Essential Playbooks for Your Security Operations Center

playbook

MALTEGO

Table of Contents

Introduction

1.

Security Operations Center (SOC) teams stand on the front lines in cybersecurity, keeping our cyber world safe from endless threats. For these teams, every second counts as they work tirelessly to identify and mitigate cyber threats targeting their organizations.

Balancing a rapid response with thorough initial assessments, all while juggling a myriad of tools, processes, and alerts, is a challenge that the teams face every single day, making efficiency both a goal and a must for survival. This is where the strategic importance of SOC playbooks comes into play.

An Overview of SOC playbooks

2.

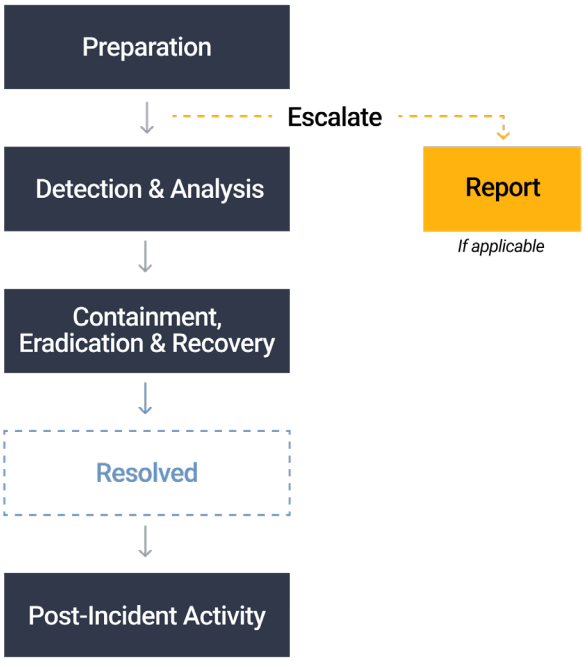
SOC Playbooks are essential for cyber defense, providing clear, step-by-step instructions tailored to various threat scenarios. They serve not merely as documents, but as lifelines that streamline decision-making processes, ensuring that every team member understands their roles and actions to take before, during, and after a security incident. Additionally, playbooks facilitate prompt communication with stakeholders in case of a security breach, thereby enhancing transparency and stakeholder relations.

Although no one-size-fits-all format exists for the SOC playbooks, most teams follow the National Institute of Standards and Technology (NIST)'s standards, including the following sections.

INVESTIGATOR NOTE

It is important to recognize that not every SOC is involved in every stage of incident response. Often, SOCs serve primarily in initial detection and analysis, assisting with tasks that Computer Security Incident Response Teams (CSIRTs) or Incident Response (IR) teams might later expand upon. Thus, in many instances, SOCs act as the foundational layer of incident response. In some scenarios, the term "SOC" might encompass the entire incident response spectrum, though this broader involvement is less typical. Remember these insights as you tailor playbooks to fit your team's needs!

A typical SOC playbook process



1. Preparation: Establishing and maintaining the capability to respond effectively to incidents, including developing policies, plans, and procedures, defining roles, training personnel, and acquiring necessary tools and resources.

2. Detection & Analysis: Identifying and investigating incidents to determine their nature and scope. This includes monitoring for and analyzing potential incidents, effectively using detection tools, and correctly identifying and documenting incidents.

3. Containment, Eradication & Recovery: Limiting the spread of an incident, removing its components, and restoring systems to normal operation. This involves executing a containment strategy, eradicating the incident's cause, and recovering affected systems and data.

4. Post-Incident Activity: Learning from the incident to improve future incident response efforts and overall security posture. This includes conducting a post-incident review, documenting lessons learned, and implementing improvements to policies and controls.

As previously stated, SOCs may play active roles in certain phases of incident response and provide support in others handled by incident response and forensic teams. Below are some of the most common playbooks used by SOC teams and we will explore each topic in detail, following four steps. For insights into enhancing incident response workflows with Maltego, and to streamline investigative processes, consider delving into the **Maltego Handbook for Incident Response**.

1. Ransomware
2. Phishing Attack
3. Malware Infection
4. Vulnerability Response
5. Insider Threats (Data Leakage)

In this section, we will discuss how security teams can significantly enhance their operational effectiveness by incorporating Maltego. We will focus on the Detection & Analysis phase, identified as the pivotal segment of the entire process. It is within this phase that Maltego's capabilities prove most advantageous.

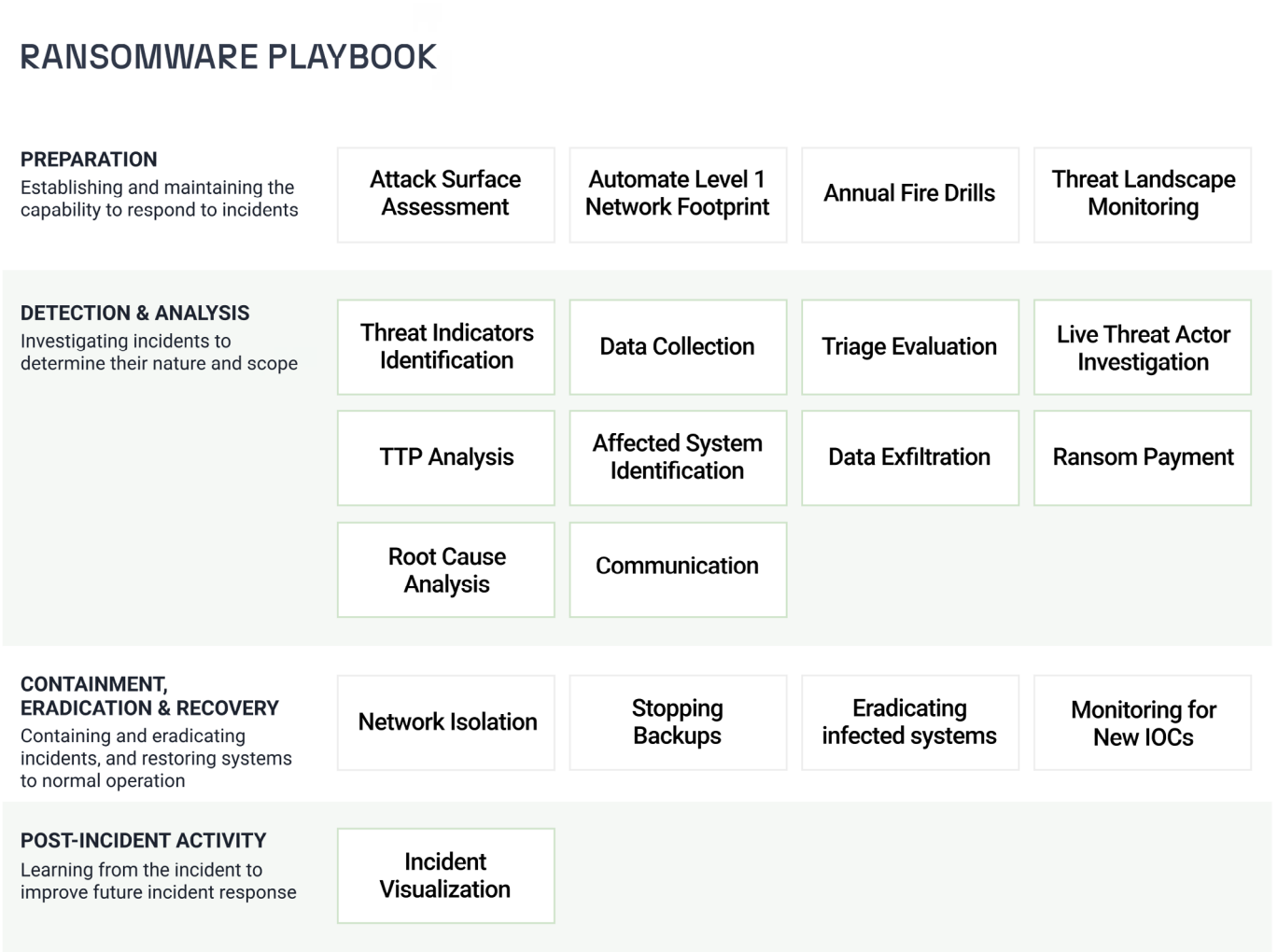
Amplifying SOC Playbooks with Maltego

3.

Security teams are constantly evolving their strategies to respond to and combat the ever-changing cyber threats. Maltego amplifies the SOC playbook's effectiveness by automating data collection and visualization, turning complex datasets into clear, actionable insights, which saves precious time and helps analysts make informed decisions faster. We will demonstrate how Maltego can be utilized for high-level playbook strategies and conduct a brief investigation using Maltego.

Ransomware

Maltego enables teams to quickly assess the impact and scope of a ransomware attack and understand the methods through which threat actors control their victims, including uncovering malicious infrastructure such as command and control servers. By speeding up the aggregation and analysis of indicators of compromise (IOCs), Maltego helps identify patterns and connections that might go unnoticed.



PREPARATION

- **Attack Surface:** Perform an attack surface assessment to identify and catalog all externally exposed hosts, including those potentially unknown to the organization. Regularly update the asset list to reflect the current state of the network environment.
- **Automated Level 1 Network Footprint:** Efficiently conduct network footprinting with Maltego Machines, saving you considerable time on information gathering, processing, and visualization.
- **Drills:** Conduct annual cybersecurity exercises to simulate ransomware attack scenarios. This practice helps validate the effectiveness of the playbook and the organization's readiness to respond to actual incidents.
- **Threat Landscape Monitoring:** Continuously monitor and analyze threat intelligence to stay informed about emerging threats to the organization, industry-specific risks, and evolving ransomware tactics. Incorporate various sources to obtain a comprehensive threat perspective.

DETECTION & ANALYSIS

- **Identify Threat Indicators:** Aggregate and analyze indicators from security solutions such as SIEMs like Splunk, AV/EDR, ticketing systems, and notifications from security personnel or users to identify potential ransomware incidents quickly.
- **Data Collection:** Collect detailed information on indicators like Bitcoin addresses, emails, file hashes, file behaviors, domain reputations, and IP communications. Enrich this data using third-party sources to assess the severity and impact of the threat.
- **Triage:** Evaluate the impact (e.g., data destruction, proliferation) and scope (e.g., number of affected hosts, additional IOCs) to prioritize response efforts. Determine if the event is a false positive; if yes, stop; if no, proceed with analysis.
- **Live Threat Actor:** If a live threat actor is identified, utilize Maltego for real-time investigations and support to block new IOCs as they are identified.
- **Identify Ransomware Family:** Use OpenCTI to identify the ransomware's TTPs, determine decryption possibilities, and identify the targeted OS. This information aids in tailoring the response strategy.
- **Identify Affected Systems Type:** Determine the types of affected systems (servers, workstations) using tools like Splunk to understand the attack's breadth and depth.
- **Data Exfiltration:** If data exfiltration is suspected, activate the Data Loss Playbook to mitigate and assess the damage.
- **Pay the Ransom:** Assess the legality and advisability of paying the ransom, acknowledging that not all ransomware threat actors are sanctioned entities, paying criminals is illegal in some jurisdictions and generally discouraged according to Business Continuity Plans (BCPs). Perform a thorough blockchain analysis to fully understand the implications and potential risks associated with a ransom payment.
- **Root Cause Analysis:** Conduct a thorough analysis to identify the attack's root cause, which is crucial for preventing future incidents.
- **Send Communication:** Communicate effectively with all stakeholders throughout the incident to ensure coordinated and informed response actions.

CONTAINMENT, ERADICATION & RECOVERY

- **Network Isolation:** Block system-to-system communication to prevent the spread of ransomware. Disconnect affected systems from the network as well as any shared drives. And make sure that threat actors can no longer control the infected systems.
- **Stop Backups:** Temporarily halt backup processes to prevent backup data encryption. Verify the integrity of the latest stable ver-

sion of backups and preserve latest backups with additional security measures.

- **Malware Infection:** Follow the Malware Playbook to remove ransomware and other implants to remotely control and preserve access from infected systems and prevent reinfection.
- **Monitor for New IOCs:** Continuously monitor new IOCs and the evolution of TTPs from the same incident or campaign during and after the containment phase to detect any lingering threats or additional points of compromise.

POST-INCIDENT ACTIVITY

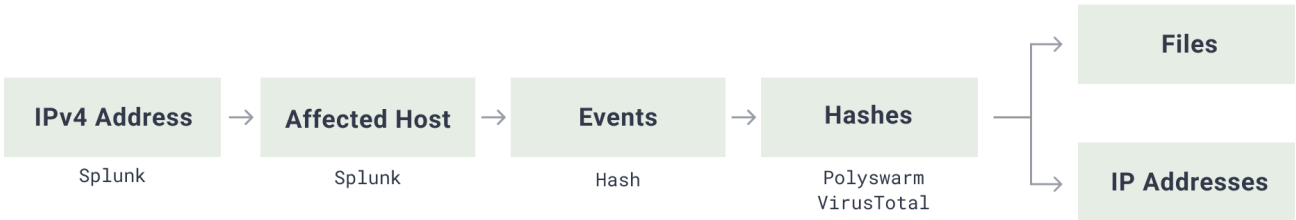
- **Incident Visualization:** Use Maltego to create a comprehensive visualization of the incident, depicting the relationships between hosts, IOCs, and the attack's progression. This visualization aids in understanding the incident's full scope and can be used for debriefing and lessons learned.

A BRIEF INVESTIGATION IN MALTEGO

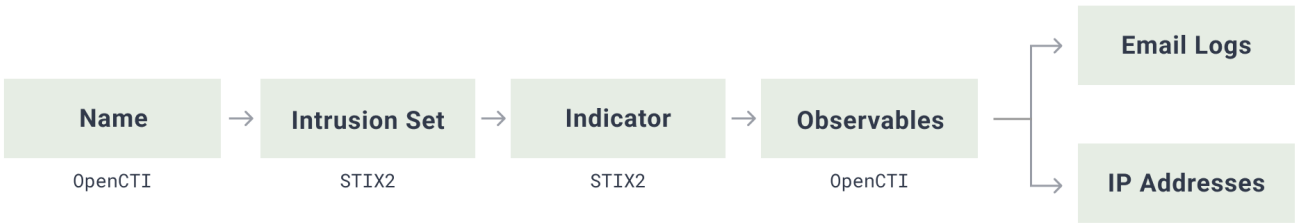
RANSOMWARE WORKFLOW

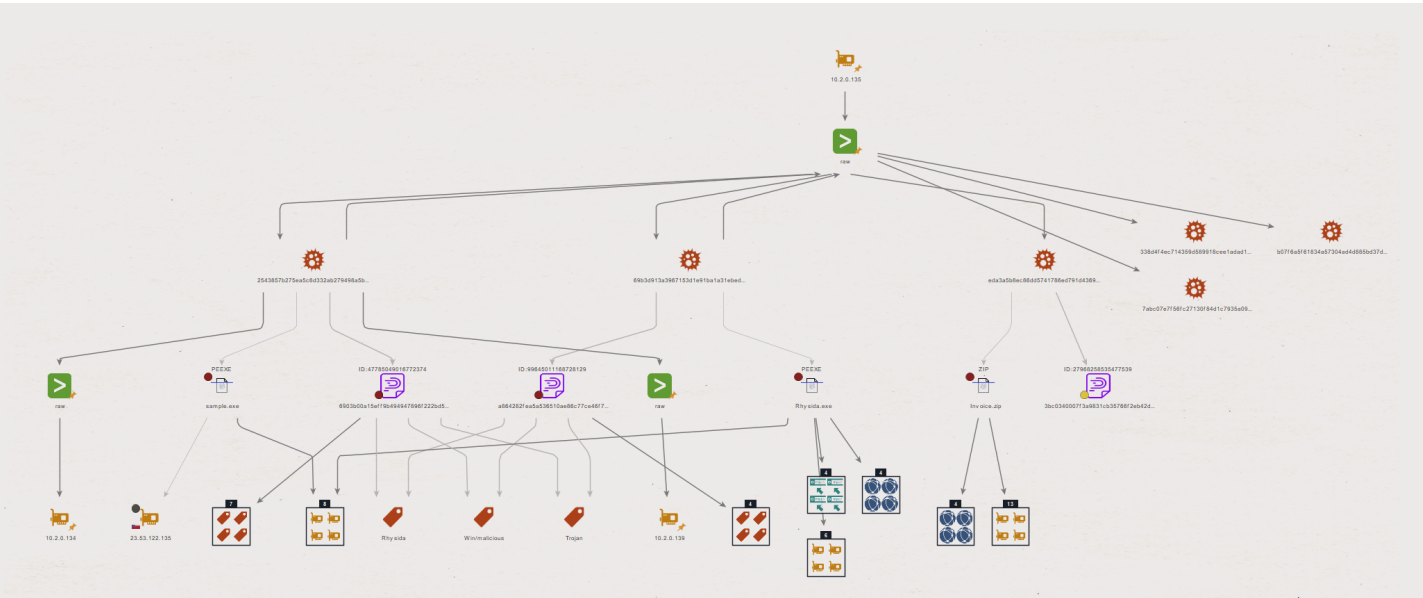
Detection & Analysis with Maltego

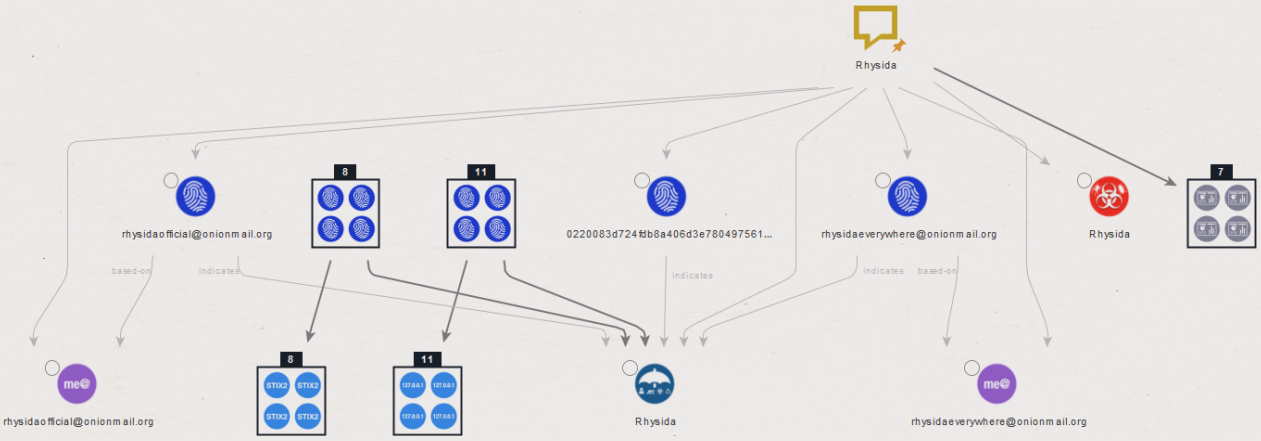
GENERAL



FURTHER INVESTIGATION







This investigation represents the detection and analysis phase of the ransomware investigation with Maltego. Our starting point is the IPv4 address from the malware sample; Rhysida ransomware.

Step 1: Drop an IPv4 Address and update it with the address of the affected host.

Step 2: Run the Transform **Get Malware Attacks Events [Splunk]** to identify any malware events associated with the host. Other early unclear events could lead to identifying an infection by investigating suspicious outbound connections. However, in our case, we will focus directly on malware attack events.

Step 3: Select all events Entities and run **To FileHash [Hash]** to extract the associated hashes. You will see hash Entities as a result.

Step 4: Select the hash Entities and run **Lookup by Hash [Polyswarm]**. This Hub item is included in the Maltego Selection for CTI.

Step 5. Select the result with the red dot and run the Transform **To Tags [Polyswarm]** to identify the malware family. This will help verify if there's a connection to the identified malware.

INVESTIGATION TIP

To find additional affected hosts, run the **Search All Events [Splunk]** Transform on the hashes associated with the same Polyswarm Entities.

Step 6: Select the hashes associated with the ransomware and run the Transform **To VirusTotal File [VirusTotal Public API]** to gather more IoCs.

Step 7: Select the file Entities and run **To Contacted IP Addresses [VirusTotal Public API]** and **To Contacted Domains [VirusTotal Public API]** Transforms. After this step, if the team wants to know about the malware(Rhysida) as much as possible, they can use the OpenCTI integration on a new graph.

Step 8: Paste the name of the ransomware family as a phrase Entity and run the Transform **Search by Phrase [OpenCTI]**.

Step 9: Select the STIX2 intrusion set and run the **Set to Indicators [STIX2]**.

Step 10: Select all STIX2 indicator Entities and run the **Indicator to all Observables [OpenCTI]**.

Step 11: Check email logs for emails generated from the identified Domains as well as connections made to/from the IP addresses by using the **Get All Mail Events [Splunk]** Transform.

Phishing Attack

Phishing attacks are among the most common threats, requiring rapid identification and mitigation. Maltego enhances this playbook by automating the tracing of phishing emails back to their source, effectively revealing the attacker's infrastructure.

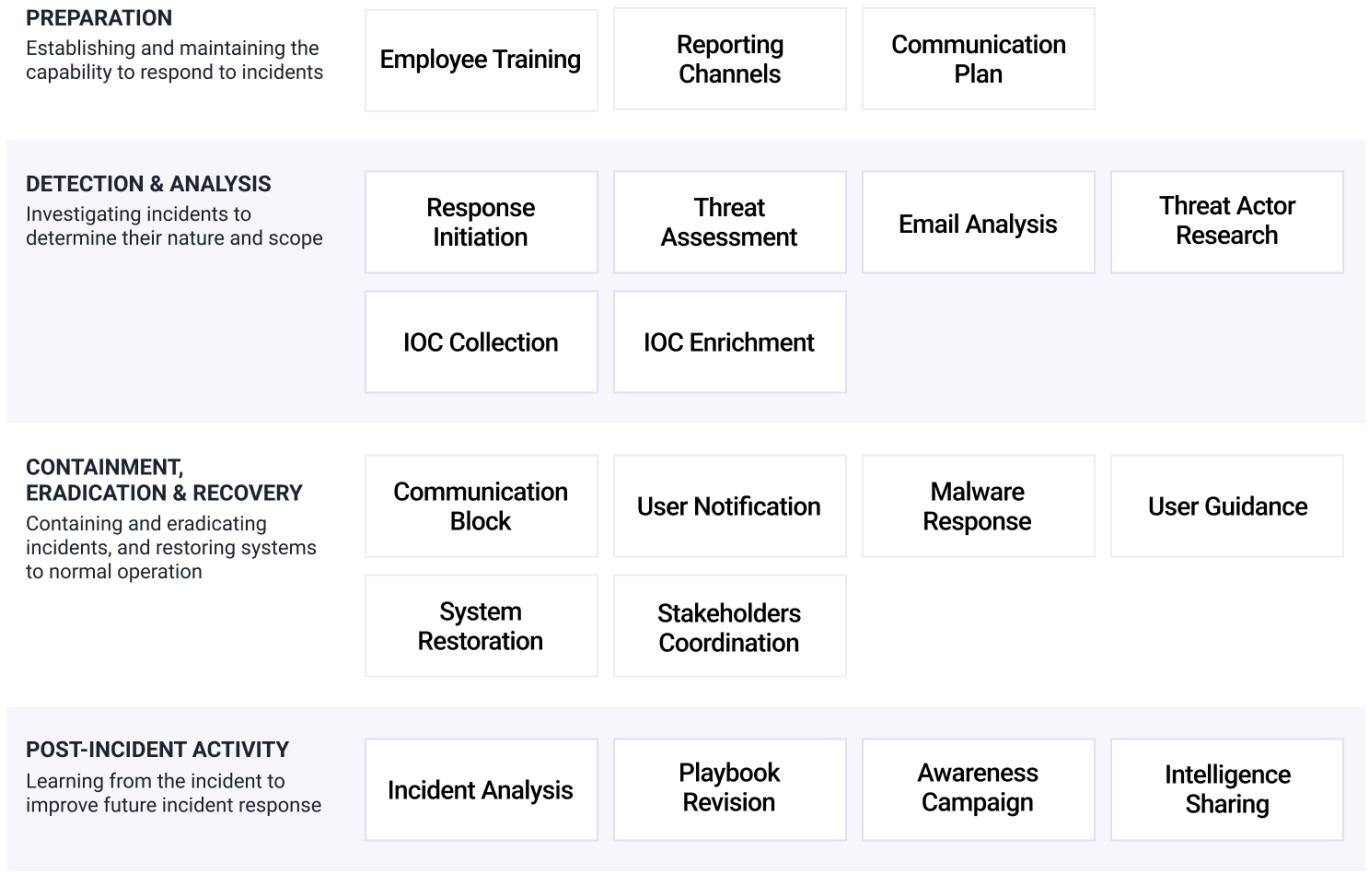
PREPARATION

- **Employee Training:** Conduct regular training sessions to recognize and report phishing attempts. Use simulated phishing exercises to enhance awareness and preparedness.
- **Reporting Mechanisms:** Establish clear and easy-to-use channels for employees and customers to report suspected phishing attempts, such as a dedicated email address or an internal reporting tool.
- **Communication Plan:** Develop a communication plan that outlines how to notify and guide employees in the event of an ongoing phishing campaign.

DETECTION & ANALYSIS

- **Response Initiation:** Upon receipt of a reported phishing email, initiate the incident response protocol to assess the threat.
- **Email Analysis:** Examine the email header to trace the source, analyze embedded links for malicious content, and inspect attachments for potential malware. Perform a lateral analysis to identify other victims targeted by the same threat/campaign.
- **IOC Collection:** Gather IOCs such as sender email addresses, URLs, IP addresses, and file hashes from the phishing email.
- **IOC Enrichment:** Enrich the collected IOCs. For example, analyze URLs with tools like VirusTotal and check IP addresses against threat intelligence databases to ascertain

PHISHING ATTACK PLAYBOOK



their reputation.

- **Threat Actor Research:** To understand the attack's context and potential impact, utilize Maltego to investigate the connections between the collected IOCs and known TTPs with the corresponding threat actors or campaigns.

CONTAINMENT, ERADICATION & RECOVERY

- **Block:** Block the sender's email address, related mail exchanges (if applicable), and malicious URLs or IP addresses at the network perimeter. Also proactively block or reset potentially compromised credentials.
- **User Notification:** Inform potentially affected users to avoid interaction with phishing emails, especially in highly relevant targeted campaigns.
- **Malware Response:** If the phishing email contains attachments, conduct a thorough scan using antivirus software to detect and remove any embedded malware, such as Infostealers.
- **Coordination with stakeholders:** In case third-party platforms are involved, properly coordinate all the steps for containment and evidence collection needed to assess the impact with stakeholders.
- **User Guidance:** Provide affected users with specific instructions for remediation, such as changing passwords or monitoring account activity if they interacted with the phishing email.
- **System Restoration:** If the phishing a¬ttack compromised any systems, follow the organization's established protocols for system restoration and data recovery.

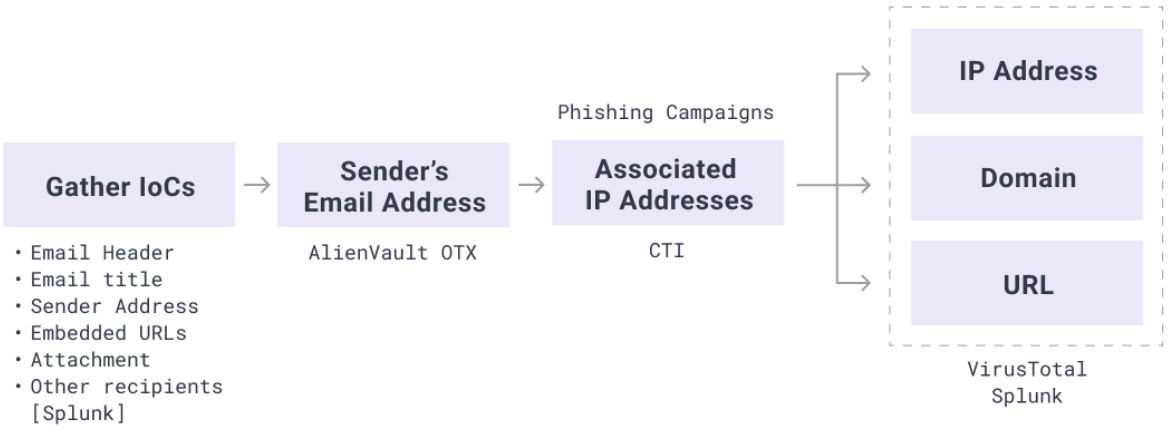
POST-INCIDENT ACTIVITY

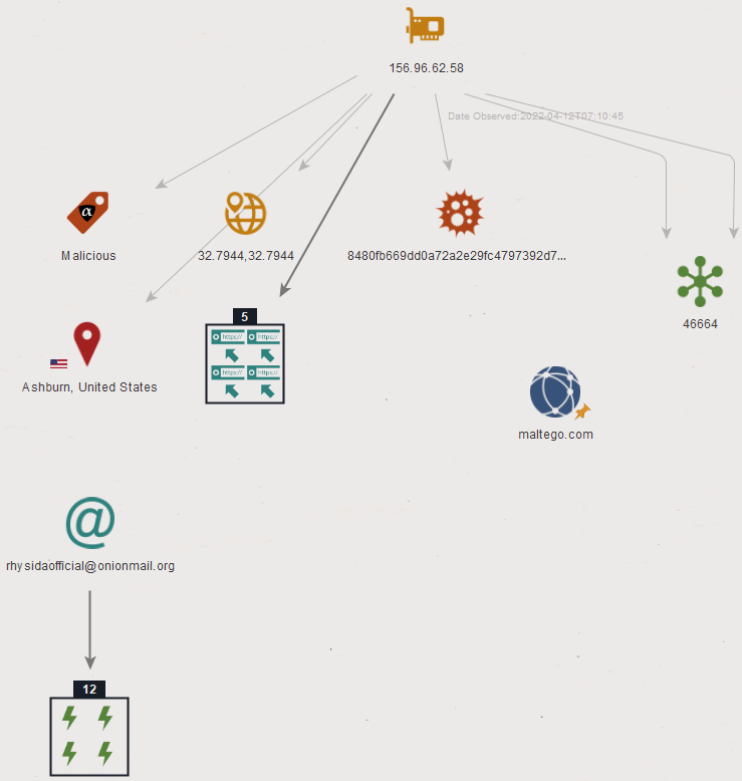
- **Incident Analysis:** Conduct a detailed review of the phishing attack to identify any lapses in the organization's defenses and user responses.
- **Playbook Revision:** Update the phishing response playbook and employee training materials based on insights from the incident analysis.
- **Awareness Campaign:** Use the incident as a case study to enhance organizational awareness and educate employees about the specifics of the phishing tactic encountered.
- **Intelligence Sharing:** Share anonymized information about the phishing attack with industry peers and relevant threat intelligence platforms to contribute to collective cybersecurity knowledge.

A BRIEF INVESTIGATION IN MALTEGO

PHISHING ATTACK WORKFLOW

Detection & Analysis with Maltego





This investigation represents the detection and analysis phase of the phishing attack investigation with Maltego. Begin with the email header of the phishing email to obtain the IP address and domain associated with the email. The graph on the left illustrates the simple enrichment process applied to the IP address.

Step 1: Gather IoCs from the suspected email such as email headers, sender address, embedded URLs, attachment hashes, and email title.

Step 2: Create corresponding Entities for each IoC. Custom transforms can be developed to automate the extraction and collection of IoCs from email platforms.

Step 3: Select all Entities and run **Search All Events [Splunk]** to find out about the other recipients of this phishing email.

Step 4: Run **Search Pulses [OTX]** Transform on the sender's email address to detect any associated phishing campaigns.

Step 5: Select the associated IP Address Entities and Run all the Transforms under the **Enrich IP Addresses [CTI]** from the menu. This Hub item is included in the Maltego Selection for CTI.

Step 6: Select all the URL Entities and run **Search Phishing IPs [CTI]**.

Step 7: Search for associated malicious files by selecting the IP address, domain, and URL Entities and running the **To Communicating Files [VirusTotal Public API]** Transform.

Step 8: Verify any newly acquired IoCs by running **Search All Events [Splunk]** Transform

Step 9: Block the sender and notify affected users. During the process, if malware is observed, then follow the procedure of the Malware Playbook on the next page.

With Maltego, analysts can visualize an entire phishing campaign in a single graph, identify related domains, emails, and malicious files, and accelerate the response time from detection to mitigation.

Malware Infection

When discussing malware threats, understanding the scope and connections of an attack is crucial. Maltego's ability to automate the collection and analysis of IOCs facilitates a deeper understanding of the malware's origins, mechanisms, and potential evolutions.

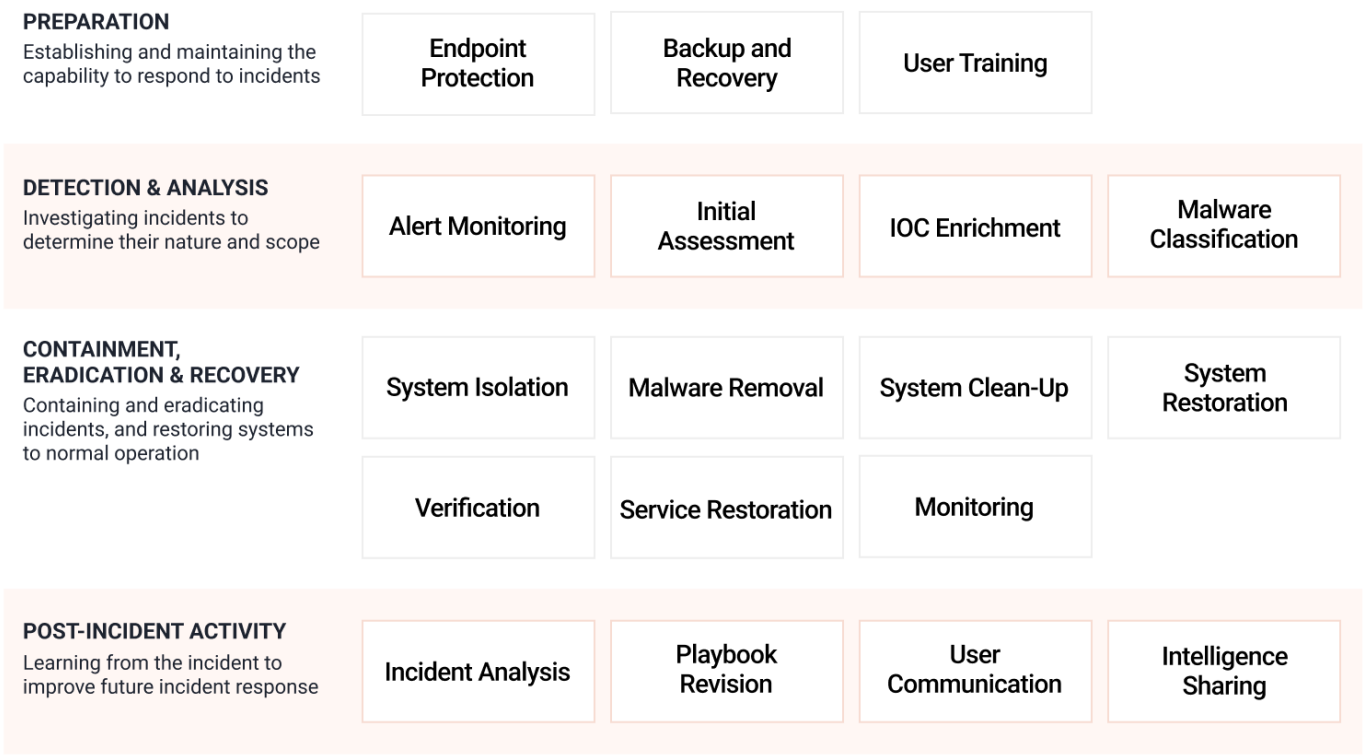
PREPARATION

- **Endpoint Protection:** Ensure that all endpoints are equipped with updated Endpoint Detection and Response (EDR) systems. Regularly scan systems to detect and remediate potential threats.
- **Backup and Recovery:** Maintain regular backups of critical data and systems. Test the recovery process to ensure data can be restored quickly and effectively in the event of a malware infection.
- **User Training:** Provide ongoing training to employees on recognizing and avoiding malicious content, including email attachments, links, suspicious websites, and giving them indications in case of a potential infection.

DETECTION & ANALYSIS

- **Alert Monitoring:** Continuously monitor and analyze alerts from endpoint protection, SIEM platforms, and network intrusion detection and prevention systems for signs of potential malware infections.
- **Initial Assessment:** Upon detecting a potential malware infection, collect and analyze relevant data, such as suspicious file hashes, IP addresses, URLs, and system behavior from the infected system or using existing malware sandboxes.
- **IOC Enrichment:** Enrich the collected IoCs by using your Threat Intelligence Platform or Intelligence Feeds. For example, submitting file hashes to VirusTotal to check against known malware signatures and analyze IP addresses and URLs for known malicious activities.
- **Malware Classification:** Determine the type of malware (e.g., ransomware, spyware, trojan) to inform the response strategy. To understand the malware's capabilities and impact, utilize online databases and malware

MALWARE INFECTION PLAYBOOK



analysis platforms. Intelligence Providers such as Mandiant or Crowdstrike might have useful information to understand the threat.

CONTAINMENT, ERADICATION & RECOVERY

- **System Isolation:** Isolate affected systems from the network to prevent the spread of malware. This may involve disconnecting from the network or shutting down the system.
- **Malware Removal:** Utilize endpoint protection tools to remove the malware from infected systems. Manual removal or rebuilding from scratch may be necessary for sophisticated malware.
- **System Clean-Up:** Perform a clean-up of the infected systems, removing any remnants of the malware and restoring altered settings, or providing a clean-safe image of the system.
- **System Restoration:** Restore affected systems from clean backups if necessary. Ensure that systems are fully remediated before reconnecting them to the network.
- **Verification:** Conduct a post-recovery scan to ensure that the malware has been completely removed and that systems are secure.
- **Service Restoration:** Gradually restore services and monitor system behavior to ensure stability and the absence of malicious activity.
- **Monitoring:** Perform close monitoring of the impacted systems for a reasonable amount of time to verify that no suspicious activity arises after the cleaning and restoration. If any suspicious activity is detected, this might indicate the threat was not completely removed.

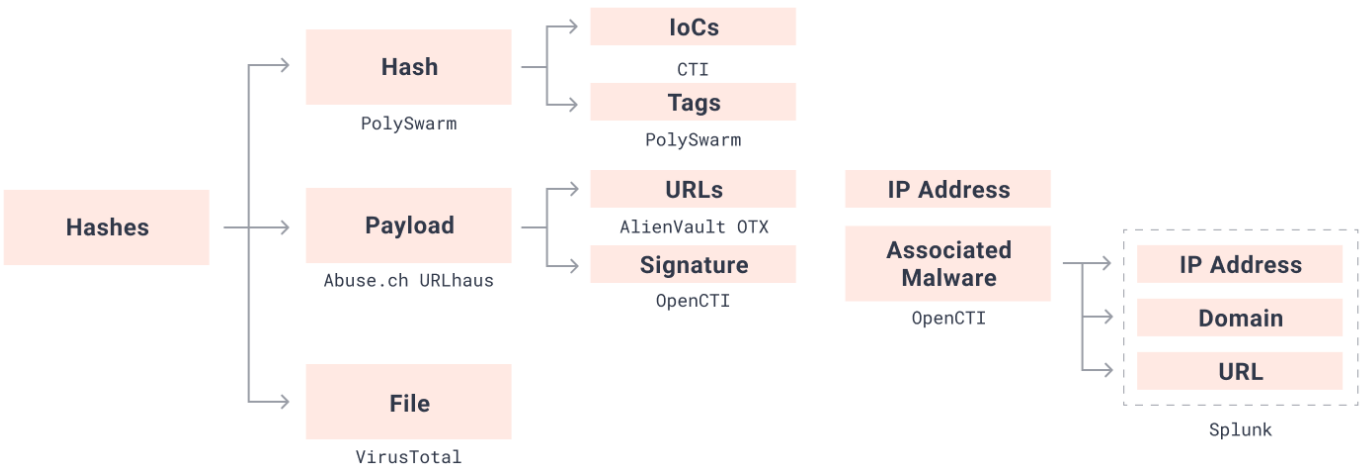
POST-INCIDENT ACTIVITY

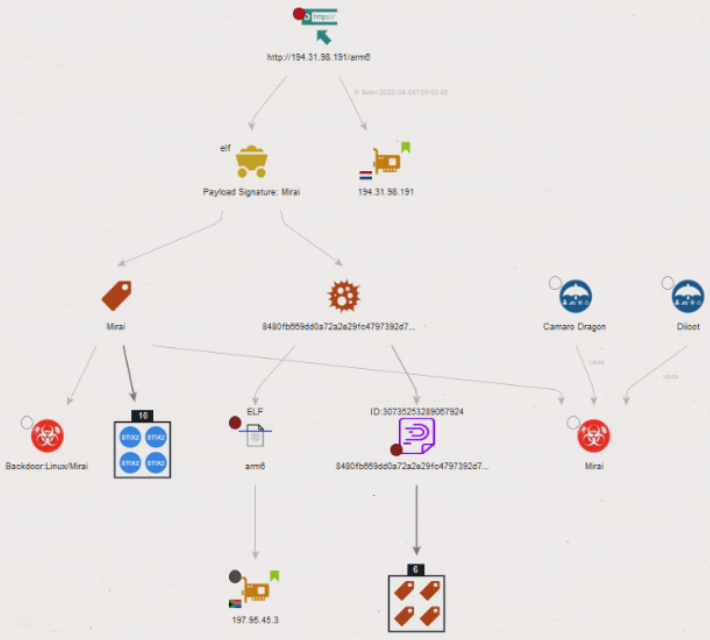
- **Incident Analysis:** Conduct a detailed review of the incident to identify the malware's entry point, propagation path, and impact. Determine the effectiveness of the response and containment efforts.
- **Playbook Revision:** Update the malware response playbook based on the insights gained from the incident. Adjust security controls and response procedures as needed.
- **User Communication:** Inform affected users about the incident and any necessary actions they need to take, such as changing passwords or monitoring account activity.
- **Intelligence Sharing:** Share anonymized indicators of compromise and other relevant information about the malware incident with the cybersecurity community to aid in broader threat intelligence efforts.

A BRIEF INVESTIGATION IN MALTEGO

MALWARE INFECTION WORKFLOW

Detection & Analysis with Maltego





This investigation represents the detection and analysis phase of the malware infection investigation with Maltego. It goes through a similar enrichment process as a phishing attack. Let's start investigating. Our starting point is the file hashes and we will be using Mirai (Linux malware) to demonstrate the playbook.

Step 1: Drop suspected file hashes and file names on a new graph in Maltego.

> **INVESTIGATION TIP**
> Determine the specific type of these new Entities, classifying them as Hash or Phrase according to their nature.

Step 2: Select the hash Entities and run the Transforms **Lookup by Hash [Polyswarm], To Payload [URLhaus],** and **To File [VirusTotal Public API]**.

Step 3: Select the Polyswarm Scan Entities from the result and run the **Find IOCs [CTI]** and **To Tags [Polyswarm]** Transforms.

Step 4: Select the Abuse.ch URLhaus Payload Entity and run the **To Payload URLs [URLhaus]** and **To Payload Signature [URLhaus]** Transforms.

Step 5: Select the URL Entities and run the **To IP Addresses [OTX]** Transform.

Step 6: Select the VirusTotal File Entity and run **Communicating Relationships [VirusTotal Public API]** to find out any domains, IPs, or URLs that this file may have communicated with.

Step 7: Select the Abuse.ch Signature Entity and run **Search by Phrase [OpenCTI]** to identify associated malware.

Step 8: Select the STIX2 Malware Entities and run **Malware to Intrusion Sets [OpenCTI]** Transform and group them using this malware.

Step 9: Select the IP Address, domain, and URL Entities, and run the **Get All Traffic Events [Splunk]** Transform to confirm the extent of impact caused by this malware.

Step 10: If malware is associated with ransomware, follow the procedure of the Ransomware Playbook.

With Maltego, security teams can quickly aggregate and analyze data from various sources, mapping out the malware's network and identifying common indicators that could prevent future infections.

Vulnerability Response

When a new vulnerability is announced, Maltego can automate the process of mapping the organization's external digital assets to identify which systems are affected. Integrations like Shodan and Censys provide real-time information on potential exposures.

PREPARATION

- **Regular Scanning:** Implement regular scanning of all systems and applications to detect vulnerabilities using automated scanning tools.
- **Patch Management:** Establish a robust patch management process to ensure the timely application of security patches and updates.
- **Inventory Management:** Maintain an up-to-date inventory of all IT assets, categorizing them by criticality and function to prioritize response efforts.

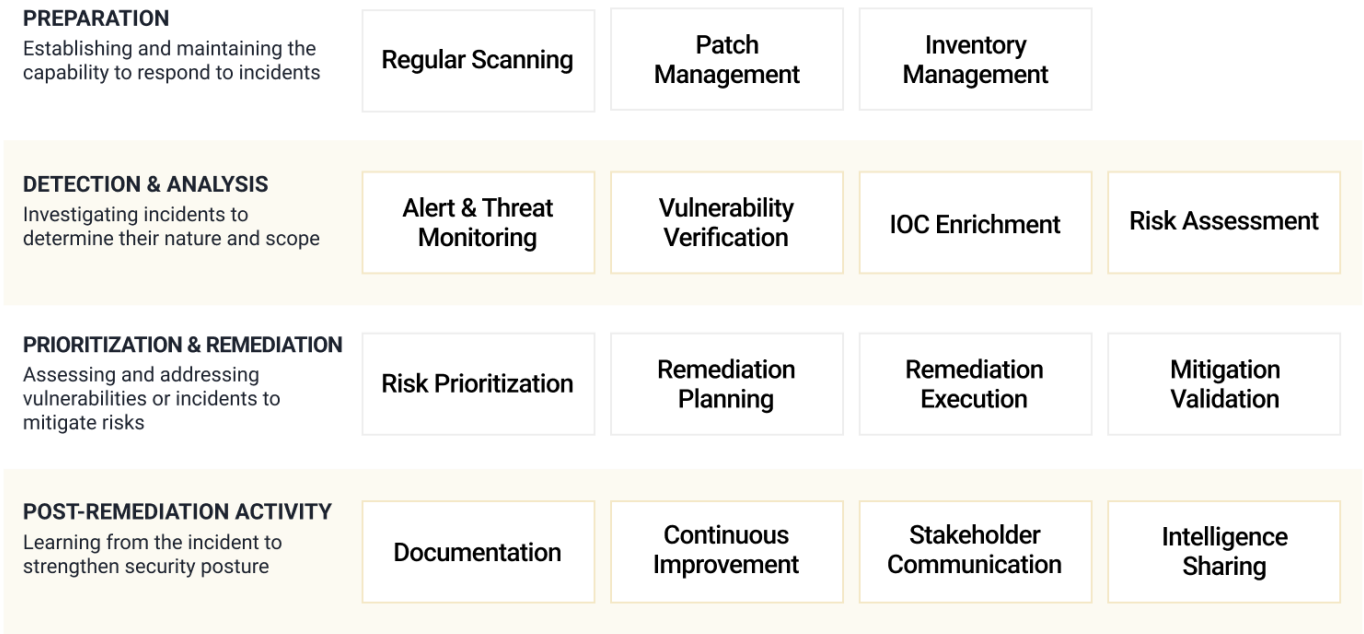
DETECTION & ANALYSIS

- **Alert Monitoring:** Monitor alerts from vulnerability scanning tools and security news feeds to stay informed about new vulnerabilities.
- **Vulnerability Verification:** Verify reported vulnerabilities to confirm their presence and assess their validity and impact on the organization.
- **IOC Enrichment:** Gather more information about vulnerability, including searching for exploits in databases like Vulners or using planforms like Shodan or Censys to understand the exploitability of the vulnerability in the wild.
- **Risk Assessment:** Evaluate the risk associated with vulnerability, considering factors such as the criticality of the affected system, the potential impact of an exploit, and the current threat landscape.
- **Threat monitoring:** activities focused on monitoring the exposed systems while vulnerabilities are patched or mitigated for potential abuse attempts.

PRIORITIZATION & REMEDIATION

- **Risk Prioritization:** Prioritize vulnerabilities based on their risk assessment, focusing

VULNERABILITY RESPONSE PLAYBOOK



first on those that pose the most significant risk to the organization.

- **Remediation Planning:** Develop a remediation plan for each prioritized vulnerability, including applying patches, implementing workarounds, or making configuration changes.
- **Remediation Execution:** Execute the remediation plan, applying patches or other mitigation measures to resolve the vulnerability.
- **Mitigation Validation:** After remediation, verify that the vulnerability has been effectively mitigated and that the fix has not introduced any new issues.
- **Review and Improvement:** Regularly review and update the vulnerability response process based on new insights, changing threat landscapes, and organizational changes.
- **Stakeholder Communication:** Communicate effectively with relevant stakeholders throughout the process, providing updates on the status of vulnerability management and any necessary actions.
- **Intelligence Sharing:** Share anonymized information about encountered vulnerabilities and their mitigation with the cybersecurity community to contribute to collective knowledge and defense.

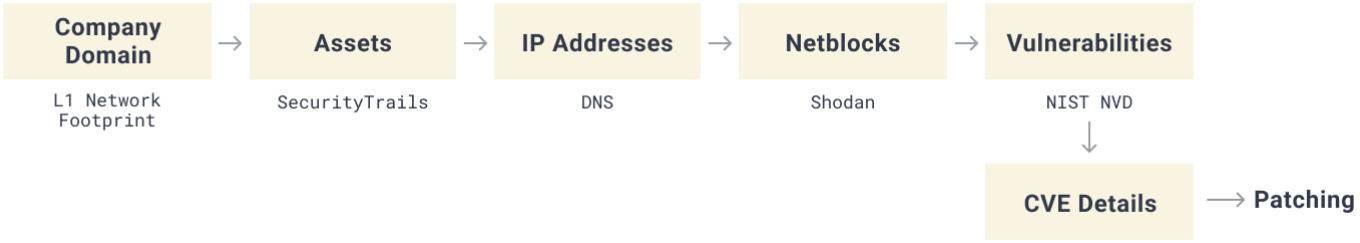
POST-REMEDIATION ACTIVITY

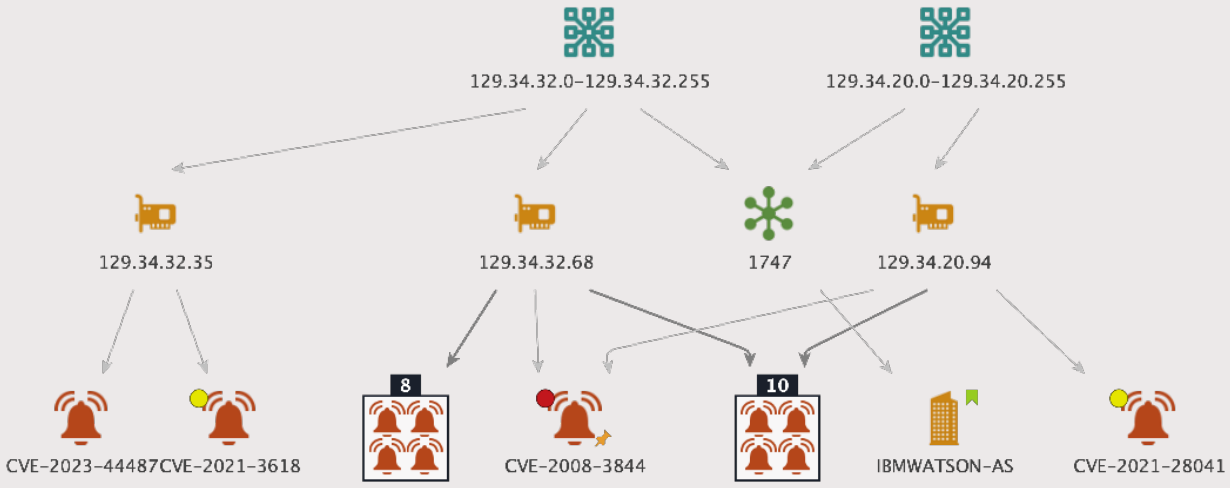
- **Documentation:** Document the vulnerability, its impact, the response actions taken, and any lessons learned to improve future vulnerability response efforts.

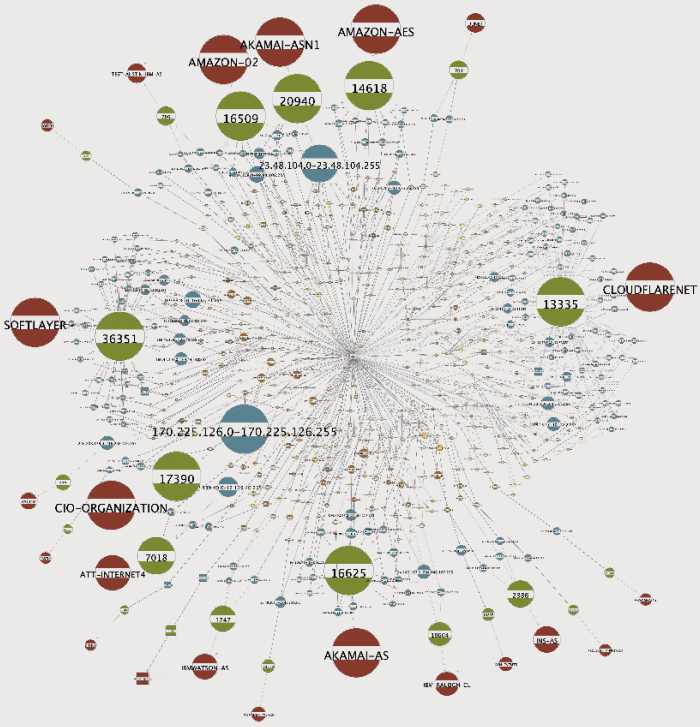
A BRIEF INVESTIGATION IN MALTEGO

VULNERABILITY RESPONSE WORKFLOW

Detection & Analysis with Maltego







This investigation represents the detection and analysis phase of vulnerability investigation with Maltego. Our starting point is the company's domain.

Step 1: Drop the company's domain into Maltego.

Step 2: Run Maltego's Level 1 Network Footprint Machine to get a fresh list of assets owned by the company.

Step 3: Select the assets associated with the company and move them to a new graph.

Step 4. From the selected assets, run the Transform **To DNS Name [SecurityTrails]** to find additional assets.

Step 5: Select the newly discovered Entities(additional assets) and run the **To IP Address [DNS]**.

Step 6: Select netblocks owned by the company and run the **To Vulnerable IP Addresses [Shodan]** Transform.

Step 7: Get a list of vulnerabilities from the IP addresses by running the Transform **To Vulnerabilities [Shodan]**.

Step 8. Select the CVE Entities and run the **Get CVE details [NIST NVD]** Transform to update the Entities with the latest CVSS score.

INVESTIGATOR NOTE

Maltego has a property for the CVSS score, and additionally, employs an overlay (in colors green, yellow, or red) on the Entity to visually indicate the severity of the CVSS score. However, in instances where there are a large number of vulnerabilities, prioritizing becomes essential. To address this, Maltego utilizes the Weight property to represent the CVSS score, calculating the weight of a CVE at its CVSS score multiplied by 10. This enables users to select all CVEs within their graph and sort them by weight in the Detail View, providing a prioritized list of CVEs based on their CVSS scores.

Step 9: Focus on patching vulnerabilities listed in CISA's Known Exploited Vulnerabilities Catalog first. In our investigation, none of the CVEs in the images appear in the catalog.

SOC teams can prioritize and streamline their response to vulnerabilities, ensuring that critical assets are patched or protected promptly, thus reducing the opportunity for attackers to exploit these weaknesses.

Insider Threats

Insider threats pose a unique challenge, requiring identifying potential malicious activity from within the organization. Maltego, with its dark web integrations, enables SOC teams to proactively search for mentions of their company or sensitive data on hidden forums and marketplaces. This capability is crucial for uncovering potential insider threats, such as employees or associates selling unauthorized access to the company's network or confidential data.

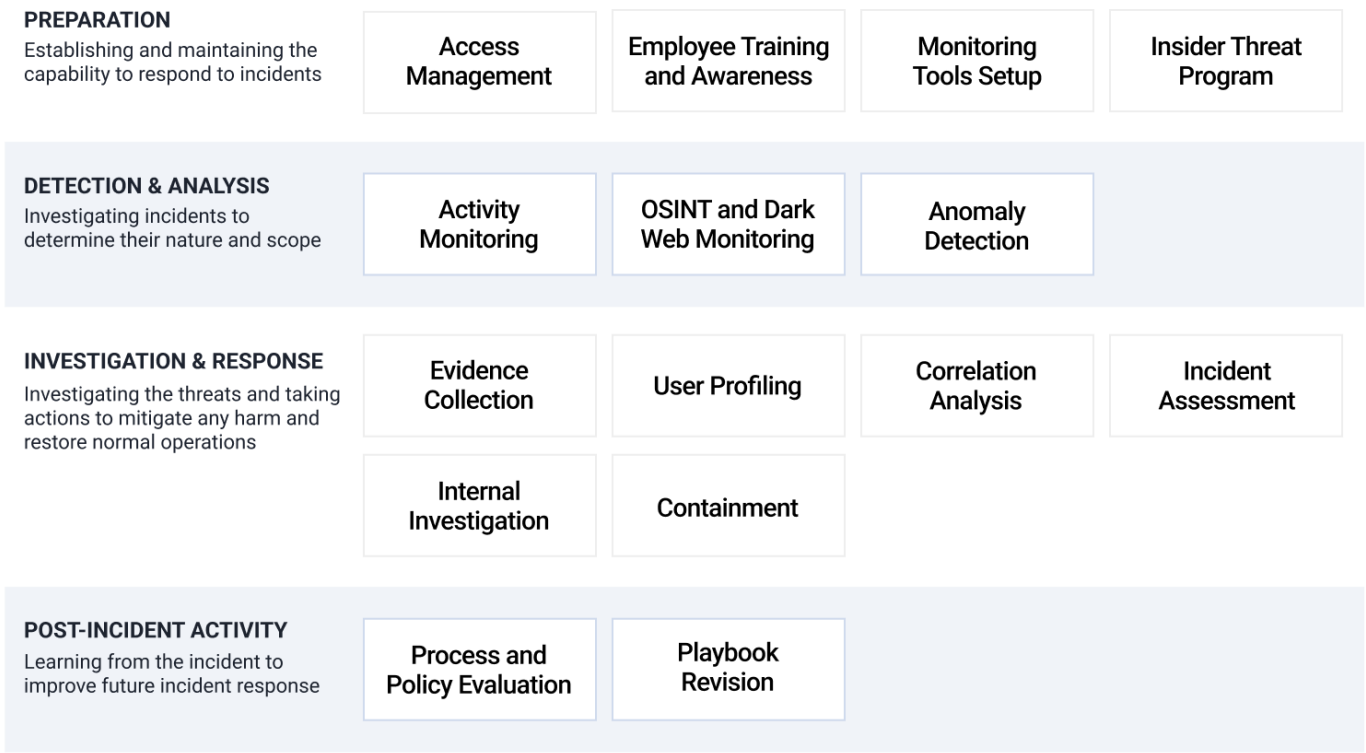
PREPARATION

- **Access Control:** Implement strict access controls and the principle of least privilege. Regularly review and adjust access rights based on job roles and requirements.
- **Employee Training and Awareness:** Conduct regular training sessions to educate employees about insider threat indicators and the importance of safeguarding sensitive information.
- **Insider Threat Program:** Set up an internal program that addresses insider threats so that the proper monitoring, response, and investigative processes and tools are deployed.
- **Monitoring Tools Setup:** Deploy monitoring tools to track user activities and data access patterns within the organization's network. Ensure these tools are configured to alert on suspicious activities.

DETECTION & ANALYSIS

- **Activity Monitoring:** Continuously monitor and analyze user activities for any abnormal behavior that could indicate an insider threat, such as unusual data access or transfer activities using User Behaviour Analytics (UBA)
- **OSINT and Dark Web Monitoring:** Monitor the dark web and other relevant OSINT sources for mentions of your company, leaked sensitive information, or any discussion that might indicate a potential insider threat. This can be done by implementing keyword

INSIDER THREATS PLAYBOOK



searches to identify company-related information or employee activities on forums, social media, and other platforms that could suggest malicious intent or data leakage.
- **Anomaly Detection:** Similar to activity monitoring, apply data analytics to detect anomalies in user behavior that deviate from established patterns, which could signify malicious activities or compromised insider accounts.

INVESTIGATION & RESPONSE

- **Evidence Collection:** Collect and preserve evidence related to the potential insider threat. This may include logs, data access records, and communications.
- **User Profiling:** Profile the suspected insider to understand their motivations, access levels, and recent activities that might have contributed to the threat scenario.
- **Correlation Analysis:** Correlate the suspicious activities with the OSINT findings to establish a comprehensive view of the potential insider threat.
- **Incident Assessment:** Assess the severity of the insider threat based on the collected evidence and analysis. Determine the impact on the organization's assets and operations.
- **Internal Investigation:** Conduct a thorough internal investigation to ascertain the full scope of the insider threat, involving HR, legal, and cybersecurity teams as appropriate.
- **Containment:** Implement immediate containment measures to limit the potential damage. This may involve revoking access rights, isolating systems, or, in severe cases, involving HR or Legal teams and law enforcement.

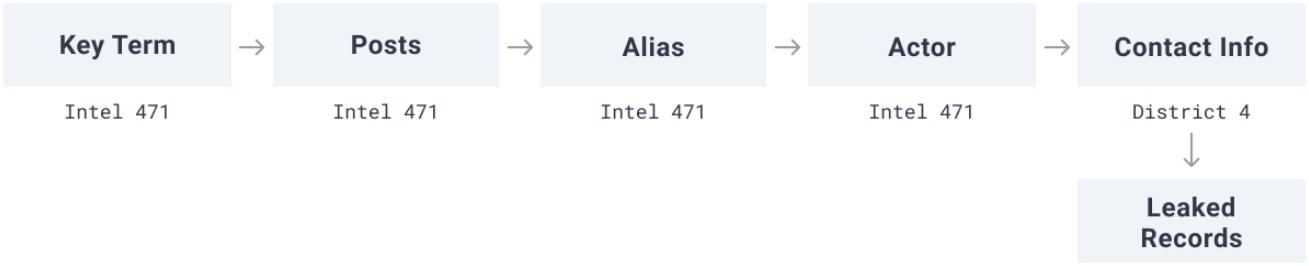
POST-INCIDENT ACTIVITY

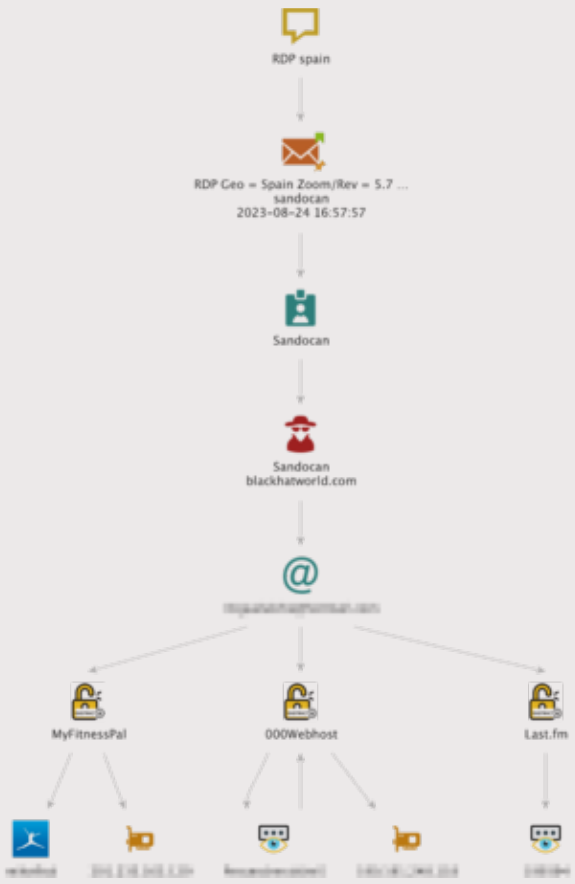
- **Review and Policies Evaluation:** Review the incident to identify any policy or process weaknesses that allowed the insider threat to materialize. Adjust policies and controls accordingly to prevent recurrence.
- **Playbook Revision:** Document the incident, the response effectiveness, and lessons learned. Update the insider threat response playbook and training materials based on these insights.

A BRIEF INVESTIGATION IN MALTEGO

VULNERABILITY RESPONSE WORKFLOW

Detection & Analysis with Maltego





This investigation represents the detection and analysis phase of the insider threats investigation using Maltego. In this instance, we are examining insider data on the dark web and working to uncover identities. This workflow does not cover steps related to addressing anomalous events found in SIEM or other platforms. We will start with the key term "RDP Spain" to demonstrate the playbook.

Step 1: Drop a phrase Entity with a relevant search term for your organization. In our case, we will paste the text "RDP Spain" into Maltego to find messages that could indicate a threat to the organization.

Step 2: Search for messages that include the specific term by running the Transform **Phrase to Post [Intel 471**].

Step 3: Select relevant posts based on their content and the recency of their posting. Organizing them by color helps distinguish them more easily.

INVESTIGATOR NOTE

The color of the bookmarks will assist in this process, for example, red and yellow signify posts from the last month, whereas green and blue indicate older posts.

Step 4: Extract the alias from the post author by running **Post to Alias [Intel 471]**.

Step 5: Pivot to any additional profiles this threat actor may possess, especially if the alias has been reused across platforms, by running the Transform **Alias to Actor [Intel 471]**.

Step 6: Extract contact information from these profiles in the Entities where it is available by running the Transform **Actor to Contact Info [Intel 471]**.

Step 7: Collect breached records in which this information can be found by running **Leaked Records Search [D4]** on email. In this step, the goal is to retrieve passwords, accounts, and IP addresses from the compromised data, which are presumably connected to the initial threat actor. Following this, you can proceed with the person of interest (POI) investigation until all available information has been fully explored. Subsequently, compile your findings to present the case either for internal disciplinary actions or for reporting to law enforcement. This investigation will facilitate a quicker resolution of the case.

Leveraging Maltego's dark web search capabilities allows organizations to extend their threat detection beyond their internal networks, uncovering potential insider threats before they materialize into significant breaches. This proactive stance on insider threat detection protects against data leaks and financial loss. It reinforces the organization's security posture by addressing threats that are often difficult to detect through conventional means.

Enhancing Playbook Automation with Maltego Machines

4.

The Maltego Machines are an absolute must as teams work toward streamlining complex investigative tasks, turning time-consuming processes into efficient, one-click operations.

What kind of Machines are available in Maltego?

1. BUILT-IN MACHINES

Pre-installed and built with Maltego Standard Transforms

2. INTEGRATION-SPECIFIC MACHINES

Included in Maltego's extensive third-party data integrations

3. CUSTOM MACHINES

Can be built by individual users to tailor their workflows

1. Built-in Machines: Maltego has built-in Machines designed to streamline everyday cybersecurity tasks. These ready-to-use Machines cover a wide range of functions, from mapping out attack surfaces to tracking digital footprints, offering SOC teams a quick way to implement automation into their playbooks. By leveraging these machines, teams can immediately enhance operational efficiency without extensive customization.

2. Integration-Specific Machines: Beyond the built-in capabilities, Maltego's extensive ecosystem of integrations with third-party tools introduces additional Machines. These integration-specific Machines are tailored to leverage the strengths of these solutions, providing SOC teams with specialized automation options that extend the functionality of their playbooks.

3. Custom Machine Creation: For teams looking to tailor their workflows closely to their unique operational needs, Maltego offers the flexibility to create custom Machines. Custom Machines can automate specific sequences of tasks, from data collection and enrichment to analysis and visualization, aligning perfectly with the team's established playbooks. Here is a complete guide on how to create custom Machines.

INVESTIGATOR NOTE

Time to explore one of the future capabilities up close as it's built to seamlessly connect all relevant third-party data like SOARs with your own data securely and at scale with automated workflows. Stay tuned for our upcoming capabilities!

Benefits of Playbook Automation with Maltego

5.

FASTER VERIFICATION OF FALSE POSITIVES

Maltego quickly identifies real threats from false positives in cybersecurity, streamlining threat validation.

UNDERSTANDING OF YOUR ATTACK SURFACE

Maltego quickly maps IT infrastructure, helping identify security gaps through unusual activities or configurations.

IDENTIFYING THREAT VECTORS

Maltego enables analysts to quickly identify and address potential threats by comparing threat data with their environment.

TESTING THE PLAYBOOKS

Maltego facilitates the testing of playbooks by simulating scenarios and visualizing outcomes, allowing for continuous improvement.

The automation of SOC playbooks with Maltego brings advantages that fundamentally transform cybersecurity operations.

1. Faster Verification of False Positive: Time is of the essence in cybersecurity. Maltego accelerates distinguishing false positives from genuine threats, streamlining the validation process and allowing teams to focus on actual concerns more swiftly.

2. Understanding of Your Attack Surface: A comprehensive understanding of an organization's IT infrastructure is critical. With Maltego, teams can quickly generate an overview of their network's infrastructure, making it easier to spot unusual activities or configurations that could indicate security gaps.

3. Identifying Threat Vectors (Threat Intel, Threat Hunting): Recognizing potential threat vectors is a proactive defense strategy. Analysts can use Maltego to cross-reference threat data against their environment, spotting potential risks before they escalate into serious threats.

4. Testing the Playbooks (Continuous Refinement): The effectiveness of a SOC playbook is only as good as its testing and refinement process. Maltego facilitates the testing of playbooks by simulating scenarios and visualizing outcomes, allowing for continuous improvement based on real-world data and results.

Conclusion

6.

As we wrap up our exploration of SOC playbooks and the transformative impact of integrating Maltego, it's clear that having robust and actionable playbooks isn't just beneficial; It's imperative.

Maltego's role in this ecosystem is not simply as an investigation platform but as a force multiplier. By enhancing SOC playbooks with its advanced data aggregation, analysis, and visualization capabilities, Maltego enables teams to respond to threats more effectively and anticipate and neutralize them proactively. Integrating Maltego turns the playbooks from static documents into dynamic, interactive manuals that lead teams through the complexities of cybersecurity threats.

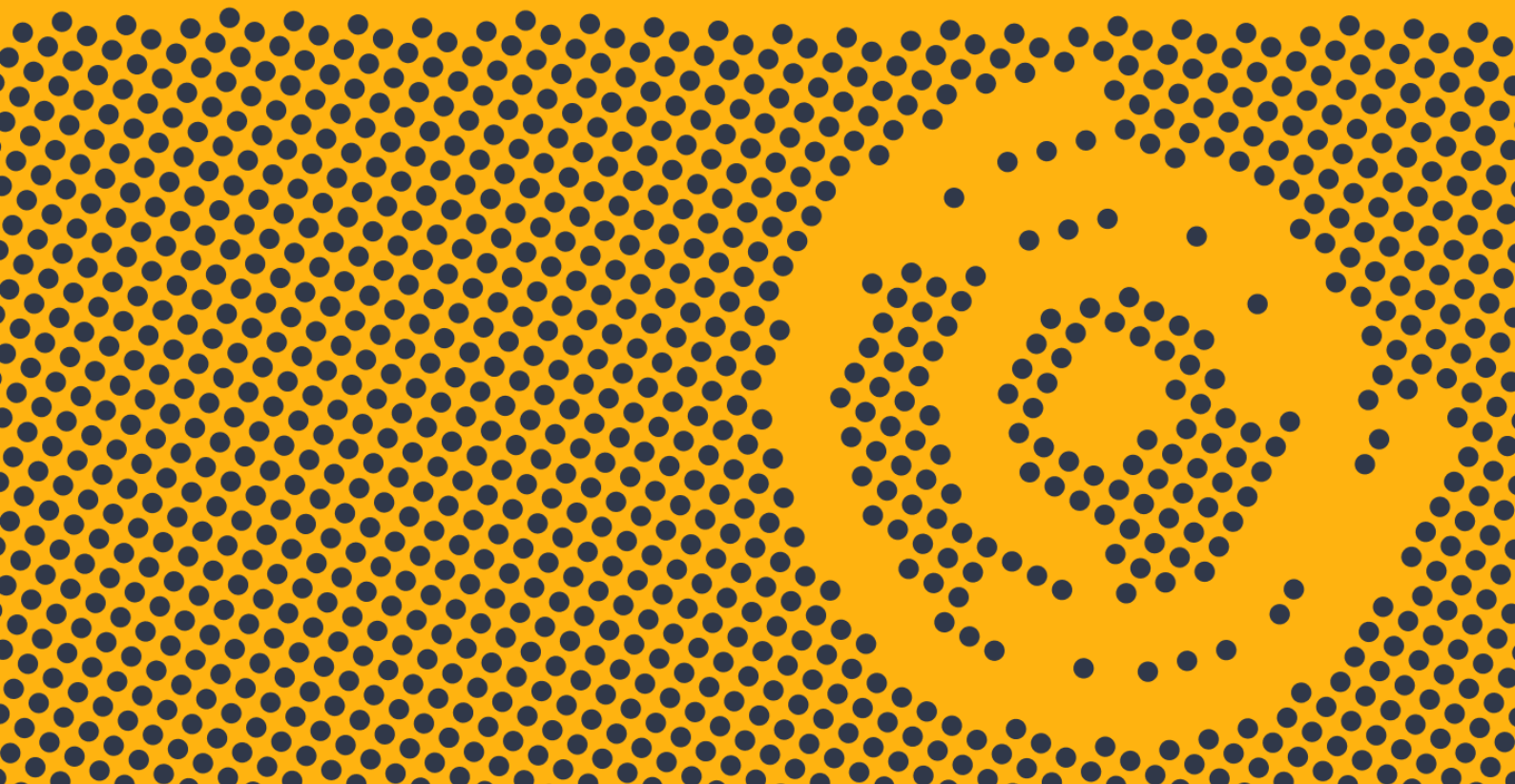
As cybersecurity professionals, we are committed to continuously refining our strategies and tools, which is crucial to staying ahead of adversaries. Embracing the synergy between SOC playbooks and Maltego's capabilities offers a pathway to enhanced security and a more empowered stance in the digital domain. The journey of bolstering our cyber defenses is ongoing, and with tools like Maltego at our disposal, it's a journey that we can undertake with greater confidence and success.

Conducting a thorough detection and analysis of the incident at this stage is paramount, as it lays the groundwork for any subsequent eradication efforts. Lacking this essential detection and analysis, the incident response team risks misallocating their time and resources, thereby potentially hampering their response effectiveness.

Learn more about how we can empower your investigations at **maltego.com**

Maltego is the all-in-one investigation platform that accelerates complex cyber investigations from hours to minutes. The Maltego platform powers preliminary quick OSINT investigations for digital profiling with Maltego Search as well as complex link analysis for large datasets with Maltego Graph. Through Maltego Evidence and Maltego Monitor, the platform enables investigators to collect, monitor, and preserve social media intelligence real-time for prosecution and public safety. Whether cyber threat intelligence teams or law enforcement, Maltego equips your teams with the most essential and relevant data, with out-of-the-box access to common data sources and over 100 ready-made connectors to more. Mine, merge, and map all your essential intelligence in one place, and uncover hidden truths with Maltego!

MINE • MERGE • MAP / DATA



Email: contact@maltego.com
Phone: +49-89-24418490

MALTEGO