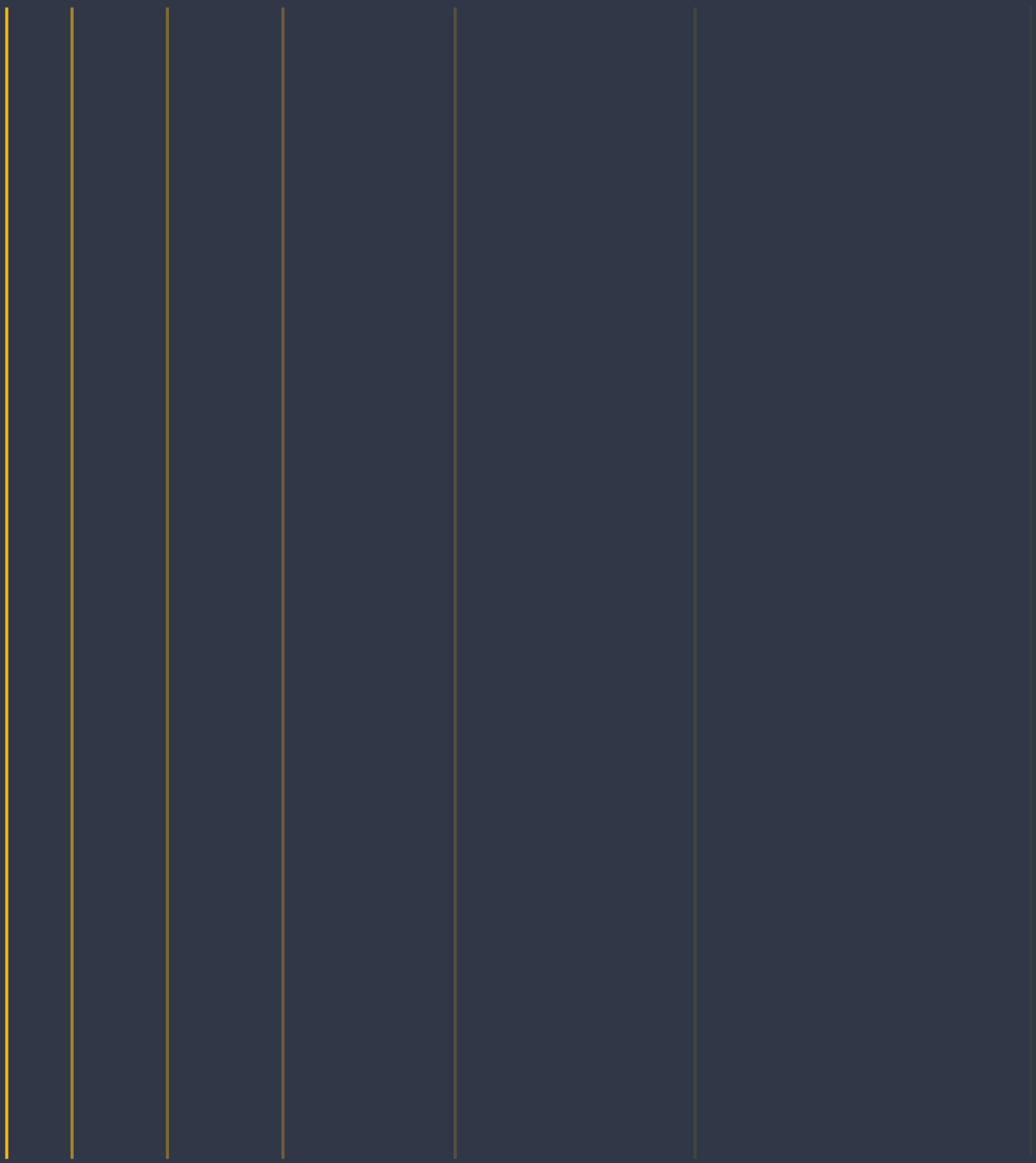
handbook

Maltego Handbook for Incident Response



MALTEGO

Table of Content

About Incident Response

1.

The threats to companies are increasing despite growing expertise and investments in IT security. Companies can no longer protect themselves effectively through prevention alone. It shows that most organizations can't detect initial intrusions (Attivo Survey, 2020)[1]. Nearly two-thirds (64%) of respondents indicated 100 days of dwell time[2]. They must therefore be in a position to react correctly to events in IT systems. As soon as a company detects violation of their security policy and raises a security incident[3], since those events mostly compromise sensitive personal & business data they needs to respond quickly (before major damage occurs). To be able to do this, the methodology of incident handling helps.

While focusing on incident response capabilities, the incident response methodology also underlies processes and procedures that can be applied to any security incident.

As we observe a rise in the number of security incidents, the IR handling processes helps with the use of attack categories to faster identify and scope the problem and apply different response strategies.

For example,the National Institute of Standards and Technology (NIST) categorizes the the types of attack incidents as follows:

- **External/Removable Media:** An attack exe cuted from removable media (e.g. flash drive or CD) or a peripheral device.
- **Attrition**: An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services.
- **Improper Usage:** Any incident resulting from violation of an organization's acceptable usage policies by an authorized user, excluding means from the above categories.
- **Loss or Theft of Equipment:** The loss or theft of a computing device or media used by the organization, such as a laptop or smartphone.
- **Other:** An attack that does not fit into any of the other categories.

Handling the given incidents is essentially the task of Computer Emergency Response Teams or Computer Security Incident Response Teams, also commonly known as CERT or CSIRT.

After an initial assessment of the situation, it is typically necessary to determine whether there is an imminent danger to life and limb (such as in the case of manufacturing and industrial plants), but also a risk of manipulation, sabotage, or exfiltration of sensitive data.

1 https://www.attivonetworks.com/research-from-1200-cybersecurity-professisonals-2019/

2 Dwell time - Time between initial breach and identification of that breach by the victim.

3 https://whatis.techtarget.com/definition/security-incident "Security Incident is an event that may indicate that an organization's systems or data have been compromised or that measures put in place to protect them have failed."

If necessary, such a danger can be contained with immediate measures, whereby the attacker should not be made aware of the existence of the incident response activities if possible. The incident response team then attempts to identify the attacker's current and past activities to a sufficient extent and observe them over a period of time to gain a picture of their capabilities, procedures and possible motives.
Information gathering is essential to tracing the activities of an incident. It ensures sufficient evidence identification and IOC development that will enable the IR team to assess and define the extent of compromise. In this critial stage of the incident response process, Maltego supports IR teams to gather intelligence from both public and paid data sources.

Typical Incident Response Processes

2.

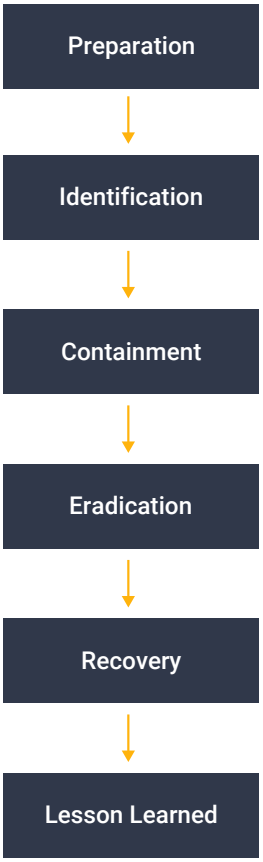
Incident response is the process designed to manage, contain, and—when possible—reduce the consequences of a cyberattack in a fast-paced and efficient manner. Maltego can help incident response teams carry out rapid analyses of digital artifacts that have triggered such a response protocol, align your operations with the best common practices, and shape your existing playbooks.

NIST Cybersecurity & Incident Response Frameworks

The National Institute of Standards and Technology (NIST) is an agency operated by the United States' Department of Commerce which provides standards and recommendations for many technology sectors. These standards and recommendations are usually voluntary for industry but mandatory for government agencies.

NIST created a high-level cybersecurity framework[4] based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk and communications amongst both internal and external organizational stakeholders. The Framework consists of five key functions that provides a comprehensive view of the lifecycle for cybersecurity management:

The NIST Information Technology Laboratory (ITL) developed one of the most extended models for incident response (IR): The Computer Security Incident Handling Guide (Special Publication 800-615). The NIST incident response process is a cyclical activity featuring ongoing learning and advancements to discover how to best protect the organization. It includes the following stages:



The core of everything is the Incident Response Plan (IRP) which is a set of documented procedures detailing the steps that should be taken

4 https://www.nist.gov/cyberframework/

5 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

in each phase of incident response, including roles and responsibilities, communication plans, and standardized response actions.

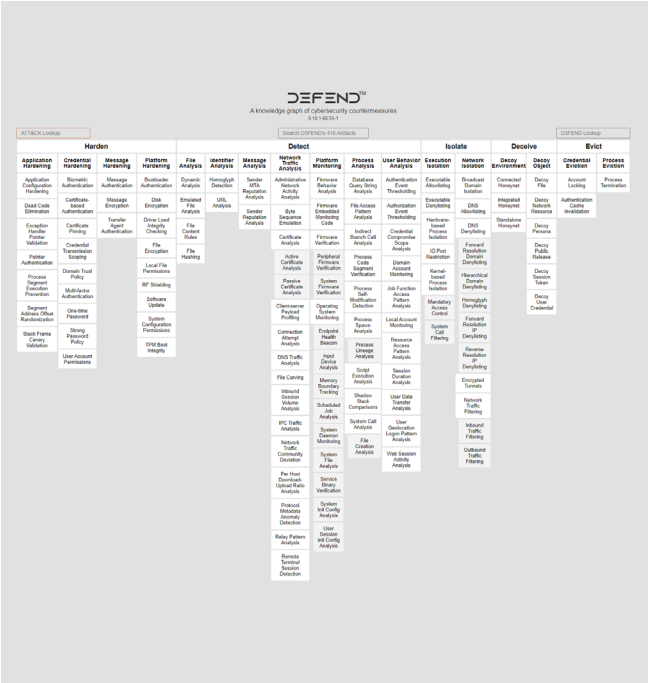
MITRE ATT&CK & D3FEND Matrixes

During the last years, incident response teams have been overwhelmed as they have not been able to properly manage the growing landscape of threats that were impacting organizations in a persistently and impactful way. In the past, it was common to define some standard operational procedures (SOPs) aligned with the common types of triggers that detection teams were potentially detecting and handling. This observations where handed over to the response teams(IR-Teams). This approach was however not sufficient, so the discipline shifted towards actively using threat intelligence for a better understanding of the threat landscape: Enumerating threat actors, their tactics, techniques and procedures (TTPs), and tracking their ongoing campaigns mapped to specific indicators of compromise (IoCs) used in every single cyberattack.

In order to properly structure all the adversary information, MITRE ATT&CK Framework[6] was born. The MITRE ATT&CK Framework is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. The knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

Most stakeholders in the industry follow this framework in order to align the generation of threat intelligence information (exchanged in well-known TIP platforms such as MISP or OpenIOC), detection signatures using standardized languages such as YARA, response capabilities such as the ones available in Security Orchestration Platforms (SOARs), and investigative OSINT/DFIR tools pivoting in digital online/offline evidence such as Maltego.

During the last year, a new complementary framework known as D3FEND[7] was born to support defenders in order to encode countermeasures in a knowledge graph. It contains types and relations that define both the key concepts in the cybersecurity countermeasure domain and the relations necessary to link those concepts to each other.



6 https://attack.mitre.org/matrices/enterprise/pre/

7 https://d3fend.mitre.org/

Accelerating Your Incident Response Workflows from Hours to Minutes with Maltego

With Maltego, analysts will not need to spend valuable time switching between multiple tools or writing a report detailing their findings for other teams and decision makers to act upon. Instead, they can carry out their analysis with all available data within one interface in Maltego and present their results directly on the graph, which will help them reduce time during the triage and analysis phase.

This handbook is meant to serve as an example of how Maltego could be utilized in standard incident response workflows to streamline investigative efforts. It is not meant to replace any established practices or tools, but to present a solution to challenges some investigators might face.

Setting up Maltego

3.

Set up your Maltego Desktop Client followings the simple five steps below.

Download Maltego

Download Maltego from our website for your Windows, Linux, or Mac machine.

↓

Activate Maltego

Open Maltego and activate your license by inputting your license key.

↓

Accept the License Agreement

Read and accept the license agreement.

↓

Install Transform Servers

Select the Transform servers you need for Desktop Client: The Public Transform Server and/or the Local Transform Server.

↓

Install Hub Items & Start Investigating!

Install the Maltego Standard Transforms and other third-party Hub items and start investigating!

Top Maltego Hub Items for Incident Response

4.

Here is a list of high-quality intelligence options for various IR investigative scenarios that have proven to be amongst our end-users' favorites and are suitable for all budget sizes. The list is sorted in alphabetical order and doesn't indicate any ranking or preference.

Main Hub Items for Daily Use

Click-and-Run

1 Abuse.ch URLhaus
Identify malicious URLs and explore underlying malware activity.

2 AbuseIPDB
Combat the spread of hackers, spammers, and abusive activity on the internet.

3 AlienVault OTX
Access threats, software targeted, and related indicators of compromise used for threat detection.

4 ATT&CK – MISP
Query MISP threat sharing instances and other MISP events, attributes, objects, tags, andgalaxies

5 Farsight DNSDB
Correlate and contextualize real-time and historical DNS data to expose networks and infrastructure.

6 Host.io
Enrich Domains with outbound links and backlinks, DNS information, location, and more.

7 Intezer Analyze
Automate end-to-end malware investigations with genetic malware analysis.

8 IPInfo
Enrich IP Addresses with domain and ASN information, precise locations, ISPs, VPNs, Tor users, and more.

9 OpenCTI
Query and explore threat intelligence data from OpenCTI instances using STIX2 Entities.

10 PeeringDB
Discover related infrastructure and connections into internet backbone systems around the world.

11 Shodan
Gain access to intelligence about the global IoT and infrastructure data.

12 VirusTotal
Leverage 15 years of malicious sightings to enrich your organization's malware observations and logs.

13 WhoisXML API
Leverage advanced IP and domain data to facilitate cybercrime detection, response, and prevention.

Commercial

1 Cisco Threat Grid
Map relationships between malware samples and indicators, campaign infrastructure, and more.

2 IBM QRadar
Extract and map context of IOCs from event logs and offenses.

3 Splunk
Cross-reference IP Addresses, domains, hashes, URLs, and other IOCs with internal intelligence.

Discover context and insights around CVEs, CPEs, and CWEs for vulnerability and threat exposure assessment.

Supplementary Hub Items

Click-and-Run

1 alphaMountain
Inform your investigations with reputation scores of the target's hosts, domains, and IP addresses.

2 Have I Been Pwned?
Check for password/domain breeches or to check if an alias or e-mail have been listed in a post to Pastebin.

3 Maltego News Transforms
Quickly query for news articles related to an Entity on the graph

4 Maltego Standard Transforms – IP QualityScore
Verify and fraud-check email addresses and phone numbers and identify suspicious IP addresses.

5 GreyNoise
Query IP address data and CVEs, Tags, or activities that an IP address has been observed scanning for.

6 NIST NVD

Commercial

1 DomainTools Iris
Map connected infrastructure, correlations, attribution, domains, and more to surface meaningful insights.

2 Recorded Future
Gain full picture of threat actors, including known exploit kits, vulnerabilities, or other TTPs.

3 ZETAlytics Massive Passive
Map and visualise relationships between different threat actors and known associates.

Looking for more data sources? Explore and find your solutions in our Transform Hub now.

The data sources you are using are not on this list? Reach out to your Account Manager at Maltego or support@maltego.com if you would like to learn more about using your current toolkit with Maltego for incident response.

Standard Workflows of Incident Response Using Maltego

5.

In this section, we will introduce the following 5 standard workflows of incident response and how investigators can carry out the operations using Maltego:

- Vulnerabilities or Threat Assessment
- Surface-Attack Review
- SIEM/XDR Event Triage
- Preliminary Investigation of Potential Breach
- IoC gathering: Operational Threat Intel Research

Let's dive right in.

Vulnerabilities or Threat Assessment

Context:

- Our Threat Intel team has some information about some potential threats impacting remarkable high and critical vulnerabilities that might be present in software or hardware used by our organization.
- The original intelligence comes from different stakeholders including an external intel provider, vendor alerts, CSIRT communities, and more.

Goal:

The incident response team needs to respond to a potential threat by evaluating whether the software used in the organization has been compromised

Starting Points:

- Product Security IRT (PSIRT) vulnerability alert website (Maltego URL Entities)
- List of the software names affected (Maltego Phrase Entities)
- Social Media, blog posts or notes (Maltego URL Entities)

Playbook:

1. Paste the PSIRT URL onto a Maltego graph
2. Select the URL Entity and pivot using Maltego Standard Transforms
   - To Regex Matches [Found on web page]
     - CVE-\d{4}-\d{4,7}
   - Obtaining different CVEs as results
3. Select the CVE Phrase Entities and pivot using NIST NVD
   - Search for CVEs [NIST NVD]
4. Select the returned CVE Entities and pivot using NIST NVD
   - To CPE [NIST NVD]
5. Select the CPE Entities and pivot using iternal CMDB Transforms or Splunk Transforms
   - To Hosts [Internal CMDB]
   - Obtaining IP addresses and/or hostnames
6. Select IP Addresses and pivot using custom Transforms for your on-premise vulnerability scanners
   - To Vulnerability Scan (Custom Internal Scanning Transforms)
7. Paste the software names as Phrase Entities onto your Maltego graph
8. Select the software names' Phrase Entities and pivot using Maltego News Transforms
   - To News Article [Maltego News]
   - Obtaining different URLs
9. Review URLs with higher weight/score and bookmark the Entities
10. Select all the URLs bookmarked and pivot using Maltego Standard Transform

- Extract links

11. Alert triage to identify applicable information
12. Review if software is being used in the organization
13. Understand if the threat applies to our organization

Data Integrations Used:

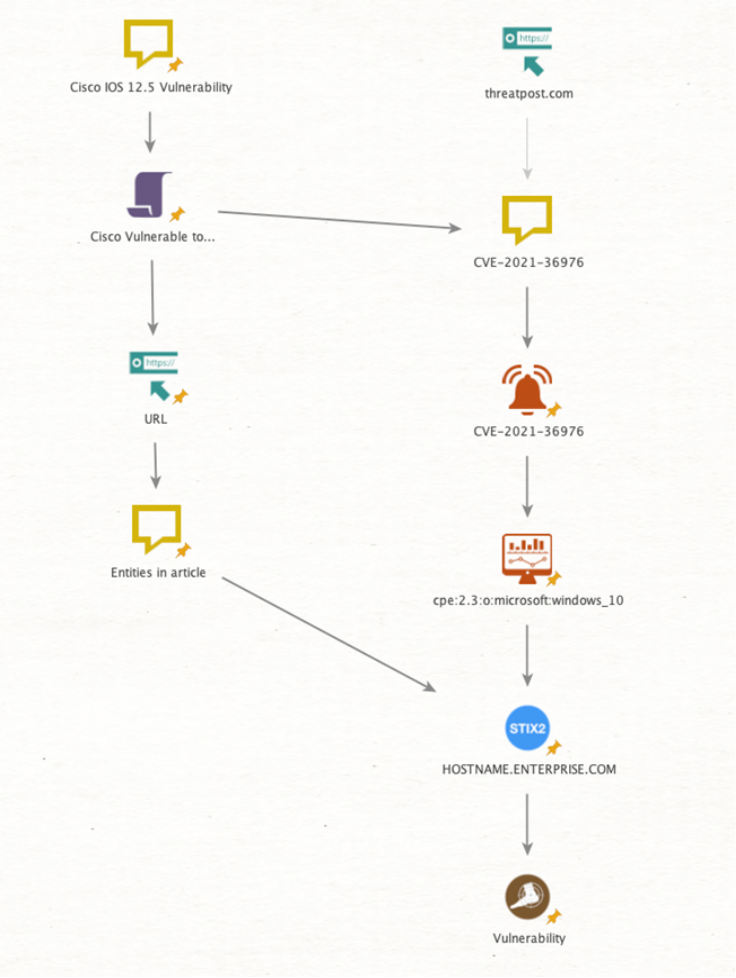
Maltego Hub Items

- Alienvault OTX
- Maltego News Transforms
- NIST National Vulnerability Database (NIST NVD)
- OpenCTI

Internal / Custom Integrations

- Internal CMDB or Splunk
- Vulnerability Assessment Tool such as Nessus or Maltego Teeth

Note: This is a mock-up diagram to illustrate the process using this incident as an example[8], starting from an blog post (URL Entity) or a phrase (Phrase Entity). To map to hostnames, you need an internal CMDB database (internal data source) or Splunk instances as well as a vulnerability assessment tool to scan the assets and find the vulnerabilities (such as Nessus or Maltego Teeth).



8 Microsoft Faces Wormable, Critical RCE Bug & 6 Zero-Days: https://threatpost.com/microsoft-wormable-critical-rce-bug-zero-day/177564/

Surface-Attack Review

Context:

Threat Actors are profiling organizations in order to find exposed assets. This includes individuals and corporate systems that might be exposed to social engineering and existing vulnerabilities.

Goal:

The incident response team needs to respond to a potential threat by evaluating whether the software used in the organization has been compromised

Starting Points:

- Name of the organization
- IP ranges/blocks
- Domains

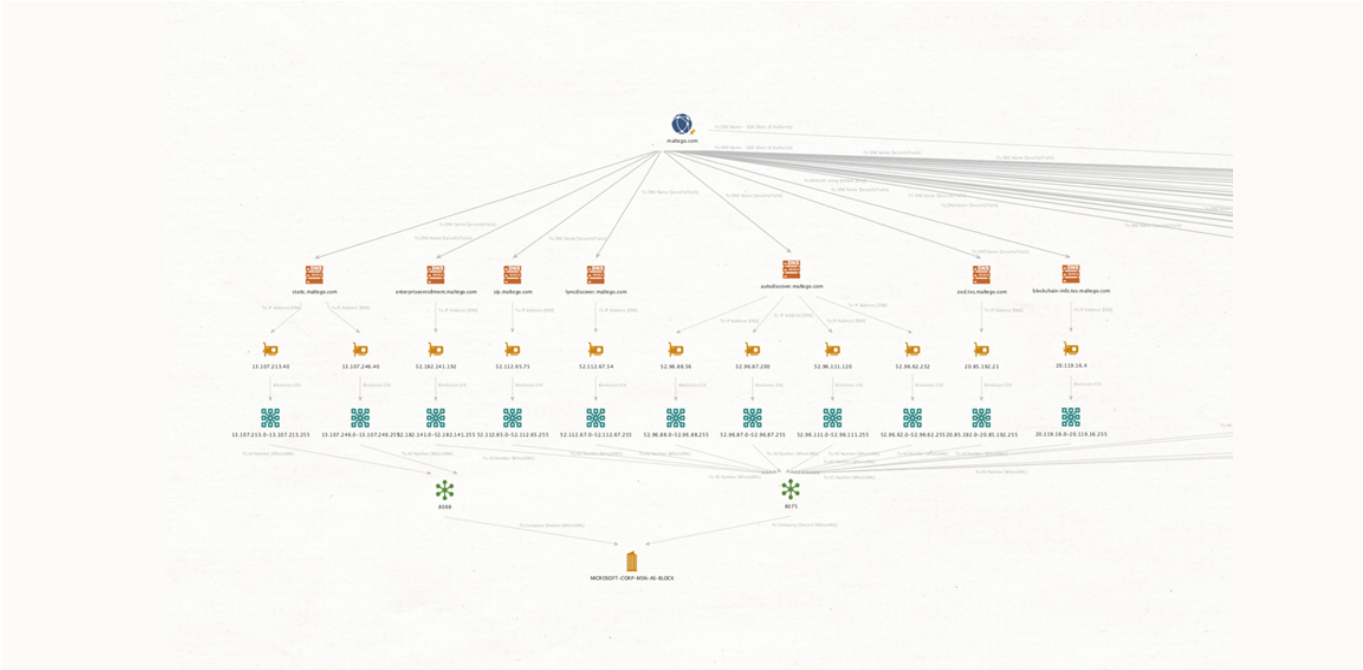
Playbook:

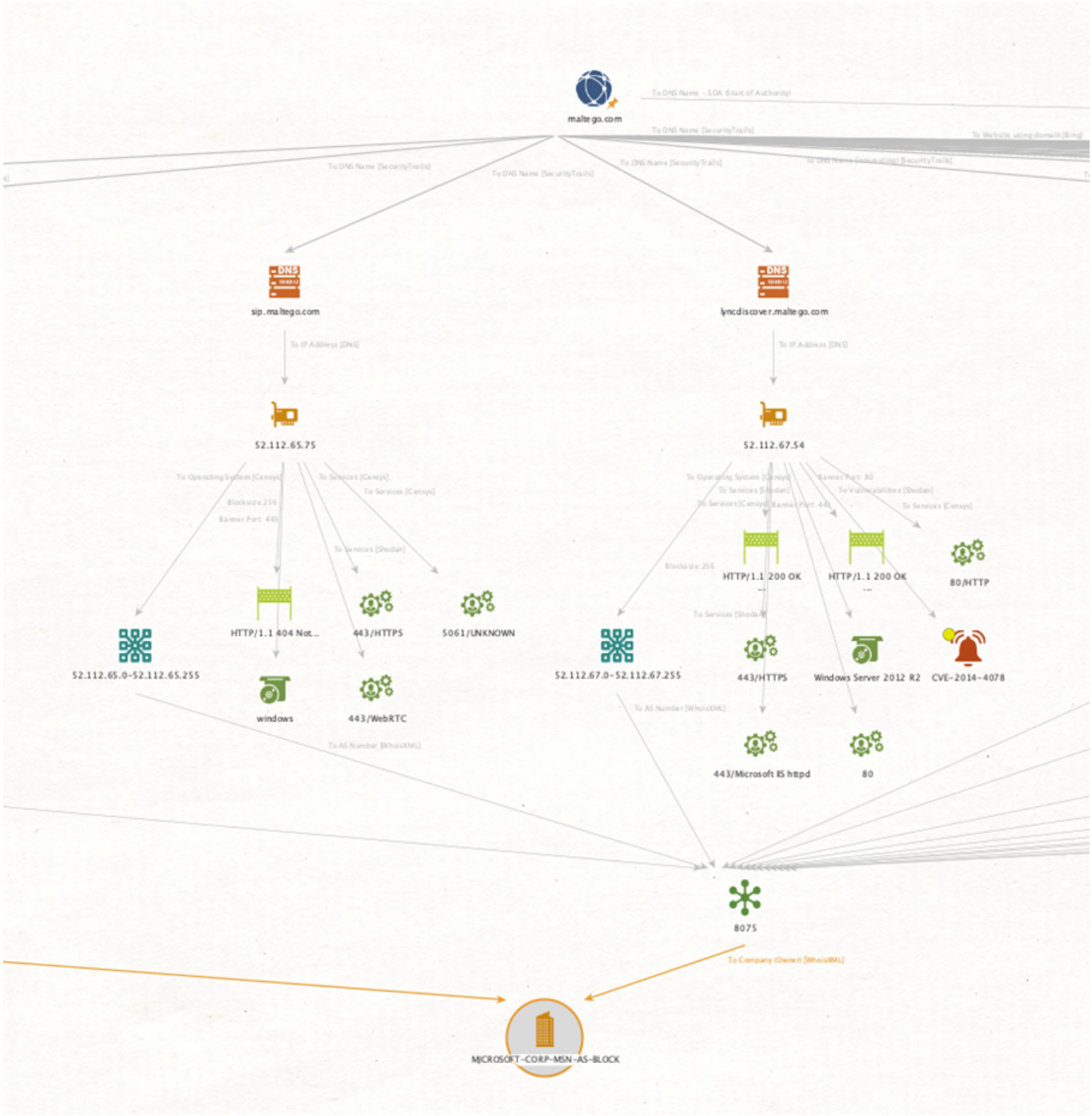
1. Paste the Domain Entity onto your Maltego graph
2. Lookup all DNS entries relevant to the domain
3. Lookup all IP addresses relevant to the found DNS entries
4. Group all IP's into natural netblocks
5. Group Netblocks to AS numbers
6. Identify AS numbers that are directly connected to the company, and then identify the relevant netblocks that the organization or company is responsible for
7. Select the IP addresses related to the identified netblocks and extract running services
8. From the same IP addresses, pivot to vulnerabilities using Shodan
9. Enrich the vulnerability details using NIST NVD Transforms.
10. (Optional) Select the netblocks and extract all the IP addresses found in the netblocks to search for more vulnerabilities and services.

Data Integrations Used:

Maltego Hub Items

- Censys
- Maltego Standard Transforms
- NIST NVD
- Shodan




maltego.com
sip.maltego.com
lyncdiscover.maltego.com
52.112.65.75
52.112.67.54
HTTP/1.1 404 Not...
443/HTTPS
5061/UNKNOWN
52.112.65.0-52.112.65.255
windows
443/WebRTC
HTTP/1.1 200 OK
HTTP/1.1 200 OK
80/HTTP
52.112.67.0-52.112.67.255
443/HTTPS
Windows Server 2012 R2
CVE-2014-4078
443/Microsoft IIS httpd
80
8075
MICROSOFT-CORP-MSN-AS-BLOCK

SIEM/XDR Event Triage

Context:

Security Operations Center (SOC) is handling cybersecurity events as a first line of defense and is escalating specific events to be triaged as potential incidents to their Incident Response Team (IRT), following their defined Standard Operational Procedures (SOP) and existing playbooks.

Goal:

Triage an event escalated by SOC that was triggered in the SIEM platform in order to verify if it is something worth to be further investigated or a false positive.

Starting Points:

- Case assigned in the Ticketing or Case Management tool (i.e. ServiceNow)
- SIEM alert linked to several security events received from one or several hosts (i.e. IBM QRadar and/or Splunk)

Playbook:

1. Pull and paste the case identification from your incident management platform onto your Maltego graph
2. Extract the URLs and indicators attached to the case
3. Read the description of the Alert Entities and/or open the URLs that provides you more context about the alarm (signature knowledge database article)
4. Extract relevant security events related with the main indicators attached to the case
5. Review them to identify anomalies considering IR expert knowledge and/or common anomalies

Data Integrations Used:

Maltego Hub Items

- Crowdstrike
- Splunk
- IBM QRadar

Internal / Custom Integrations

- Internal data lakes
- ServiceNow

This is a mock-up diagram illustrating the process, starting from a case in the investigator's Case Management Platform and/or SIEM (i.e. ServiceNow orIBM QRadar) and then extracting indicators such as the name of the alert, hostname, victim and IoCs (hashes). From the Hash Entity, we review all the security events logged in Splunk. From those events, we extract the IPs and other information with which the analyst can triage what happened.

Preliminary Investigation of Potential Breach

Context:

- There is an external notification coming from your national or regional CSIRT, Information Security Analysis Center (ISACs), or Cybersecurity Agency, including threat information that:
  - They know for sure has infiltrated your organization since your IP addresses, domain names, or other technical data has been found on criminal infrastructure
  - They have a high degree of confidence that the threat actors have targeted your organization and similar ones
- Your Threat Intel Team is:
  - Sharing a threat actor report provided by a private intelligence service provider, mentioning your organization or other similar victims in your industry.
  - Sharing information about systems or data from your organization being sold on Deep & Darkweb markets by criminally trusted operators such as initial access brokers (IABs)

Goal:

Verify of the potential data breach in your organization and establish the scope of the systems or platforms that might have been impacted.

Starting Points:

- Potentially compromised public IP addresses found in a C&C database/flows
- List of IoCs and artifacts used by an specific threat actor

Playbook:

1. Review notification and/or threat intel report
   - Understand the threat
   - Extract actionable intelligence
   - Obtain additional intelligence
     - i.e. Use Recorded Future, Silobreaker or other data providers
     - i.e. Search in MISP instance and/or TIPs like OpenCTI
2. Define the scope of investigation
   - Environments and/or systems
   - Platforms and/or data sources involved
3. Create a list of the IoCs/TTPs to search for
   - Yara rules
   - Regex and/or keywords
   - Specific filters and/or thresholds
4. Insert the IoCs from your ticketing platform into Maltego
5. Search for the IoCs in you Splunk and/or integrated data lake
6. Search for the IoCs in your XDR/EDR platforms such as Crowdstrike
7. If there are hits found, drill down/triage on them
   - Search in Splunk/SIEM for additional activity from the affected host
     - Hashes of suspicious files
     - Suspicious network connections
   - Pivot on found hashes, IPs, filenames
     - Using Virustotal, Intezer, and other relevant data sources

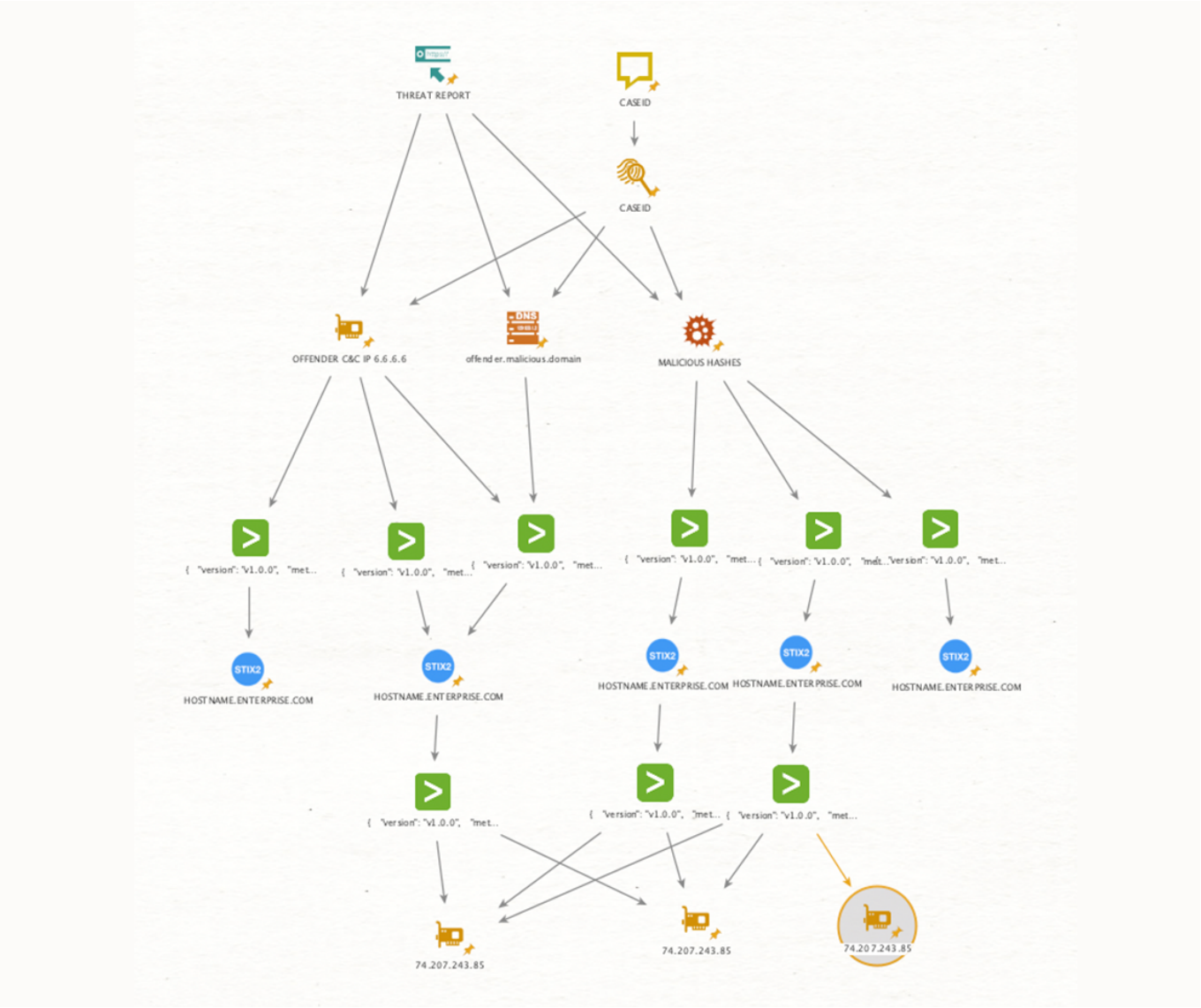
Data Integrations Used:

Maltego Hub Items

- ATT&CK – MISP
- Crowdstrike
- Intezer Analyze
- OpenCTI
- Recorded Future
- Silobreaker
- Splunk
- VirusTotal

Internal / Custom Integrations

- Internal data lakes



This is a mock-up diagram illustrating the process, starting from a reported information that could be from online (URL) or inside a case in Case Management Platform (i.e.ServiceNow). Indicators such as malicious C&C IPs or domains and crimeware hashes are then extracted. Those indicators are investigated in the SIEM/Event platform (i.e. Splunk), from which we pivot into the hosts to see the systems potentially impacted. From those hosts, we go deeper into other events close to the same time window to identify other IPs or common indicators.

IoC Gathering: Operational Threat Intel Research

Context:

There is an existing well-known threat notified by the threat intel team, but we do not have any specific or relevant information collected in our internal platforms such as initial access brokers (IABs)

Goal:

Obtain operational information including TTPs and IoCs known for an specific threat in order to make that information actionable for future investigations and operations.

Starting Points:

- Name or codename of the threat actor/ group
- URL of the notification and/or report in the threat intel platform

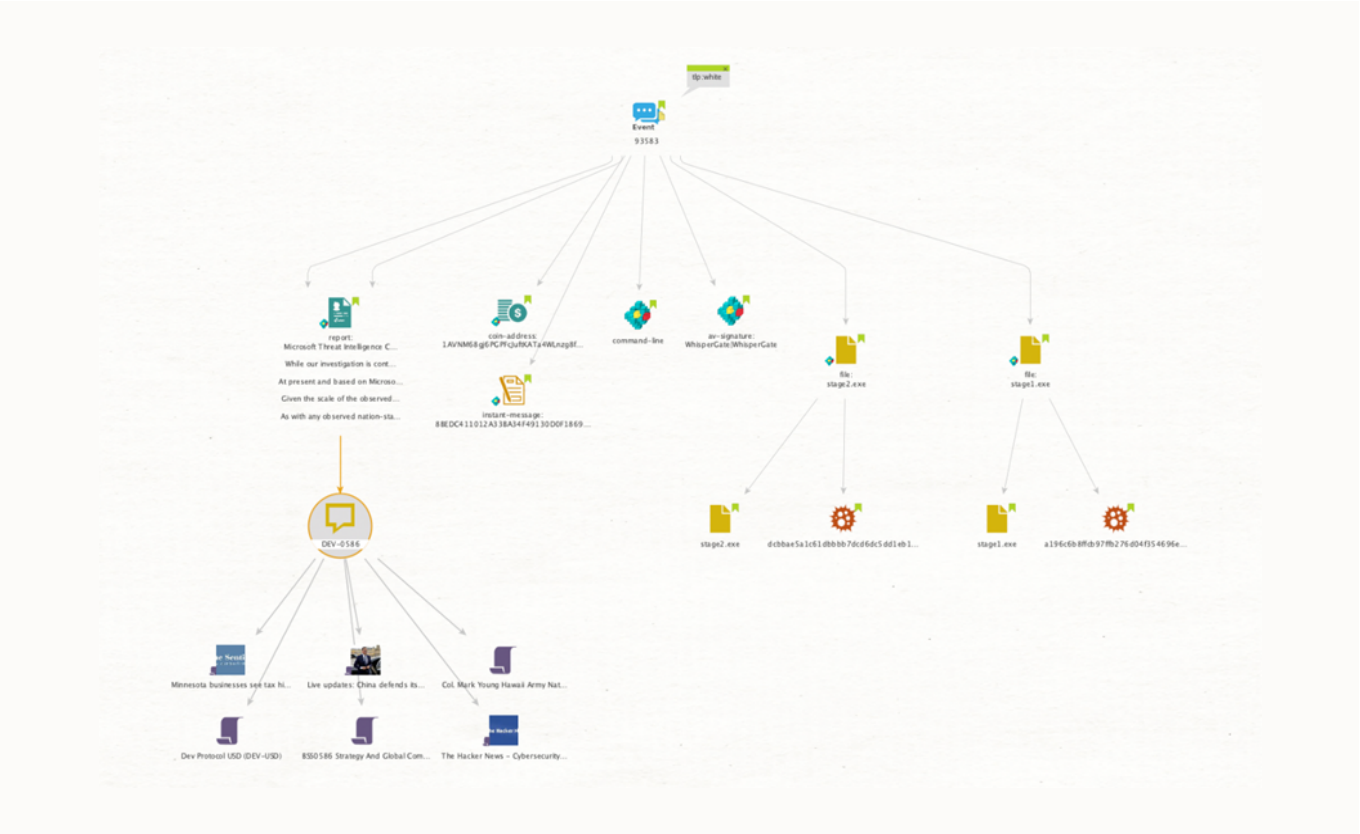
Playbook:

1. 1. Search for the threat actor codename in the threat intel platform, in this case, MISP
   - Search in MISP [MISP]
2. Pivot from intel reports to MISP Events
   - To MISP Events [MISP]
3. Obtain attributes of the MISP Events
   - To Attributes/Objects [MISP]
4. Further enrich findings using the retrieved attributes
   - To Related Objects [MISP]
5. Search for the threat actor codename in news reports within a selected time period
   - To News Article [Maltego News]
6. Browse and read the articles in the Entity Detail View or in a browser
7. Extract information form articles
   - To Entities [IBM Watson]
   - To Regex Matches [Found on web page]
     - Hashes
       - [0-9a-fA-F]{32}
     - IP addresses
     - CVEs

Data Integrations Used:

Maltego Hub Items

- • ATT&CK – MISP
- Maltego News Transforms
- Maltego Standard Transforms



This workflow can also be carried out using Maltego, OpenCTI, Silobreaker, and Recorded Future. Please see Example 1[9] and Example 2[10] for reference for this sample workflow image.

9 Destructive malware targeting Ukrainian organizations: https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/

10 Malware attacks targeting Ukraine government: https://blogs.microsoft.com/on-the-issues/2022/01/15/mstic-malware-cyberattacks-ukraine-government/

Example Use Cases

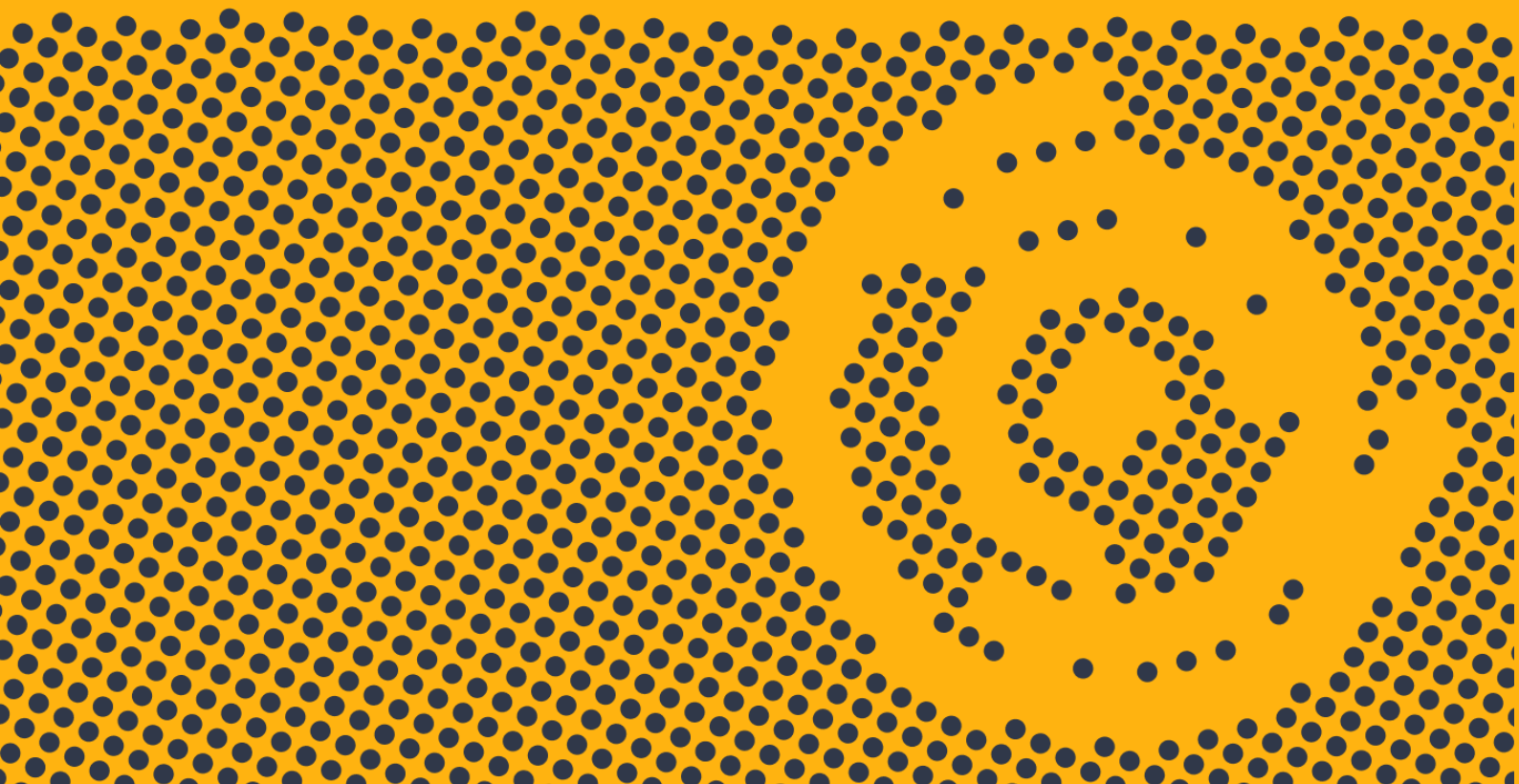
6.

Rapid Analysis for Incident Response with VirusTotal and Maltego - Maltego	https://www.maltego.com/blog/rapid-analysis-for-incident-response-with-virustotal-and-maltego/
SIEM-plifying Investigations with Splunk and Maltego!	https://www.maltego.com/blog/simplify-your-investigations-with-splunk-and-maltego/

For more information, please visit
maltego.com

Maltego is a comprehensive tool for graphical link analyses that offers real-time data mining and information gathering, as well as the representation of this information on a node-based graph, making patterns and multiple order connections between said information easily identifiable. With Maltego, you can easily mine data from dispersed sources, automatically merge matching information in one graph, and visually map it to explore your data landscape. Maltego offers the ability to easily connect data and functionalities from diverse sources using Transforms. Via the Transform Hub, you can connect data from over 30 data partners, a variety of public sources (OSINT) as well as your own data. Our different Desktop Client versions, data sources, and server solutions enable you to tailor Maltego to your specific needs in terms of data access, functionalities, and security requirements.

MINE • MERGE • MAP / DATA



Maltego Technologies GmbH
Address: Paul-Heyse-Strasse 29, 80336 Munich
Email: contact@maltego.com
Phone: +49-89-24418490

MALTEGO