbook include:

- A summary of the top domains queried by your devices
- A breakdown of the DNS query types and response codes
- A map of the geographic locations of the DNS servers contacted by your devices
- A list of the suspicious domains that may indicate malicious activity
- A timeline of the DNS events over time

You can use the filters and parameters in this workbook to customize your view and drill down into specific details. You can also use the links in this workbook to navigate to other workbooks or resources for further investigation.


Microsoft Azure (Preview)
Search resources, services, and docs (G+/)
rotrent@microsoft.com
MICROSOFT
Home > Microsoft Sentinel > Microsoft Sentinel | Workbooks >
DNS Solution Workbook
cybersecuritysoc
Auto refresh: Off
DNS Essentials
The 'DNS Essentials' solution provides real-time insights into activity and potential threats in your network. This solution is designed for network teams, security architects, analysts, and consultants to monitor DNS assets as well as identify and investigate DNS threats. This Workbook gives a summary of analysed DNS traffic and helps with threat analysis and investigating suspicious domains and IPs.
The "SummarizeDNSData" Playbook installed along with the solution helps in summarizing the logs and improving the performance of the Workbook and data searches. This Workbook leverages the default as well as DNS summarized data tables for visualising the data. Although enabling the summarization playbook is optional, we highly recommend enabling it for a better user experience in environments with high EPS (events per second) data ingestion. Please note that summarization would require the playbook to run on a scheduled basis to utilise this workbook's capabilities.
Subscription: CyberSecSOC
Workspace: cybersecuritysoc
Time Range: Last 14 days
DNS Overview
Top Queries
Investigate
Events by Source Type over time
1.08 M
43.6 K
DNS Events over time
1.12 M
Dns events by EventType
1.12 M
DNS events by Query Type
944 K
132 K
25.6 K
21.5 K
1.03 K
812
12
Query Type over time
A (Sum) 944 K
AAAA (Sum) 132 K
DNAME (Sum) 25.6 K
SRV (Sum) 21.5 K
CNAME (Sum) 1.03 K
NS (Sum) 812
DNS - Requests Vs Responses
1.12 M
Unique domains queried over time
14.5 K
Requests to non-existent domains over time
124 K
DNS Events by Result type
1 M
124 K
293

How to Mitigate a DNS Spoofing Attack Using Microsoft Sentinel?

To mitigate a DNS spoofing attack using Microsoft Sentinel, you need to use the analytics rules and playbooks features. Analytics rules are the logic that runs on your data and generates alerts when certain conditions are met. Playbooks are the automated workflows that run-in response to alerts or other triggers and perform actions such as sending notifications, creating tickets, running scripts, or invoking APIs.

Microsoft Sentinel provides several built-in analytics rules and playbooks that can help you mitigate DNS spoofing attacks. Some of these include:

- An analytics rule that detects anomalous DNS queries from devices based on machine learning models.
- An analytics rule that detects malicious domains based on threat intelligence feeds.
- An analytics rule that detects DNS tunneling activity based on query length and frequency.
- A playbook that blocks malicious domains by using Azure Firewall
- A playbook that isolates infected devices by using Microsoft Defender for Endpoint
- A playbook that sends an email notification to the security team with relevant details

You can also create your own analytics rules and playbooks based on your needs and preferences. You can use the query language (Kusto Query Language or KQL) to write custom logic for your analytics rules and use the graphical interface or the code view to design your playbooks.

The following KQL query is an example that does a lookup on some of the more common ToR proxies:

```
//Identifies IP addresses performing DNS lookups associated with common ToR
proxies
DnsEvents
| where Name contains "."
| where Name has_any ("tor2web.org", "tor2web.com", "torlink.co", "onion.to",
"onion.ink", "onion.cab", "onion.nu", "onion.link", "onion.it", "onion.city",
"onion.direct", "onion.top", "onion.casa", "onion.plus", "onion.rip",
"onion.dog", "tor2web.fi", "tor2web.blutmagie.de", "onion.sh", "onion.lu",
"onion.pet", "t2w.pw", "tor2web.ae.org", "tor2web.io", "tor2web.xyz",
"onion.lt", "s1.tor-gateways.de", "s2.tor-gateways.de", "s3.tor-gateways.de",
"s4.tor-gateways.de", "s5.tor-gateways.de", "hiddenservice.net")
| extend timestamp = TimeGenerated, IPCustomEntity = ClientIP,
HostCustomEntity = Computer
```

The following example utilizes the content of the Threat Intelligence Indicator table to find matches against the DNSEvents table.

```
//TI Lookup that match DNS events
let dt_lookBack = 1h;
let ioc_lookBack = 14d;
ThreatIntelligenceIndicator
| where TimeGenerated >= ago(ioc_lookBack) and ExpirationDateTime > now()
| where Active == true
// Picking up only IOC's that contain the entities we want
| where isnotempty(NetworkIP) or isnotempty(EmailSourceIpAddress) or
isnotempty(NetworkDestinationIP) or isnotempty(NetworkSourceIP)
// As there is potentially more than 1 indicator type for matching IP, taking
NetworkIP first, then others if that is empty.
// Taking the first non-empty value based on potential IOC match availability
| extend TI_ipEntity = iff(isnotempty(NetworkIP), NetworkIP,
NetworkDestinationIP)
| extend TI_ipEntity = iff(isempty(TI_ipEntity) and
isnotempty(NetworkSourceIP), NetworkSourceIP, TI_ipEntity)
| extend TI_ipEntity = iff(isempty(TI_ipEntity) and
isnotempty(EmailSourceIpAddress), EmailSourceIpAddress, TI_ipEntity)
| join (
    DnsEvents | where TimeGenerated >= ago(dt_lookBack)
    | where SubType =~ "LookupQuery" and isnotempty(IPAddresses)
    | extend SingleIP = split(IPAddresses, ",")
    | mvexpand SingleIP
    | extend SingleIP = tostring(SingleIP)
    // renaming time column so it is clear the log this came from
    | extend DNS_TimeGenerated = TimeGenerated
)
on $left.TI_ipEntity == $right.SingleIP
| summarize LatestIndicatorTime = arg_max(TimeGenerated, *) by IndicatorId
| project LatestIndicatorTime, Description, ActivityGroupNames, IndicatorId,
ThreatType, Url, ExpirationDateTime, ConfidenceScore, DNS_TimeGenerated,
```

```
TI_ipEntity, Computer, EventId, SubType, ClientIP, Name, IPAddresses,
NetworkIP, NetworkDestinationIP, NetworkSourceIP, EmailSourceIpAddress
| extend timestamp = DNS_TimeGenerated, IPCustomEntity = ClientIP,
HostCustomEntity = Computer, URLCustomEntity = Url
```

Summary

DNS spoofing is a serious threat that can compromise your security and privacy. Microsoft Sentinel is a powerful solution that can help you detect and mitigate DNS spoofing attacks across your enterprise. By using Microsoft Sentinel, you can leverage the cloud-native, AI-powered, and automated capabilities of this SIEM solution to protect your data and assets from DNS spoofing and other cyberattacks.

Microsoft Sentinel SOC 101: How to Detect and Mitigate Advanced Persistent Threats (APTs) with Microsoft Sentinel

Slaying Gorgon

Advanced persistent threats (APTs) are stealthy and sophisticated cyberattacks that aim to gain and maintain unauthorized access to a target network for a long period of time, often with the intention of stealing sensitive data or conducting espionage. APTs are usually carried out by well-resourced and skilled threat actors, such as nation-state or state-sponsored groups, or organized cybercrime syndicates. APTs can pose a serious threat to the security and reputation of any organization, especially those with high-value information or critical infrastructure.

To effectively combat APTs, organizations need a comprehensive and scalable security solution that can provide visibility, detection, investigation, and response capabilities across their entire enterprise. Microsoft Sentinel is a cloud-native security information and event management (SIEM) solution that delivers intelligent

security analytics and threat intelligence across the enterprise. With Microsoft Sentinel, you can:

- Collect data at cloud scale across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds.
- Detect previously uncovered threats and minimize false positives using analytics and unparalleled threat intelligence from Microsoft.
- Investigate threats with AI and hunt suspicious activities at scale, tapping into decades of cybersecurity work at Microsoft.
- Respond to incidents rapidly with built-in orchestration and automation of common tasks.

In this post, I'll talk about how to use Microsoft Sentinel to detect and mitigate APTs in your environment. Let's dig into the following steps:

- Connect your data sources to Microsoft Sentinel.
- Use workbooks to monitor your data and identify anomalies.
- Use analytics rules to correlate alerts into incidents.
- Use playbooks to automate and orchestrate common tasks.
- Use hunting queries to proactively search for threats.

Connect your data sources to Microsoft Sentinel

The first step to use Microsoft Sentinel is to connect your data sources to the solution. Microsoft Sentinel comes with many connectors for Microsoft solutions that are available out of the box and provide real-time integration. Some of these connectors include:

- Microsoft sources like Microsoft 365 Defender, Microsoft Defender for Cloud, Office 365, Microsoft Defender for IoT, and more.

- Azure service sources like Azure Active Directory, Azure Activity, Azure Storage, Azure Key Vault, Azure Kubernetes service, and more.

Microsoft Sentinel also has built-in connectors to the broader security and applications ecosystems for non-Microsoft solutions. You can also use common event format (CEF), Syslog, or REST-API to connect your data sources with Microsoft Sentinel.

To connect your data sources to Microsoft Sentinel, follow these steps:

1. Sign into the Azure portal.
2. Search for and select **Microsoft Sentinel**.
3. Select the workspace that you want to use or create a new one.
4. In the navigation pane, select **Data connectors**.
5. Browse or search for the connector that you want to use and select it.
6. Follow the instructions on the connector page to configure it.

Use workbooks to monitor your data and identify anomalies

After you connect your data sources to Microsoft Sentinel, you can use workbooks to monitor your data and identify anomalies. Workbooks are interactive reports that provide insights into your data using charts, tables, maps, timelines, and more. You can use pre-built workbooks that are provided by Microsoft or create your own custom workbooks.

To use workbooks in Microsoft Sentinel, follow these steps:

1. In the Azure portal, select **Microsoft Sentinel** > **Workbooks**.
2. Browse or search for the workbook that you want to use and select it.
3. Configure the parameters of the workbook as needed.

4. Explore the workbook tabs and visuals to analyze your data.

For example, you can use the **Threat Intelligence - Overview** workbook to get an overview of the threat intelligence indicators (TIIs) in your environment. You can see the distribution of TIIs by severity, confidence, source type, category, file type, domain type, IP type, URL type, email type, etc. You can also see the top malicious entities by TIIs count and drill down into specific entities for more details.

Use Analytics Rules to correlate alerts into Incidents

To detect APTs in your environment, you need to correlate alerts from different data sources into incidents that represent potential security breaches. Analytics rules are the core detection logic in Microsoft Sentinel that enable you to do this. Analytics rules run automated queries over your data at regular intervals and generate alerts when certain conditions are met. You can use pre-built analytics rules that are provided by Microsoft or create your own custom analytics rules.

To use analytics rules in Microsoft Sentinel, follow these steps:

1. In the Azure portal, select **Microsoft Sentinel** > **Analytics**.
2. Browse or search for the rule that you want to use and select it.
3. Review the rule details and enable it if needed.
4. Optionally, customize the rule logic, alert details, incident settings, and automation options as needed.

For example, you can use the **Potential DGA detected** rule to detect potential domain generation algorithm (DGA) activity in your environment. DGA is a technique used by some malware to generate random domain names for command and control (C2) servers. This rule runs a query over your DNS data and generates an alert when it

detects a high number of requests to domains with high entropy or low popularity.

Use Playbooks to automate and orchestrate common tasks

To respond to incidents rapidly and efficiently, you need to automate and orchestrate common tasks that are part of your incident response process. Playbooks are the automation component of Microsoft Sentinel that enable you to do this. Playbooks are based on Azure Logic Apps and allow you to create workflows that can perform actions such as sending an email, creating a ticket, blocking an IP address, running a script, etc. You can use pre-built playbooks that are provided by Microsoft or create your own custom playbooks.

To use playbooks in Microsoft Sentinel, follow these steps:

1. In the Azure portal, select **Microsoft Sentinel** > **Automation**.
2. Browse or search for the playbook that you want to use and select it.
3. Review the playbook details and enable it if needed.
4. Optionally, customize the playbook trigger, actions, parameters, and logic as needed.

For example, you can use the **Block IP with Azure Firewall** playbook to block an IP address that is associated with an incident in your environment. This playbook is triggered when an incident is created or updated in Microsoft Sentinel and has a specific tag. The playbook then retrieves the IP address from the incident entity and adds it to a deny list in Azure Firewall.

Use Hunting queries to proactively search for threats

To proactively hunt for threats in your environment, you need to run queries over your data and look for suspicious activities or

indicators of compromise (IOCs). Hunting queries are the proactive hunting component of Microsoft Sentinel that enable you to do this. Hunting queries are based on Kusto Query Language (KQL) and allow you to create custom queries that can run over your data sources and return results that can be further investigated or added to incidents. You can use pre-built hunting queries that are provided by Microsoft or create your own custom hunting queries.

To use hunting queries in Microsoft Sentinel, follow these steps:

1. In the Azure portal, select **Microsoft Sentinel** > **Hunting**.
2. Browse or search for the query that you want to use and select it.
3. Review the query details and run it if needed.
4. Explore the query results and take actions such as bookmarking, adding to incidents, or creating new incidents as needed.

For example, you can use the **Detect SSH Brute Force Attack** query to detect SSH brute force attack attempts in your environment. This query runs over your Syslog data and returns results that show the source IP address, destination IP address, destination port, number of failed attempts, and number of unique usernames used for each SSH brute force attempt.

See: *Microsoft Sentinel SOC 101: How to Detect and Mitigate Brute Force Attacks with Microsoft Sentinel*

Summary

In this post, I've talked about how to use Microsoft Sentinel to detect and mitigate APTs in your environment. We have covered how to connect your data sources, use workbooks, analytics rules, playbooks, and hunting queries in Microsoft Sentinel. By using these features, you can leverage the power of cloud-native SIEM and

AI to enhance your security posture and protect your organization from sophisticated threats.

Microsoft Sentinel SOC 101: How to Detect and Mitigate Botnet Attacks with Microsoft Sentinel

Botswana

In today's digital landscape, the security of our networks is of utmost importance. Cybercriminals are constantly evolving their tactics to breach our defenses and gain unauthorized access to our systems. One such threat that has become increasingly prevalent is botnet attacks. These attacks use a network of compromised devices to carry out malicious activities, such as distributed denial of service (DDoS) attacks, spam campaigns, or data theft. To effectively protect our networks, we need robust detection and mitigation solutions like Microsoft Sentinel.

Understanding Botnet Attacks and Their Impact on Network Security

Before we delve into the role of Microsoft Sentinel in detecting and mitigating botnet attacks, let's first understand the nature of these attacks and their impact on network security. A botnet is a network of compromised devices, often referred to as "bots" or "zombies," that are under the control of a central command-and-control server operated by cybercriminals. These devices can include computers, servers, smartphones, or even Internet of Things (IoT) devices.

Botnet attacks can have severe consequences for network security. They can be used to launch large-scale DDoS attacks, overwhelming targeted systems with massive traffic and causing service disruptions. Botnets can also be used to distribute malware or conduct phishing campaigns, leading to data breaches and financial losses. Additionally, botnets can be rented out for various malicious purposes, making them a lucrative business for cybercriminals.

Introduction to Microsoft Sentinel and Its Role in Detecting and Mitigating Botnet Attacks

Microsoft Sentinel is a cloud-native security information and event management (SIEM) solution that provides real-time threat

detection, response, and investigation capabilities. It leverages the power of artificial intelligence (AI) and machine learning (ML) to analyze vast amounts of security data and identify potential threats, including botnet attacks.

With Microsoft Sentinel, organizations can gain comprehensive visibility into their network activities and detect botnet-related anomalies in real-time. The solution collects and analyzes data from various sources, such as firewalls, intrusion detection systems, and endpoint protection platforms, to identify suspicious patterns and behaviors indicative of botnet activity. It also integrates with threat intelligence feeds to stay updated on the latest botnet campaigns and indicators of compromise.

Key Features of Microsoft Sentinel for Botnet Detection and Mitigation

Microsoft Sentinel offers several key features that are specifically designed to detect and mitigate botnet attacks effectively. Let's explore some of these features in detail:

Advanced Analytics and Machine Learning

Microsoft Sentinel utilizes advanced analytics and machine learning algorithms to detect anomalies and patterns associated with botnet attacks. By baselining normal network behavior, the solution can identify deviations indicative of botnet activity. It can detect unusual traffic patterns, spikes in network activity, or suspicious communication with known command-and-control servers.

The machine learning algorithms continuously learn from new data and adapt their detection capabilities, ensuring that organizations stay protected against emerging botnet threats. This

proactive approach enables early detection and swift response, minimizing the potential damage caused by botnet attacks.

Threat Intelligence Integration

To enhance botnet detection capabilities, Microsoft Sentinel integrates with various threat intelligence feeds. These feeds provide up-to-date information on known botnet campaigns, malicious IP addresses, domain names, and other indicators of compromise. By leveraging this threat intelligence, Microsoft Sentinel can identify and block botnet-related communication, preventing devices within the network from becoming part of a botnet or interacting with botnet infrastructure.

The integration with threat intelligence also enables organizations to proactively hunt for botnet-related activities and indicators within their network. By correlating internal network data with external intelligence, security teams can identify compromised devices, malware infections, or unauthorized communication with known malicious entities.

Automated Incident Response

In the event of a botnet attack, rapid response is crucial to minimize the impact and prevent further spread. Microsoft Sentinel offers automated incident response capabilities that enable organizations to automatically block or quarantine compromised devices, shut down malicious processes, or isolate affected segments of the network. These automated response actions can be triggered based on predefined rules and alerts, ensuring a swift and consistent response to botnet threats.

Additionally, Microsoft Sentinel provides playbooks that guide security teams through the incident response process, ensuring a standardized and effective approach to botnet mitigation. The

playbooks can be customized to align with an organization's specific security policies and procedures, streamlining the incident response workflow.

Setting Up Microsoft Sentinel for Optimal Botnet Threat Detection

To maximize the effectiveness of Microsoft Sentinel in detecting and mitigating botnet attacks, organizations need to set up the solution correctly. Here are some essential steps to consider:

Data Collection and Integration

To detect botnet-related anomalies, Microsoft Sentinel requires access to relevant security data from various sources within the network. Organizations should ensure that their firewalls, intrusion detection systems, endpoint protection platforms, and other security tools are configured to send logs and events to Microsoft Sentinel. This data will serve as the foundation for botnet detection and analysis.

Microsoft Sentinel supports a wide range of data connectors that facilitate the integration of security data from both Microsoft and third-party sources. These connectors should be configured to collect and ingest data into Microsoft Sentinel for comprehensive visibility and analysis.

Rule and Alert Configuration

Microsoft Sentinel provides a range of preconfigured rules and alerts specifically designed for botnet detection. However, organizations should review and customize these rules to align with their network environment, security policies, and specific botnet threat landscape. By tailoring the rules and alerts, organizations can

reduce false positives and focus on the most relevant botnet-related events.

It is also recommended to create custom rules and alerts based on specific botnet indicators or behaviors that are unique to an organization's network. This customization ensures that Microsoft Sentinel is finely tuned to detect botnet activity that may be specific to the organization's industry or infrastructure.

Continuous Monitoring and Analysis

Botnet threats are constantly evolving, and organizations need to continuously monitor their network for new indicators and patterns of botnet activity. Microsoft Sentinel's advanced analytics and machine learning capabilities enable real-time monitoring and analysis of network traffic, log data, and security events.

Organizations should regularly review and fine-tune their detection rules and alerts based on the latest threat intelligence and security trends. By staying proactive and adaptive, organizations can stay one step ahead of botnet attacks and effectively mitigate them before significant damage occurs.

Configuring Custom Alerts and Rules for Botnet Detection in Microsoft Sentinel

Microsoft Sentinel offers organizations the flexibility to create custom alerts and rules tailored to their specific botnet detection requirements. By configuring custom alerts, organizations can enhance the sensitivity and accuracy of their botnet detection capabilities. Here are some key considerations for configuring custom alerts and rules in Microsoft Sentinel:

Define Baseline Network Behavior

Before creating custom alerts and rules, organizations should establish a baseline of normal network behavior. This baseline represents the expected patterns and activities within the network under normal circumstances. By defining a baseline, organizations can identify deviations that may indicate botnet activity more effectively.

To establish a baseline, organizations should collect and analyze historical network traffic, log data, and security events. This analysis can help identify normal communication patterns, typical traffic volumes, and expected behaviors of network devices. The baseline can be adjusted periodically to accommodate changes in network infrastructure or security policies.

Identify Botnet Indicators

Once the baseline is established, organizations should identify specific indicators or behaviors associated with botnet activity. These indicators can include unusual communication patterns, connections to known malicious IP addresses, or excessive traffic volumes from specific devices or subnets.

Organizations should leverage threat intelligence feeds, security research reports, and industry-specific botnet detection techniques to identify relevant indicators. Microsoft Sentinel's integration with threat intelligence feeds can also provide valuable insights into the latest botnet campaigns and indicators of compromise.

Create Custom Detection Rules and Alerts

Based on the identified botnet indicators, organizations can create custom detection rules and alerts in Microsoft Sentinel. These rules

should be designed to trigger alerts whenever the defined indicators are observed within the network.

When configuring custom rules, organizations should consider the specific log sources, data fields, or event attributes that are most relevant to botnet detection. They should also define the severity levels and response actions associated with each rule. For example, a high-severity alert may trigger an automated response action, while a low-severity alert may require manual investigation.

By creating custom rules and alerts, organizations can fine-tune their botnet detection capabilities and focus on the most critical events that require immediate attention.

A good couple examples of queries for Botnet detection using TI are:

- **AbuseCH Botnet C2 Indicators Of Compromise**
- **Abuse.ch Botnet C2 IP Blacklist to detect external C2 connections**

Analyzing and Investigating Botnet Attacks Using Microsoft Sentinel's Advanced Analytics and Visualization Tools

In the event of a botnet attack, prompt analysis and investigation are crucial to understand the scope and impact of the attack and develop an effective mitigation strategy. Microsoft Sentinel provides advanced analytics and visualization tools that enable security teams to gain deep insights into botnet attacks and expedite the investigation process.

Log Search and Query

Microsoft Sentinel's log search and query capabilities allow security teams to search, filter, and analyze vast amounts of security data in real-time. Security analysts can use query languages like Kusto

Query Language (KQL) to construct complex queries that extract relevant information related to a botnet attack.

For example, analysts can search for specific IP addresses associated with known botnet command-and-control servers or identify compromised devices based on unusual communication patterns. By leveraging log search and query, security teams can quickly identify the root cause of a botnet attack and take appropriate action.

Advanced Analytics and Machine Learning

Microsoft Sentinel's advanced analytics and machine learning capabilities play a crucial role in identifying botnet-related anomalies and patterns. The solution can automatically detect and correlate events that may indicate botnet activity, such as multiple devices communicating with a known malicious IP address or a sudden increase in outbound network traffic.

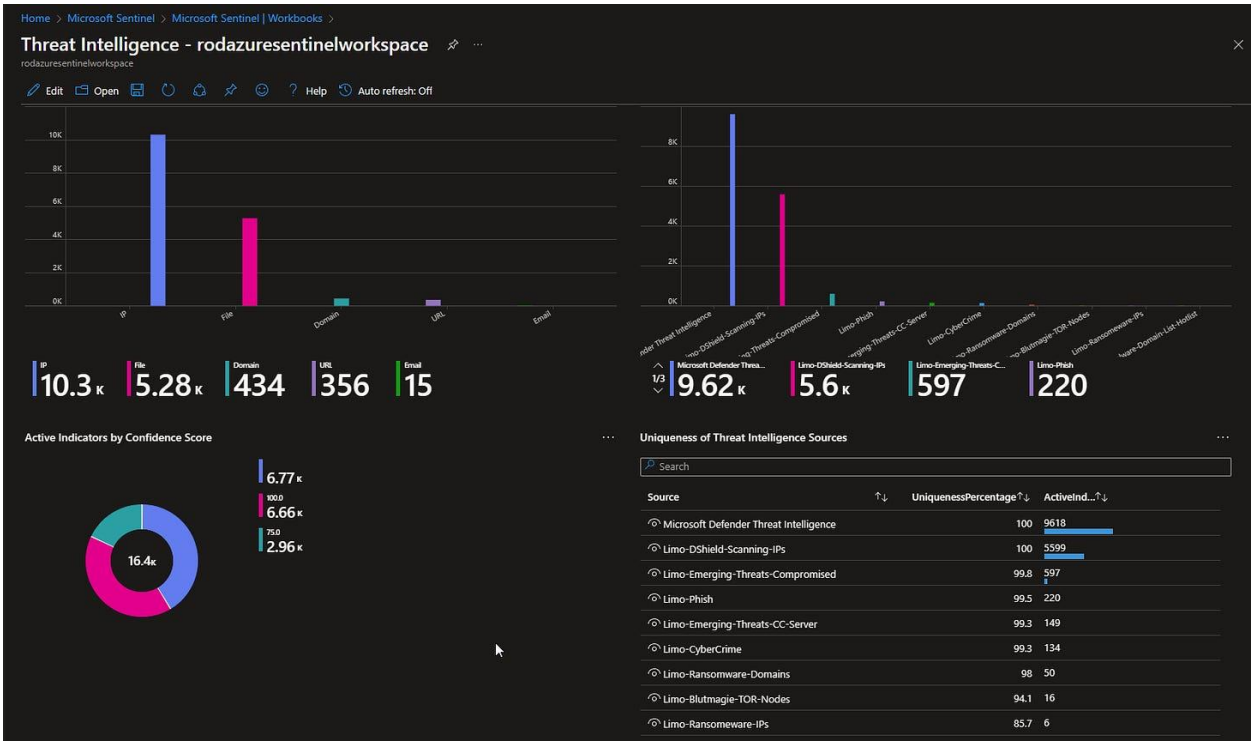
These analytics capabilities enable security teams to identify botnet-related events that may have gone unnoticed through manual analysis. By leveraging machine learning, Microsoft Sentinel continuously improves its detection capabilities based on new data and emerging botnet threats.

Visualization and Dashboarding

Microsoft Sentinel provides interactive visualizations and customizable dashboards that enable security teams to visualize and understand the data related to botnet attacks effectively. These visualizations can include network traffic flows, geographic maps displaying botnet activity, or timelines showing the progression of an attack.

By visualizing the data, security analysts can identify patterns, trends, or relationships that may not be apparent through raw log data. The visualizations can help in identifying the scale and impact of a botnet attack and guide the decision-making process for effective mitigation.

The **Threat Intelligence Workbook template** is a valuable visualization to enable. This workbook displays information about the Threat Intelligence that is being used and is available to use to develop better queries.



Best Practices for Mitigating Botnet Attacks with Microsoft Sentinel

While Microsoft Sentinel provides powerful capabilities for detecting and mitigating botnet attacks, organizations should follow

best practices to maximize their botnet defense. Here are some essential best practices to consider:

Regularly Update and Patch Systems

Botnet attacks often exploit vulnerabilities in software and hardware to compromise devices and recruit them into a botnet. To minimize the risk of botnet infections, organizations should establish a robust patch management process and ensure that all systems and applications are regularly updated with the latest security patches.

By promptly patching vulnerabilities, organizations can reduce the attack surface and make it harder for botnet operators to compromise their network.

Implement Strong Access Controls

Unauthorized access to devices within the network can provide an entry point for botnet attacks. Organizations should implement strong access controls, including strong passwords, multi-factor authentication, and least privilege principles.

By limiting user privileges and enforcing strong authentication mechanisms, organizations can prevent unauthorized access and reduce the likelihood of devices being compromised and recruited into a botnet.

Educate Employees on Security Awareness

Human error is often a significant factor in successful botnet attacks. Organizations should invest in security awareness training programs to educate employees about the risks of botnet attacks and common attack vectors.

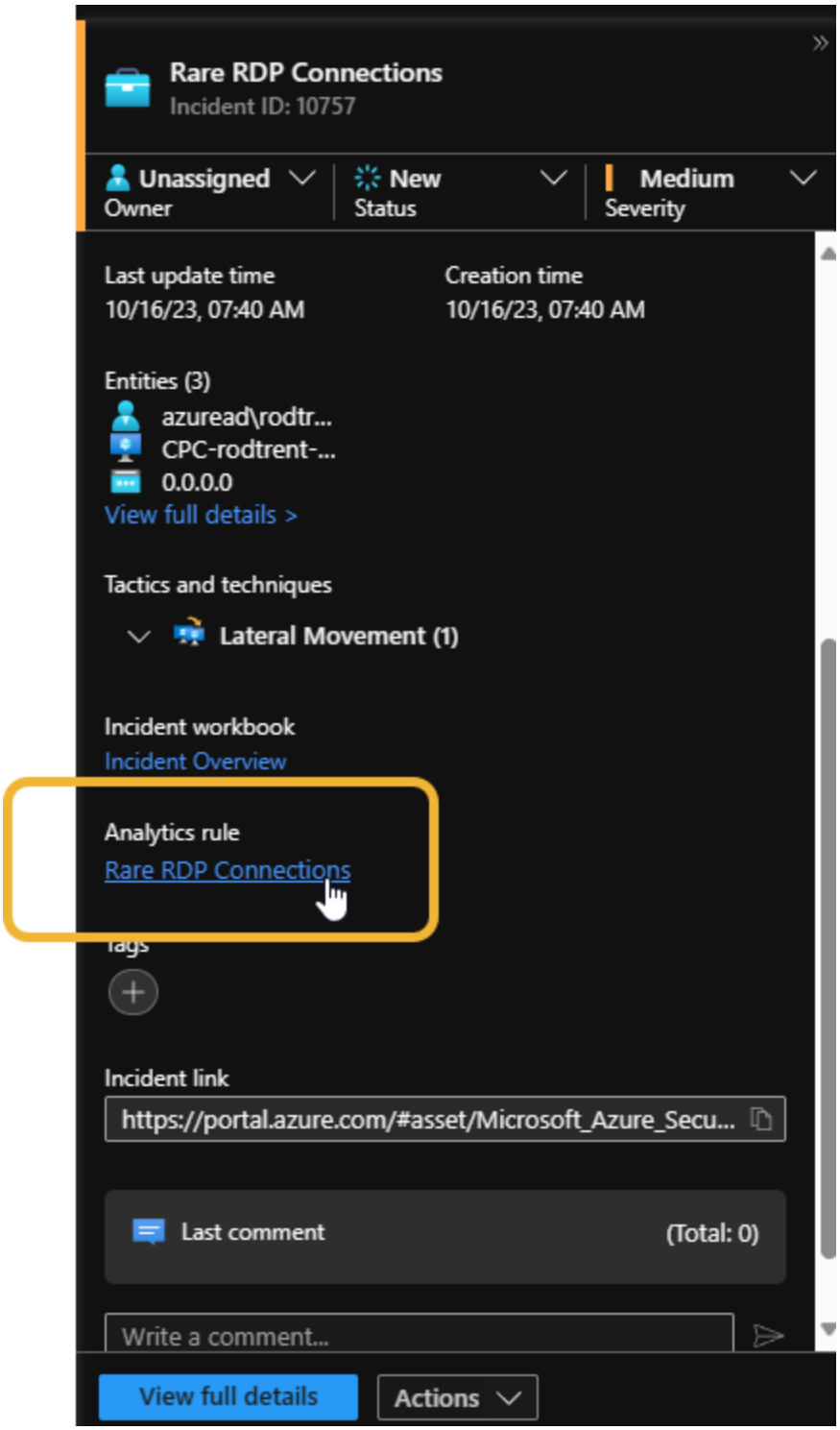
Employees should be trained to recognize phishing emails, avoid suspicious downloads, and report any unusual network activities promptly. By fostering a security-conscious culture, organizations can significantly reduce the risk of botnet infections.

Regularly Review and Fine-Tune Detection Rules

Botnet threats are constantly evolving, and organizations need to adapt their detection rules and alerts accordingly. Regularly reviewing and fine-tuning detection rules based on the latest threat intelligence and security trends ensures that Microsoft Sentinel remains effective in detecting emerging botnet threats.

Organizations should also collaborate with their security teams and share knowledge and insights to continuously improve their botnet defense capabilities.

Over time, Analytics Rules should be reviewed and tuned to ensure they are collecting the right data. Microsoft Sentinel provides direct link access to the Analytics Rule that generates each Incident, making it easy to evolve the rule as part of the investigation process.


Rare RDP Connections
Incident ID: 10757
Unassigned
Owner
New
Status
Medium
Severity
Last update time
10/16/23, 07:40 AM
Creation time
10/16/23, 07:40 AM
Entities (3)
azuread\rodtr...
CPC-rodtrent-...
0.0.0.0
View full details >
Tactics and techniques
Lateral Movement (1)
Incident workbook
Incident Overview
Analytics rule
Rare RDP Connections
Tags
Incident link
https://portal.azure.com/#asset/Microsoft_Azure_Secu...
Last comment
(Total: 0)
Write a comment...
View full details
Actions

Collaborating with Security Teams and Leveraging Threat Intelligence for Effective Botnet Defense

Effective botnet defense requires collaboration between security teams within an organization and an understanding of the broader threat landscape. By collaborating with security teams, organizations can leverage diverse expertise and perspectives to enhance their botnet defense capabilities. Here are some key aspects to consider:

Security Operations Center (SOC) Collaboration

Organizations should establish close collaboration between their security operations center (SOC) and Microsoft Sentinel administrators. The SOC team can provide valuable insights into the organization's network and security challenges, which can be used to fine-tune botnet detection rules and alerts.

The SOC team can also benefit from the visibility and insights provided by Microsoft Sentinel. By sharing information and collaborating on incident response, organizations can streamline the detection and mitigation of botnet attacks.

Sharing Threat Intelligence

Threat intelligence sharing is a critical aspect of effective botnet defense. Organizations should actively contribute to and benefit from threat intelligence sharing communities, both within their industry and across sectors. By sharing information on botnet campaigns, malicious IP addresses, or indicators of compromise, organizations can collectively improve their botnet detection capabilities.

Microsoft Sentinel's integration with threat intelligence feeds enables organizations to automatically receive the latest threat

intelligence updates. By leveraging this intelligence, organizations can stay ahead of emerging botnet threats and proactively defend their networks.

Microsoft Sentinel SOC 101: How to Detect and Mitigate a VIP Account that has Multiple Failed Logons within a Threshold with Microsoft Sentinel

Vee-eye-pee

Microsoft Sentinel is a cloud-native solution that provides security information and event management (SIEM) and security

orchestration, automation, and response (SOAR) capabilities. It can help organizations defend against modern attacks by collecting, analyzing, and responding to security events across the enterprise. One of the common scenarios that Microsoft Sentinel can help with is detecting and mitigating brute-force attacks on VIP accounts, such as executives or administrators, who have access to sensitive data or resources.

A brute-force attack is a type of cyberattack that involves trying many possible combinations of passwords or other credentials to gain unauthorized access to an account or system. Brute-force attacks can be performed by automated tools or scripts that attempt to guess passwords based on common patterns, dictionaries, or leaked databases. Brute-force attacks can also be targeted at specific accounts or systems that are known to be valuable or vulnerable.

A VIP account is an account that belongs to a user who has a high level of privilege, influence, or visibility in an organization. VIP accounts may include executives, administrators, managers, or key employees who have access to confidential information, critical systems, or strategic decisions. VIP accounts are attractive targets for attackers who want to compromise the organization's security, reputation, or operations.

To detect and mitigate a VIP account multiple failed logins within a specified number of minutes using Microsoft Sentinel, you can follow these steps:

Step 1: Define the VIP accounts and the logon threshold

The first step is to define which accounts are considered VIP accounts in your organization and what is the acceptable number of failed logon attempts within a certain time period. You can use the following criteria to identify VIP accounts:

- The account has a high level of permission or role in the organization, such as global administrator, domain administrator, executive officer, etc.
- The account has access to sensitive data or resources, such as financial records, customer information, intellectual property, etc.
- The account is frequently used for communication or collaboration with external parties, such as partners, customers, media, etc.

You can use the following criteria to determine the logon threshold:

- The number of failed logon attempts that indicate a possible brute-force attack. This may vary depending on the complexity and length of the passwords used by the VIP accounts. A common value is 6 failed logon attempts within 10 minutes.
- The time window that defines the frequency of the failed logon attempts. This may vary depending on the normal usage pattern of the VIP accounts. A common value is 10 minutes.

You can use Microsoft Entra ID PowerShell cmdlets to get a list of VIP accounts based on their roles or permissions. For example, you can use this command to get all global administrators in your tenant:

```
Get-AzureADDirectoryRoleMember -ObjectId (Get-AzureADDirectoryRole | Where-
Object {$_.displayName -eq "Global Administrator"}).ObjectId
```

Step 2: Create a custom detection rule in Microsoft Sentinel

The second step is to create a custom detection rule in Microsoft Sentinel that triggers an alert when a VIP account exceeds the logon threshold within the time window. You can use Kusto Query Language (KQL) to write the query for the detection rule. For

example, you can use this query to detect when an account has more than 6 failed logon attempts in 10 minutes:

```
SigninLogs
| where ResultType == "50126" // Failed sign-in due to bad username or
password
| summarize count() by UserPrincipalName // Count the number of failed sign-
in attempts by user
| where count_ > 6 // Filter by users who have more than 6 failed sign-in
attempts
| join kind=inner ( // Join with the original sign-in logs table
    SigninLogs
    | where ResultType == "50126"
    | summarize min(TimeGenerated), max(TimeGenerated) by UserPrincipalName
// Get the first and last failed sign-in time by user
) on UserPrincipalName
| where (max_TimeGenerated - min_TimeGenerated) < 10m // Filter by users who
have failed sign-in attempts within 10 minutes
| project UserPrincipalName, count_, min_TimeGenerated, max_TimeGenerated //
Select the relevant columns
```

Consider taking the results from this PowerShell script and create a Watchlist in Microsoft Sentinel that can be maintained. Then modify the Analytics Rule to check against the Watchlist when it runs so it only identifies the elevated accounts.

See:

- **Create watchlists in Microsoft Sentinel**
- **Build queries or detection rules with watchlists in Microsoft Sentinel**
- **Manage watchlists in Microsoft Sentinel**

You can use the Microsoft Sentinel portal to create the custom detection rule. You need to provide the following information:

- The name and description of the rule
- The data source and the query for the rule
- The schedule and frequency of the rule execution
- The severity and category of the alert generated by the rule
- The entity mapping and alert details of the rule

Step 3: Investigate and respond to the alert in Microsoft Sentinel

The third step is to investigate and respond to the alert in Microsoft Sentinel when it is triggered by a VIP account that exceeds the logon threshold within the time window. You can use the following guidelines to investigate and respond to the alert:

- Review the alert details, such as the user name, the number of failed logon attempts, and the time range of the failed logon attempts.
- Review the user's investigation priority score and compare it with the rest of the organization. This will help you identify which users pose the greatest risk.
- Review the user's activity history and timeline to gain an understanding of the context and impact of the failed logon attempts. Look for any indicators of compromise or suspicious behavior, such as unusual locations, devices, applications, or actions.
- Review the user's device information and compare it with known device information. Look for any signs of malware infection, compromise, or tampering.
- Review the user's threat intelligence information and compare it with known threat actors or campaigns. Look for any matches or similarities that could indicate a targeted attack or a common technique.
- Contact the user and verify their identity and activity. Ask them if they recognize or remember any of the failed logon attempts or if they have any issues with their account or device.
- Reset the user's password and enable multi-factor authentication (MFA) for their account. This will help prevent further brute-force attacks and improve their account security.

- Create an Incident in Microsoft Sentinel and assign it to an analyst or a team for further investigation and remediation. You can also use playbooks in Microsoft Sentinel to automate and orchestrate common tasks, such as sending notifications, creating tickets, blocking IPs, etc.

Microsoft Sentinel SOC 101: How to Detect and Mitigate Rare Domains Seen in Cloud Logs

Everything including the moo

Microsoft Sentinel is a cloud-native security information and event management (SIEM) solution that helps organizations detect, investigate, and respond to security threats across their hybrid

environments. One of the features of Microsoft Sentinel is the ability to hunt for threats using advanced queries that leverage the Kusto Query Language (KQL). In this article, I'll will explore how to use one of the built-in hunting queries in Microsoft Sentinel to find rare domains seen in cloud logs, and how to mitigate them using automation and orchestration.

What are rare domains and why are they important?

Rare domains are domain names that are not commonly seen or used by legitimate users or applications in an organization's cloud environment. They may indicate malicious or suspicious activity, such as:

- Command and control (C2) communication: attackers may use rare or newly registered domains to communicate with compromised devices or servers in the cloud and send commands or exfiltrate data.
- Phishing or malware delivery: attackers may use rare or spoofed domains to trick users into clicking on malicious links or downloading malicious files from the cloud.
- Data exfiltration: attackers may use rare or encrypted domains to hide the destination of data transfers from the cloud.

Detecting rare domains seen in cloud logs can help security analysts identify potential security incidents and investigate them further using other data sources and tools.

How to use the built-in hunting query for rare domains seen in cloud logs

The following query uses the OfficeActivity table, which contains data from various Microsoft 365 services, such as Exchange Online, SharePoint Online, OneDrive for Business, and Microsoft Teams. The query also uses the ThreatIntelligenceIndicator table, which

can contain data from various threat intelligence providers, such as AlienVault OTX, VirusTotal, etc.

The query works by:

- Filtering the OfficeActivity events by OperationName (such as FileDownloaded, FileUploaded, etc.)
- Joining the domain names with the ThreatIntelligenceIndicator table to check if they are known to be malicious or suspicious
- Calculating the rarity score of each domain name based on its frequency and threat intelligence status
- Sorting the results by rarity score in descending order

```
// Define the time range to look for OfficeActivity events
let Lookback = ago(7d);
// Get the OfficeActivity events and filter by OperationName
let OfficeEvents = OfficeActivity
| where TimeGenerated > Lookback
| where Operation in ("FileDownloaded", "FileUploaded")
| extend Domain = tostring(split(SourceRelativeUrl, "/")[2]) // extract the
domain name from the file URL
| project TimeGenerated, UserId, Operation, SourceFileName, Domain;
// Get the ThreatIntelligenceIndicator records and filter by ThreatType
let TIRecords = ThreatIntelligenceIndicator
| where TimeGenerated > Lookback
| where ThreatType == "DomainName"
| project Domain = NetworkDestinationAsn, ThreatSeverity;
// Join the OfficeEvents and TIRecords tables on Domain
let JoinedEvents = OfficeEvents
| join kind=leftouter (
    TIRecords
) on Domain;
// Calculate the rarity score of each domain based on its frequency and
threat level
// The rarity score is defined as log10(Count) * (ThreatLevel + 1), where
Count is the number of events for each domain and ThreatLevel is a numeric
value from 0 to 3
// The higher the rarity score, the more rare and potentially malicious the
domain is
let RarityScore = JoinedEvents
| summarize Count = count() by Domain, ThreatSeverity // count the number of
events for each domain and threat level combination
| extend RarityScore = log10(Count) * (ThreatSeverity + 1) // calculate the
rarity score
| order by RarityScore desc; // order by rarity score in descending order
// Display the results
RarityScore
```

The query can be customized by changing the parameters at the beginning of the query, such as:

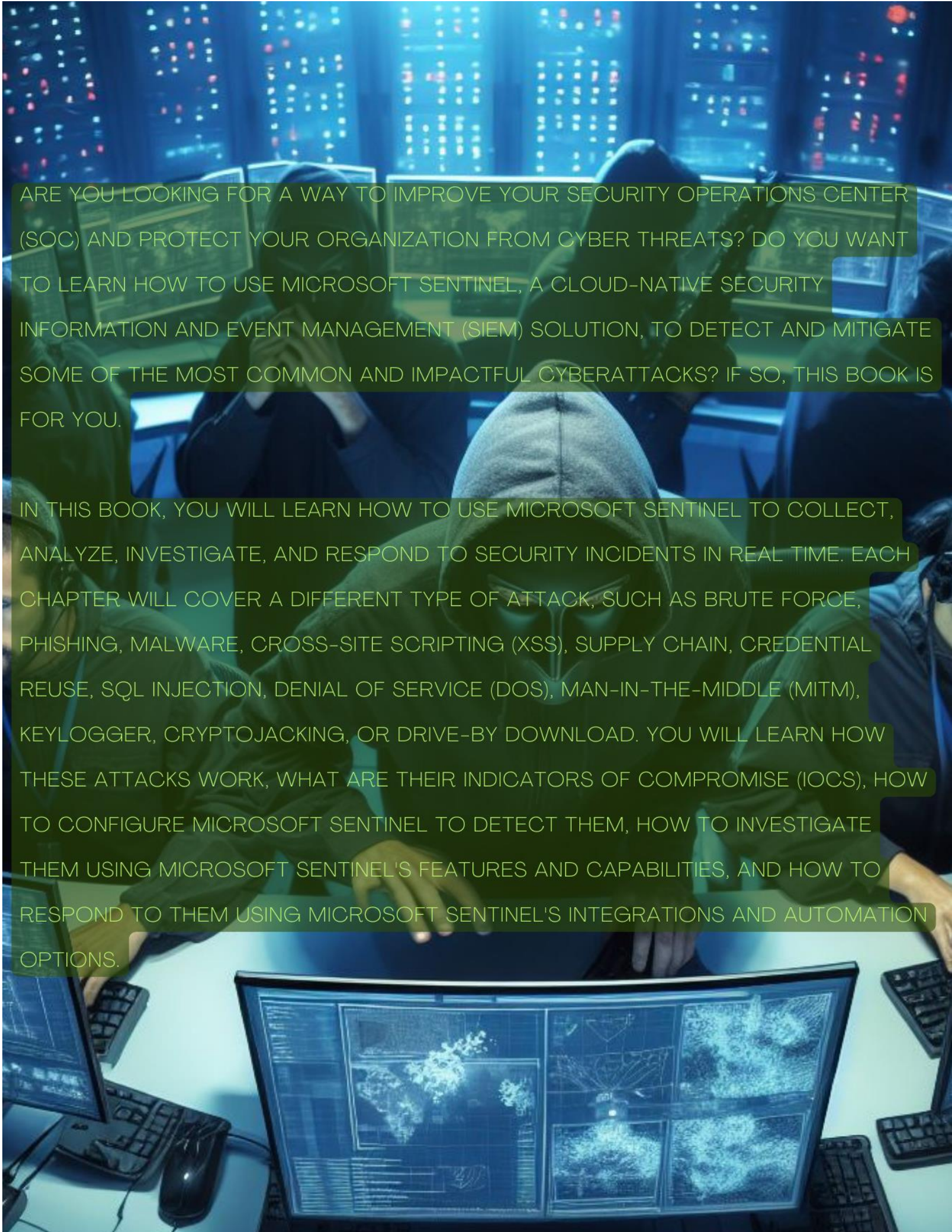
- TimeRange: the time range to search for events
- OperationNameList: the list of operation names to filter by
- ResultStatusList: the list of result statuses to filter by
- DomainRarityThreshold: the threshold for rarity score to filter by

The query can be run manually or scheduled to run periodically. The results can be viewed in a table or a chart format. The results can also be exported to a CSV file or a Power BI report for further analysis.

Once the Analytics Rule is created, it will run according to the specified schedule and create incidents based on the query results. The incidents can be viewed and managed from the Incidents dashboard. The incidents can also trigger other automated responses, such as sending an email notification, creating a ticket in a ticketing system, blocking a domain in a firewall, etc.

Summary

In this article, we learned how to use Microsoft Sentinel to detect and mitigate rare domains seen in cloud logs. We used one of the built-in hunting queries to find rare domains based on their frequency and threat intelligence status. We also used automation and orchestration capabilities to create incidents and respond to rare domains. Microsoft Sentinel is a powerful solution that can help organizations improve their security posture and reduce their attack surface in the cloud.



ARE YOU LOOKING FOR A WAY TO IMPROVE YOUR SECURITY OPERATIONS CENTER (SOC) AND PROTECT YOUR ORGANIZATION FROM CYBER THREATS? DO YOU WANT TO LEARN HOW TO USE MICROSOFT SENTINEL, A CLOUD-NATIVE SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) SOLUTION, TO DETECT AND MITIGATE SOME OF THE MOST COMMON AND IMPACTFUL CYBERATTACKS? IF SO, THIS BOOK IS FOR YOU.

IN THIS BOOK, YOU WILL LEARN HOW TO USE MICROSOFT SENTINEL TO COLLECT, ANALYZE, INVESTIGATE, AND RESPOND TO SECURITY INCIDENTS IN REAL TIME. EACH CHAPTER WILL COVER A DIFFERENT TYPE OF ATTACK, SUCH AS BRUTE FORCE, PHISHING, MALWARE, CROSS-SITE SCRIPTING (XSS), SUPPLY CHAIN, CREDENTIAL REUSE, SQL INJECTION, DENIAL OF SERVICE (DOS), MAN-IN-THE-MIDDLE (MITM), KEYLOGGER, CRYPTOJACKING, OR DRIVE-BY DOWNLOAD. YOU WILL LEARN HOW THESE ATTACKS WORK, WHAT ARE THEIR INDICATORS OF COMPROMISE (IOCS), HOW TO CONFIGURE MICROSOFT SENTINEL TO DETECT THEM, HOW TO INVESTIGATE THEM USING MICROSOFT SENTINEL'S FEATURES AND CAPABILITIES, AND HOW TO RESPOND TO THEM USING MICROSOFT SENTINEL'S INTEGRATIONS AND AUTOMATION OPTIONS.