AXONIUS

CONTROL COMPLEXITY WITH AXONIUS AND SPLUNK

TODAY'S CHALLENGE

Organizations today are struggling to keep their finger on the pulse of their ever growing cyber attack surface. Combine this with the economic pressures facing every business and expanding perimeters into the cloud, security and IT leaders are struggling to allocate their teams' time and resources to adequately address the multitude of alerts and incidents cluttering their inboxes daily.

Traditional security tools help keep threats at bay — but often are acting in silos, speaking different languages, and are unable to provide a holistic view of an organization's risk. This presents an onslaught of challenges when trying to secure the attack surface. A short-list of these challenges includes prioritizing incidents, adhering to security policies, and identifying current threat actors and security coverage gaps.

THE SOLUTION

To address the above challenges, an organization must have a clear view of their network environments. Axonius connects via simple API connections to the tools organizations already use, collecting source data about assets and asset-related information. Axonius correlates that data to gain a comprehensive analysis of the environment, and presents a unified view of the entire attack surface. Devices, users, SaaS applications, and cloud workloads are uniformly presented with deeper context, and, when combined with the power of Splunk, gives organizations a clear and actionable picture of every asset within their network. Customers can leverage Axonius's correlation of asset-related data across their existing security tools within their Splunk consoles or within the Axonius platform, enriching the existing data known to Splunk with greater context in addition to discovering assets that were previously unaccounted for such as OT, IoT and ephemeral devices.

KEY BENEFITS

COMPREHENSIVE ASSET INVENTORY

Axonius correlates and aggregates data from Splunk with other connected 3rd party security controls to provide customers with a comprehensive asset inventory and related security posture of all devices and users at a granular level.

ACCELERATE INCIDENT RESPONSE

Axonius provides rich, correlated data on devices, users, and cloud instances that when combined with Splunk's real-time event-based findings reduces alert triage time. Thus freeing up valuable time and resources to improve alert prioritization and criticality.

REDUCED TIME TO REMEDIATION

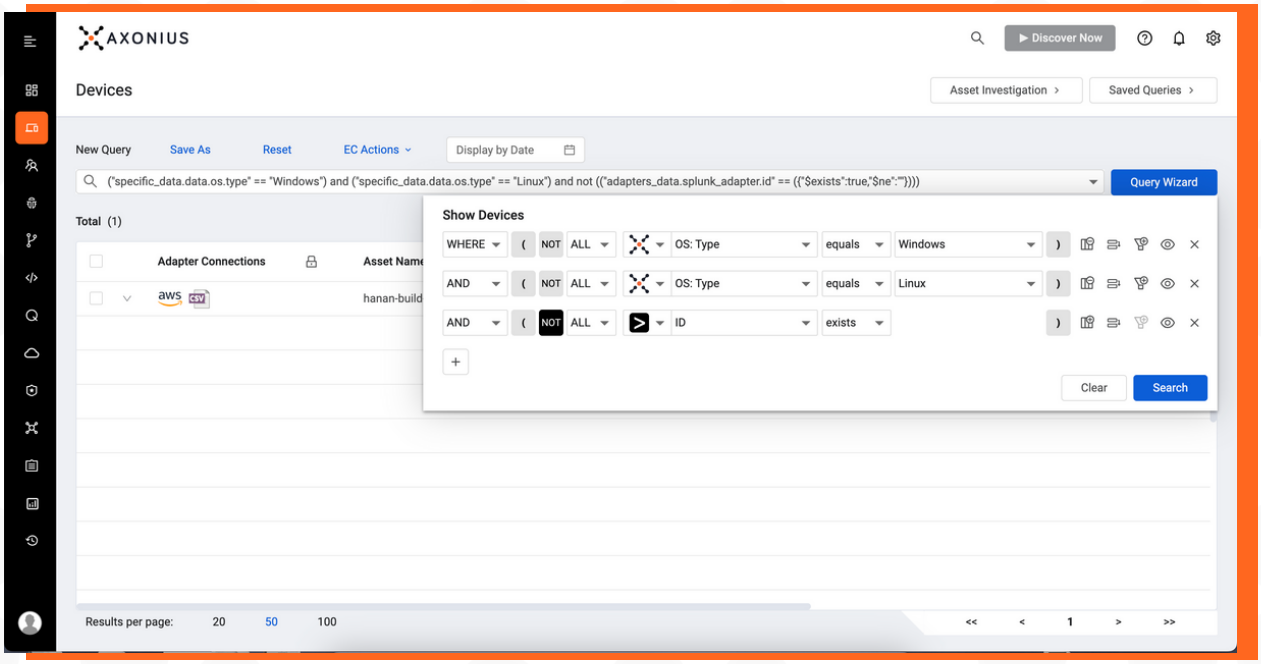
With a comprehensive and contextual asset inventory, including security log collection from Splunk, customers are able to quickly identify gaps in security policy and take action to remediate in the Axonius Enforcement Center.

AXONIUS

How It Works

Customers can connect Splunk in Axonius via a username and password or API key. Via Splunk search Macros, Axonius then ingests Splunk findings, normalizes, de-duplicates and correlates Splunk's event-based data against other 3rd party connected security tools and provides a complete and comprehensive inventory of the customers heterogeneous environment.

After this, Splunk can pull data from Axonius back into the Splunk Enterprise or SOAR platforms via the Axonius Add-On for Splunk and the Axonius App for SOAR (Phantom). Thus enabling Splunk users to view Axonius' enriched deduplicated and correlated asset, user, software and vulnerability inventory information alongside their traditional existing Splunk and Splunk Enterprise Security dashboards and investigators.



Interested in seeing what Axonius can do for your organization?

LET'S TALK