SYGNIA CTI ENRICHMENT TECHNIQUES

SYGNIA

Search Engines

Points of Consideration

IP ENRICHMENT:

Check reputation and past related activities of the IP using these portals:

AbuseIPDB
OTX
GreyNoise
ThreatFox
Twitter IOC
Feodo Tracker

> General information about the IP - geo-location, IP range, hosting ISP etc.
> Has this IP been reported as malicious?
> What activities was it involved with?
> Does the IP relate to any specific campaign or threat group?
> When was the IP reported as related to malicious activity?

Use Spur, ExoneraTor and tornodes to check whether this IP serves as a VPN. Proxy or TOR node

> If it does - it means it is not indicative to monitor further activities
> It might also be an indication that the IP is used for malicious activity

Use Shodan / Censys to check for additional characteristics of the IP

> Unusual open ports (specifically ones recently added)
> Issued certificates, related computer names
> JARM/JA3 fingerprints
> Unique/suspicious additional behaviors

Use VirusTotal search for additional relations, reputation and IOCs enrichments

> Malicious files related to the IP - might be used by potential threat actor (pay attention to upload date and number of submissions)
> Check for unique URLs that relate to the IP
> Check for any comments or collections this IP is part of

Search the IP in Google and use the site filter to search the IP in Twitter.

> Does the IP appear in security blogs, security tweets etc.

Use RiskIQ to gather information about suspicious IP records and relations

> Domains that currently/previously resolved to IP - might also be related to the suspicious activity
> Does the IP serve as a hosting server of legitimate domains?
> When were the IP records registered/updated?
> Which ASN hosts this IP?
> Does the current WHOIS record seem legit (specifically if registration fields are not restricted and seem credible)?
> Any OSINT mentions of the IP?
> Certificates issued to the server (past and current) - pay attention to issuers and dates
> Unique trackers that might be useful as fingerprints

Further monitoring and pivoting

> Choose pivoting characteristics for further enrichment and expansion - resolved domains, related files, unique certificates, JARM trackers etc.

FILE ENRICHMENT:

Use VirusTotal search to gather and extract information about the file* based on its HASH

*In case the file isn't found on VirusTotal we recommend to upload it for scanning

> When was the file first uploaded and how many uploads/scans are recorded?
> AV detections (pay attention to signatures names as they might be indicative)
> Meta data - file names, signature, pdb path, size, creation time etc.
> Additional related files (parents, dropped files etc.)
> Related domains and IPs (embedded, downloaded from, communicating etc.)
> Explore similar files (based on IMPHASH, SSDEEP etc.)
> Check behavior tab for logged activities and verified detection rules
> Check content (if the file is textual)
> Check for any comments or collections this file is part of

Check reputation and past related activities of the file using Intezer, ThreatFox, OTX, MalwareBazaar, Twitter IOC hunter

> Has this file been reported as malicious?
> What activities was it involve with?
> Does the file relate to any specific campaign or threat group?

Search a sandbox report for the file's HASH using JoeSandbox; Triage; Any.Run; FileScan.

* Consider uploading the file to one or more of these engines in case it is not recognized

> Check for unique characteristics, artifacts, TTPs, IOCs and communication patterns
> Look for additional related/similar files

Search the file HASH (or any other relevant indicator) in Google and use site filter to search in Twitter (use all 3 hashing methods).

> Does the file appear in security blogs, security tweets etc.

Further monitoring and pivoting

> Choose pivoting characteristics for further enrichment and expansion - other related files, related IPs, related domains, unique detected signatures, unique meta-data/ strings, similarities engines etc.

DOMAIN ENRICHMENT:

Check reputation and past related activities of the domain using these portals:

OTX
GreyNoise
ThreatFox
Twitter IOC hunter
Feodo Tracker

> Has this domain been reported as malicious?
> What activities was it involved with?
> Does the domain relate to any specific campaign or threat group?
> When was the domain reported as related to malicious activity?

Use urlscan.io to explore the content of domain

> Check whether the content seems legit based on site's screenshot (current and historic)
> Check for any redirections or suspicious behavior

Use RiskIQ to gather information about suspicious domain's records and relations

> IPs that currently/past resolved to domain - might also be related to the suspicious activity
> Does current IP/IPs serve as a hosting server/s of legitimate domains?
> Additional domains that resolve to original domain's IP/IPs
> When was domain's records registered/updated?
> Does the current WHOIS record seem legit?
> Any OSINT mentions of the domain?
> Certificates issued to the domain (past and current) - pay attention to issuers and dates

Use VirusTotal search for additional relations, reputation and IOCs enrichments

> Malicious files related to the domain - might be used by potential threat actor (pay attention to upload date and number of submissions)
> Check for unique URLs that relate to the domain
> Check for any comments or collections this domain is part of

Search the domain in Google and use the site filter to search the domain in Twitter.

> Does the domain appear in security blogs, security tweets etc.

Further monitoring and pivoting

> Choose pivoting characteristics for further enrichment and expansion - resolved IPs, related files, unique certificates, JARM trackers etc.

EMAIL ADDRESS ENRICHMENT:

Check email reputation with Emailrep

Check mail server's reputation with MxToolbox

> Are the e-mail/mail server related to malicious activities?

Use IntelTechniques email search tool to gather information about the e-mail address

> Use variety of provided engines to explore the e-mail address - Google mentions, registered assets, related malicious activities etc.

Check if an email address was compromised using HaveIBeenPwned, Dehashed or Spycloud

> If so - it might be an indication for malicious usage of legitimate e-mail

Use RiskIQ to check whether the e-mail was used to register a domain or an IP ; check legitimacy of the mail server domain based on WHOIS records, resolved IP etc.

> Any domain or IP that were used for registration might be leads to further investigations and monitoring
> If the mail server domain seems suspicious it might be a good lead for further investigation

Retrieve accounts associated with an email address using Epieos.

> Any additional accounts might be good leads for further investigation and monitoring.

Use Google to look for additional information about the e-mail

> Does it appear to be legitimate and related to credible usage?

In case you got a suspicious e-mail sample - you can use Email Header Analyzer to make headers human readable

> Extract additional information that might lead to further investigation - IPs, domains, URLs, subject etc.

Use VirusTotal search to search for files containing this e-mail address (content:"<email>")

> Might lead to finding phishing mails sent from this account

Further monitoring and pivoting

> Choose pivoting characteristics for further IOCs enrichment and expansion
> Use abovementioned techniques to extract additional IOCs for internal monitoring