LogicHub

Intelligent Security Automation Use Case

Automating Threat Intelligence Searches

Introduction:

LogicHub is the leading Intelligent Security Automation Platform that marries a powerful Decision Engine to a flexible Workflow Engine. Proven to deliver 10x the performance of traditional Security Orchestration Automation and Response (SOAR) solutions, it is the only platform of its kind to deliver analysis and decision-making automation to exponentially improve alert triage, incident response, and threat hunting.

One of the many use cases that LogicHub customers have implemented and benefited from is that of automating the search for Indicators of Compromise (IOCs), that are distributed from various 3rd party sources, within their environment.

Threat Intel Challenges:

- Constant flow of IOCs
- IOCs can lack detail
- Senior leadership wants to know if IOC is in the environment
- Limited cycles in the Security Operation Centers (SOC)
- Tedious and time consuming to search

LogicHub Solution:

Automate the searching and enrichment of the data with LogicHub. This can be accomplished by collecting the IOCs described in the 3rd party threat intel and allowing LogicHub to process through them searching against both internal logs and intel tools to enrich the data.

Collect the Data and Combine

SOCs receive large amounts of data from various 3rd party intelligence feeds, some of which are paid services. Leadership wants to see a return on investment from these paid premium services. This leads to an expectation of the SOC to make the most of this data.

This information can be collected and combined into a single file with just a list of the IOCs that the SOC would like to have more information about. This file can then be put on a network share that is monitored by a flow within LogicHub. Once there it will be downloaded and processed by LogicHub. The results will be uploaded after the job has been completed.

Figure 1: Sample IOC file

	A	B
1	type	ioc
2	hash	c6d1fac3295a6cad4ea86b39b63bc26a
3	hash	af42ad289661e2915621802176172839
4	ip	192.168.0.0
5	ip	10.11.12.13
6	email	badmailer@legitnotbadsite.org
7	email	spammerdude@trustednewzsite.biz
8	cve	CVE-2015-9999
9	cve	CVE-2012-8888
10	url	notphishingattack.com
11	url	notabadplace.net

IOC Environment Search

LogicHub will take the IOCs and divide them into separate tables to be searched against pre-defined sources. These results are valuable to the SOC as they can quickly identify possibly compromised machines within the network. The searches are catered to the specific environment in both tools searched and the output fields/format.

- **File Hash**
  - Endpoint Detection and Response (EDR) tools have access to large amounts of useful data when searching for potentially compromised machines. Useful searches for file hash include; running processes, source process for network connections, and files on disk.
- **IP Address**
  - Security Information and Event Management (SIEM) products generally have logs from several different data sources and are a useful way to search logs for different tools simultaneously. IP addresses could be searched against firewall logs, proxy logs, netflow, etc.
  - Web Proxy logs will have connections from internal machines to the internet. Searches against these logs could find outbound connections to malicious IP addresses.
  - Email solutions will have metadata for inbound and outbound emails within your environment. Searching both the email body and sender's email could help identify users in the environment who may have received malicious emails.

- **URL**
    - URLs are generally searched in a similar fashion to IP addresses in regard to IOCs. Suggested searches would be web proxy logs and email message bodies.
- **Email Address**
    - Similar to IP address, searching email metadata relevant to the sending email address would quickly identify emails and users to be investigated further.
- **CVE**
    - Vulnerability Scanning products generate reports that can be used to search for vulnerable hosts within the environment. If a specific CVE is being actively exploited by a particular group or hacking campaign, this may influence the patching schedule within your environment.

IOC Enrichment

The intel received from 3rd party sources comes in many different forms with varying degrees of supporting data. In addition to searching your environment for IOCs, LogicHub can also enrich the IOCs with information that will aid the SOC in determining any mitigating actions that may need to be taken. The SOC can make use of the intel even if no signs of compromise are found during the environment search.

- **File Hash**
    - Search in online tools for antivirus coverage and return a ratio of detected versus undetected by various vendors.
    - Check coverage against your own antivirus solution.
    - Online blacklists may also have other characteristics such as family or malware class.
    - Blacklists within your own environment.
- **URL/IP Address**
    - Categorization lookup against the product used within your environment for proxy blocking.
    - Searches against online blacklists, depending on which are used different data could be provided such as purpose, phishing or command and control.

This enrichment not only gives the SOC information about mitigating factors currently in place within your environment, but it also gives them more detail for IOCs with no mitigations in place and can help them make a decision whether there needs to be or not.

Figure 2: Sample Enrichment Output

	A	B	C	D	E	F
1	type	ioc	av_score	av_family	blacklist	proxy_category
2	hash	c6d1fac3295a6cad4ea86b39b63bc26a	28/56	dropper	N/A	N/A
3	hash	af42ad289661e29156218021761728839	3/56	trojan	N/A	N/A
4	ip	192.168.0.0	N/A	N/A	0/42	none
5	ip	10.11.12.13	N/A	N/A	20/42	Malicious
6	url	notphishingattack.com	N/A	N/A	17/42	Phishing
7	url	notabadplace.net	N/A	N/A	3/42	none

Conclusion

Automating the search and enrichment of threat intel helps the SOC identify potentially compromised machines and identify gaps in your environment's security. This particular use case does not make any changes to the environment that could cause potential outages or block legitimate business processes, but instead provides insight to help with those changes.

For more security automation use cases, visit www.logichub.com.