White Paper

White Paper

Real Cyber Threat Intelligence Tells a SOC What Its Security Stack Cannot Detect

"Threat Intelligence Feeds" Are Information, Not Intelligence.

Actionable cyber threat intelligence should inform a security operations center's prioritization of the most critical applications and infrastructure to the business and threat hunt program in ways a security stack cannot. With hypotheses-led, defined use cases that focus on signatures and more importantly behavior, threat hunting programs can operationalize threat intelligence by mapping threats to data sources and decision matrices that provide alerts and subsequent action. As a deliverable, a SOC can then count the actionable alerts versus the total alerts and, if captured appropriately, a security program can scale by reducing time to respond with fewer resources.

"Threat Intelligence Feeds" are information - not intelligence - unless they are timely, relevant, and actionable. Rarely are such feeds useful for context without tremendous analyst and data engineering resources that map the threats to the risk of the business and establish the appropriate metrics to enable security engineering resources to prioritize remediation and reduce the risk.

We've previously discussed building a threat hunt team around categorizing the threat around a coverage map, cyber analytics repository, measuring what matters through effective reporting, and valuing the risk for remediation. After this foundation of a threat hunting program is established, a SOC should implement actionable threat intelligence through a series of hypotheses to inform what a security stack cannot detect. Only then for example, can an organization use the various data sources to build robust alerts and defend against attacks that target other organizations within the same industry.

Deriving Use Cases from Threat Information to Create Actionable Intelligence

After understanding the visibility gaps and determining the appropriate coverage map, it's important for a SOC to determine what use cases are important to them. With these use cases in mind, the SOC can properly prioritize data sources external to their network to make best use of tools that are usually expensive and labor intensive to integrate into a SIEM. Common examples include:

- Credential Leaks
- Company Data in Non-Public Sources
- Malware Not Detected by Current Security Controls
- Threat Actor Activity
- Third Party Compromise

Based on the use cases and coverage maps, organizations should procure data sources in the least costly manner possible based on the specific threats they face from nation states, criminal groups, hacktivists, etc. Some typical datasets include:

- Global netflow data.
- Upload hashes and IOCs against common AV products.
- Geolocation data, corporation associated IPs, ad-tech data graph databases.
- Threat intelligence content including indicator of compromise (IOC) artifacts—external threats, attackers, and their related infrastructure.
- Datasets containing internet facing devices (webcams, routers, servers, etc.).
- Credential pairs collected from public releases of breached datasets.
- Deep and dark web content.
- Passive DNS: a system of record that stores DNS resolution data for a given location, record, and time period.

Use Cases can be Mapped to Data Sets and Goals

Use Case	Data Set	Goal
Credential Dumps	Credential pairs collected from public releases of breached datasets	Roll credentials on accounts that have been leaked online.
Company Data in Non-Public Sources	Deep and dark web content	Alert stakeholders to any sensitive company data that has been seen for sale on the deep and dark web forums.
Malware Not Detected by Current Security Controls	Upload hashes and IOCs against common AV products Threat intelligence content including indicator of compromise (IOC) artifacts—external threats, attackers, and their related infrastructure	Supplement current security controls with IOCs that are alerted on by vendors not in the current security stack.
Threat Actor Activity	Threat intelligence content including indicator of compromise (IOC) artifacts—external threats, attackers, behavior, and their related infrastructure	Identify previously unknown IOCs, behaviors, and TTPs that can be used to update security controls and create new threat hunting hypotheses.
Third Party Compromise	Global netflow data Geolocation data, corporation associated IP's, ad-tech data graph databases Monitor and query datasets containing internet facing devices (webcams, routers, servers, etc.)	Assess a third party's general network hygiene and alert to any indication of compromise.

Operationalizing Intelligence

After data sources are aggregated, it's important for a SOC to provide the appropriate decision matrix when an alert goes off. Examples below:

Use Case: Credential Dumps

Alert	Action
Credential leak discovered.	Notify users. Roll creds regardless if the creds discovered belong to a company account. This will eliminate the risk posed by password reuse.

Use Case: Company Data in Non-Public Sources

Alert	Action
Access to network found for sale	Engage Threat Hunt team to search for any indication of compromise. Engage IR to begin rolling credentials.

Use Case: Malware Not Detected by Current Security Controls

Alert	Action
Malware discovered that it is not alerted by current security controls.	Gather malware IOCs and deploy alerting to security controls.

Use Case: Threat Actor Activity

Alert	Action
Threat actor behavior identified. A host is connecting to an odd server every 10 minutes for the past 10 days. This user logged on to the domain controller when he has never done that before.	Threat hunt team spends a lot of time baselining what's normal in a network and investigating what's unusual. If an anomaly turns out not to be malicious, throw that on the knowledge base of normalcy. If an anomaly turns out to be bad, it becomes an incident for the IR team.

Use Case: Third Party Compromise

Alert	Action
Third party is the victim of a compromise.	Engage in information sharing with the third party, ask for IOCs. Engage Threat Hunting to monitor any network accesses the third party may have inside the network. Engage with IR to begin rolling creds of accounts associated with the third party.

Deliverables and Output for Remediation by the Business

A SOC can count the actionable alerts versus the total alerts and if captured appropriately, a security program can scale by reducing time to respond with fewer resources. Ideally, more actionable intelligence alerts would ideally result in a decrease of alerts related to actual compromise. If tuned, automated, configured, and operationalized properly, the threat hunt team would have clear objectives and metrics that demonstrate the appropriate threat intelligence was either handled and remediated by the threat hunt team or the incident response team, depending on the severity of the access gained by the intruder. In addition, these metrics should flow through to the security engineering team for appropriate remediation.

For additional information, visit www.nisos.com or contact info@nisos.com.