splunk>

12-04-2022

Using the Splunk Enterprise Security assets and identities framework

Your organization currently uses a cybersecurity platform within the SIEM space that does not allow you to provide contextual information surrounding alerts. You have decided to switch to Splunk Enterprise Security so that you can take advantage of the capabilities of the Assets and Identities Manager, so your analysts and incident responders get the information they need to work more effectively. You want to learn best practices for using this system.

Solution

Splunk Enterprise Security uses an asset and identity management system to correlate asset and identity information with events to provide context and enrich data. This framework takes data from external authoritative platforms to populate lookups, which Splunk Enterprise Security correlates with across your datasets at search time.

The asset and identities framework specifically addresses issues larger-scale customers face:

- CIM Zones for overlapping address or identity space
- Moving to KVStore versus lookups
- Reset functionality
- Search head cluster support

How might you ingest assets and identity data within Splunk Enterprise Security? Here are the most common methods:

Assets		
Source	**Pro**	**Con**
CMDB	Your use case can add a much-needed boost towards the overall CMDB effort	Often not complete and slow to correct
Active Directory (LDAP)	Doesn't require universal forwarder to be installed on Domain Controller	If an asset isn't on the domain, it won't be on this source
Active Directory (ADMON)	Only sends when a record has changed versus complete set in LDAP	If an asset isn't on the domain, it won't be on this source
Vulnerability Scanner	Configured and controlled by cybersecurity team and can be easily adjusted to 'locate' missing assets	Lacks contextual information to help identify business units or function of asset

Assets		
Source	**Pro**	**Con**
Active Directory (LDAP)	High fidelity data source - like assets, doesn't require universal forwarder to be installed on Domain Controller	Doesn't contain local user accounts
Active Directory (ADMON)	High fidelity data source - like assets, only sends when a record has changed versus complete set in LDAP	Doesn't contain local user accounts
HR Management System	Great source for categorization and prioritization	Lacks some contextual information to stand alone
Mainframe	Contains identities of truly critical accounts	Difficult to obtain the dataset

The table above is not exhaustive. It provides information on only the most common methods found in the field.

After selecting the data source to serve as the authoritative dataset, many organizations identify a second data set to act as an enrichment opportunity to further enhance their assets and/or identities. Locate the common field between the two data sets.

- For assets, it might be the hostname.
- For identities, it might be the email address.

Then, merge them within the Splunk Enterprise Security Asset and Identity Manager.

The goal of assets and identities should be to only fill out what's important to the SOC analyst and to aid in specific use cases. Remember, the more data you put into the table, the larger the search bundle containing the information will be. Larger bundles can have search performance impacts. To limit the scope and maintain performance, the most common attributes to fill out per entity are:

- **Assets**. IP, Hostname, FQDN, Priority, Category, Owner, Business Unit
- **Identities**. Identity, First, Last, Email, Priority, Category, Business Unit, Manager, Phone

Most of these attributes are self-explanatory, but let's focus on two of the most important:

- **Priority**. Priority is all about the impact. Remember that you refer to the system of record to aid in that assignment. You might reference the fact the user is in the Domain Administrator organizational unit or that the system is part of the platinum application group. Some other questions to think about are:
  - What is the impact to your organization and bottom line if that account or endpoint is compromised?
  - How much per day would your company lose?
  - What access does this entity have to corporate IP, customer information, or other protected data?

    - What loss of availability to your end customer would only create small issues and what would create larger problems that could damage your reputation?
- **Category**. Categories are logical classifications, piped delimited, that you can use to group together assets or identities for mass inclusion or exclusion in a particular use case. For example, you may want to group together all administrative accounts or Windows servers to quickly identify exposure of recently published vulnerability.

Next steps

After assets and identities are sourced, populated, and implemented, you are ready to use them. Right within search, you can now answer many questions you always wanted insight into. For example:

- Need to see the username associated with the Windows event that only contains the SID?
- Can't remember what service accounts that don't follow the standard naming convention?
- Always wondered what the source IP hostname was in a Cisco ASA event?
- How about network segment names within DNS query logs?

Need more help? We recommend the following:

- BlueVoyant: BlueVoyant combines internal and external cyber defense capabilities into an outcomes-based platform called BlueVoyant Elements™. BlueVoyant's approach to cyber defense revolves around three key pillars—technology, telemetry, and talent—that delivery industry-leading cybersecurity to more than 700 customers across the globe. Contact BlueVoyant Expeditionary Services for help evaluating your Splunk Enterprise Security maturity today.
- Product Tip: Identifying high-value assets and data sources
- Splunk Docs: Add asset and identity data to Splunk Enterprise Security