Offense investigation Tips

Offense investigation Tips

- How to detect IP reputation.
- How to detect malicious URL
- How to detect malicious Hash
- How to detect malicious Domain
- File reputation

- How to detect asset is compromised or not.
- How to block attacking network or IP.
- How to perform effective search.
- How to troubleshoot and find the cause before contacting to SIEM Engineer.

How to detect IP reputation

Risky IP list : e.g 5.2.69.13
https://www.maxmind.com/en/high-risk-ip-sample-list

Where to check IP reputation :

1) VIRUSTOTAL - https://www.virustotal.com/gui/home/search
2) Cisco Talos - https://talosintelligence.com/reputation_center/
3) IBM Xforce - https://exchange.xforce.ibmcloud.com/?_ga=2.204692368.1039500200.1616940022-1052170797.1568133000&cm_mc_uid=63299777242715595936893&cm_mc_sid_50200000=43366721615676180045
4) Webroot BrightCloud : https://www.brightcloud.com/tools/url-ip-lookup.php
5) IP Quality Score : https://www.ipqualityscore.com/ip-reputation-check
6) Mx ToolBox : https://mxtoolbox.com/blacklists.aspx

How to detect Hash reputation

Where to check Hash reputation : https://virusshare.com/hashes

Example 1: 185e4f14021ae686071081dda2a28fcf256b24e10f16d07c1fd7173b653df6d8

Example 2: bbe9fc719f21247d7c76ccab9953e3438abed35659dd6fd2a10f35e122129ea3

1) VIRUSTOTAL - https://www.virustotal.com/gui/home/search
2) IBM Xforce - https://exchange.xforce.ibmcloud.com/?_ga=2.204692368.1039500200.1616940022-1052170797.1568133000&cm_mc_uid=63299777242715595936893&cm_mc_sid_50200000=43366721615676180045

How to detect URL reputation

Risky URL list :
https://research.metaflows.com/stats/worst_urls/

Example :
www.coreftp.com/download/coreftplite64.exe

Where to check URL reputation :

1) VIRUSTOTAL - https://www.virustotal.com/gui/home/search
2) Cisco Talos - https://talosintelligence.com/reputation_center/
3) IBM Xforce - https://exchange.xforce.ibmcloud.com/?_ga=2.204692368.1039500200.1616940022-1052170797.1568133000&cm_mc_uid=63299777242715595936893&cm_mc_sid_50200000=43366721615676180045

How to detect Domain reputation

Where to check Domain reputation : e.g ipvolume.net / selectel.ru

1) VIRUSTOTAL - https://www.virustotal.com/gui/home/search
2) Cisco Talos - https://talosintelligence.com/reputation_center/
3) IBM Xforce - https://exchange.xforce.ibmcloud.com/?_ga=2.204692368.1039500200.1616940022-1052170797.1568133000&cm_mc_uid=63299777242715595936893&cm_mc_sid_50200000=43366721615676180045
4) Webroot BrightCloud : https://www.brightcloud.com/tools/url-ip-lookup.php
5) IP Quality Score : https://www.ipqualityscore.com/ip-reputation-check
6) Barracuda : https://www.barracudacentral.org/lookups/lookup-reputation
7) MX ToolBox : https://mxtoolbox.com/blacklists.aspx
8) Google postmaster : https://postmaster.google.com/u/0/managedomains?pli=1

File reputation

1) VIRUSTOTAL - https://www.virustotal.com/gui/home/search
2) Cisco Talos - https://talosintelligence.com/reputation_center/
3) IBM Xforce - https://exchange.xforce.ibmcloud.com/?_ga=2.204692368.1039500200.1616940022-1052170797.1568133000&cm_mc_uid=63299777242715595936893&cm_mc_sid_50200000=43366721615676180045

Some Tips

- How to detect asset is compromised or not.

→ Historical search, Vulnerability

- How to block attacking network or IP.

→ IP block / CIDR block

- How to perform effective search.

→ Start with small timeframe and grow slowly. Don’t search blindly otherwise it will kill core processes and it might break search functionality

- How to troubleshoot and find the cause before contacting to SIEM Engineer.

→ Historical search
→ Create saved search
→ Always search for anomalies

Thank you