graylog

Reading the Tea Leaves: Expanding Security Log Enrichment Beyond Threat Intelligence

Effective security is a moving target—that's not news. So how can an organization stay ahead of the game? By giving itself the ability to see farther.

The power of centralized log data is the ability to see more by giving your security data more context. And as most analysts know, context can mean the difference between an automated, proactive threat defense and fallout from an actual attack.

The problem is that the ability to see data doesn't guarantee the ability to interpret what it means. Context can only be considered successful if it provides enough information that analysts can respond appropriately to a situation. The question then becomes: how do we get accurate and actionable security data out of centralized log management?

One way is to enrich security logs with third-party intelligence, which is beneficial for the following reasons.

1) It adds valuable context, making it easier for an analyst to make a good decision on the fly.
2) It answers more sophisticated security questions, broadening an analyst's reach.
3) It enables security automation, saving time, money, and resources.
4) It ultimately increases efficiency and improves security outcomes.

While log enrichment is a powerful way to improve your ability to respond quickly and accurately to security threats, the reality is that many viable enrichment sources are often overlooked. Let's take a look at some standard and advanced third-party intelligence.

TYPES OF ENRICHMENT

Most people default to threat intelligence when enriching security log data. But there's actually a wide variety of third-party information that can augment log data to make it useful, depending on an analyst's objectives. They tend to fall into two categories: ***standard sources*** and ***advanced options***.

STANDARD SOURCES

Standard sources are third-party data sources typically used to help address common security issues or investigations.

Threat Intelligence

The go-to enrichment source for security logs, threat intelligence helps match up suspect activity with known threat indicators so analysts can determine if a threat is benign or malicious. This source can be useful in typical security scenarios such as cross-referencing an IP address or domain with a list of known threats.

Hash Values

A shorthand value (or “fingerprint”) used to indicate a much larger chunk of data, hash values known to be malicious or associated with malware can be used to identify and root out suspicious files. They can, for instance, help automate blacklisting of known malware files or whitelisting of benign files.

IP Geolocation

GeoIP allows analysts to identify the geographical location of an IP address. This identification helps them differentiate between legitimate and malicious activity by assigning the IP address geographical context down to country, city, or even latitude/longitude. So, if several IP addresses involved in suspect activity share the same location, an analyst can determine if the activity is a malicious attack or legitimate traffic.

WHOIS Data

Enriching security logs with WHOIS data allows analysts to identify the person or organization a domain or IP address is registered to. This enrichment source can be useful if an organization is being attacked by a specific domain and needs to contact the owner of the domain, for example.

LDAP/Active Directory

Using LDAP or AD data can help differentiate a legitimate internal user or account from a suspicious one. This type of enrichment can help an analyst in multiple ways, from providing contextual contact information when reporting an incident to determining the risk level of the user (e.g., administrative responsibilities, access to high risk data, or access to high risk compliance zones).

DNS Lookup and Reverse DNS Lookup

The ability to map an IP address to a domain (or vice versa) gives additional context to a domain or IP address trying to access a system/network. If an analyst notices a system is demonstrating suspicious DNS activity, he or she can use DNS or reverse DNS lookup for additional context to help identify whether the system has actually been compromised.

Departmental Information

Lists of personnel in the organization by title, department, supervisor, group membership, etc., can help analysts map activity back to real people and teams. This type of enrichment can help report and curb policy violations, such as an employee using a personal account instead of a service account, and support security automation, such as automatically notifying a particular group if there are a large number of lockouts for an account associated with that group.

ADVANCED OPTIONS

Advanced enrichment options are more esoteric intelligence sources that are useful for specific security scenarios. They fall into three categories: compliance, tracking, and risk calculation.

Compliance

Compliance data can be used to flag people and/or assets based on differentiated levels of access.

PCI

PCI DSS (Payment Card Industry Data Security Standard) is a set of security regulations that companies must follow if they process, store, or transmit credit card information. Enriching security logs with PCI data allows you to add zone data (such as "trusted" and "untrusted" zones) to clarify relationships between people and/or assets, identifying whether untrusted entities are trying to access trusted objects. For example, this type of enrichment could help prohibit an untrusted device from attempting to access a trusted device without authentication.

HIPAA

HIPAA (Health Insurance Portability and Accountability Act) regulates data privacy and security for medical information. Like PCI data, HIPAA enrichment provides zone detail to help analysts identify the relationships between objects and/or people. This enrichment source could help prohibit non-HIPAA secured environments from touching secured environments except through approved authenticating proxy or applications.

Sarbanes-Oxley

This set of regulations helps safeguard against fraudulent accounting practices, accounting errors, and inaccurate corporate financial disclosures to protect investors and shareholders. Enriching security logs with this data makes it possible to track access to relevant data or to devices that carry relevant data. During audit compliance, for instance, access and audit logs can be tracked to relevant devices or accounts and provided in a scheduled report to the auditor to prove compliance instead of relying on users to track the logs.

GDPR

GDPR (General Data Protection Regulation) is a set of EU regulations regarding the processing of personal data to increase protection and privacy. Adding GDPR data as context to security logs helps analysts differentiate the types of data specific users can see and what format they'll see based on their access. This enrichment source can be used to tag data with its GDPR access level and filter user views based on their access level to ensure no one is viewing off-limits information.

Tracking

Tracking is the ability to see when people (and devices attached to them) are physically on the move.

User to DHCP Mapping

You can use this data to answer two security questions: (1) are people/devices where they should be, and/or (2) are they in two places at once? This enrichment source can be used to manage physical security concerns, such as developing heat maps of physical spaces (such as conference and common rooms) to understand usage, or to identify physical security vulnerabilities, such as a tendency of employees to congregate near a certain door, increasing the risk of tailgating.

Mac to User Mapping via NAC

This data is useful to help diagnose device-related issues. For instance, let’s say a user gets locked out of his account. The analyst can identify the root cause as a saved password on their iPhone based on the fact that a Mac address recently failed several authentication attempts.

Workstation History to User Mapping

Mapping workstation history to user mapping ties user behavior to device/network impact. This data gives analysts the ability to make judgment decisions on how to apply and/or automate security rules. One example is the ability to identify users who may be at greater risk of being targeted by (and uniquely vulnerable to) phishing attacks, then creating more stringent phishing rules and alerting for those users or groups.

Antivirus History to Workstation Mapping

Historical antivirus usage for a particular workstation helps identify workstations where antivirus software has been at work. Among other uses, this data can help pinpoint and investigate objects that keep getting reinfected with a virus, requiring intervention by an antivirus solution.

Risk Calculation

Risk calculation helps identify users and groups particularly vulnerable to attacks.

User’s Signing Authority

User’s signing authority is data that categorizes users’ access to company resources or their ability to make decisions in the organization. The benefit of this type of enrichment is to help defend against phishing or other security threats on behalf of vulnerable and/or targeted personnel that the company is too large to be able to directly identify. So, large organizations that may be unaware of which employees are most likely to be targeted by attacks can elevate security alerts for people based on their signing authority.

Group Membership

Group membership is data that categorizes internal teams and groups to fend off phishing or other threats on behalf of personnel the company *knows* is more vulnerable and/or targeted. For instance, an oil and gas company could identify their legal group as the biggest target for information theft attempts due to their ability to negotiate leases. Consequently, security can be elevated for that group.

CONCLUSION

When it comes to security data enrichment, it's helpful to think beyond threat intelligence. Tapping other enrichment sources makes it possible to add layers of valuable context, answer more sophisticated security questions, enable more effective automation, and ultimately, increase efficiency to improve security outcomes.

Whether you start with a question you want to answer, a problem you want to troubleshoot, or blind spot you want to identify, embracing a broader definition of third-party enrichment changes the trajectory of your security initiatives.