Silverfort App for Splunk

Splunk is a key component in security teams' detection and response capabilities. However, a SIEM is only as good as the data it receives and when it comes to Identity-based attacks that utilize compromised credentials, existing IAM solutions often do not provide enough data to detect ongoing malicious activity. The Silverfort platform solves this challenge by providing Splunk with granular and analyzed identity-protection data that empowers security analysts to drastically reduce investigation time and resolve identity threats more efficiently.

Rapid and Efficient Detection of Identity Threats

The Silverfort app for Splunk enables security teams to aggregate and correlate concrete detected identity threats. Instead of manually investigating security logs from cloud and on-premise IdPs like Entra ID, Okta, Ping and Active Directory, the Silverfort app provides security analysts with actionable threat detection information about identity-based threats such as Pass the Hash, Kerberoasting, Brute Force, etc. Moreover, Silverfort also provides the ultimate IoC of denied MFA requests, equipping security teams with detailed dashboards and security reporting that provide immediate insights into which users and machines are compromised, and how to respond accordingly. Using the Silverfort app for Splunk, security teams can easily monitor all authentication logs and requests, and identify and protect against malicious activity.

How the Silverfort App for Splunk Works

The Silverfort platform provides real-time monitoring and risk analysis for all user authentications and access requests and sends the correlated data to the Silverfort app for Splunk. Silverfort transfers all the identity and authentication data via Syslog to Splunk which correlates it with the data it receives from other sources in the environment. The app provides rich visualizations and in-depth details of MFA requests, attack methods, entities' risk levels, service accounts, user risk levels, and identity-based threat information. Together, integrating Splunk and Silverfort will empower SoC teams to detect in realtime identity-based attacks such as account takeovers and lateral movement across all their on-prem and cloud environments.

KEY BENEFITS

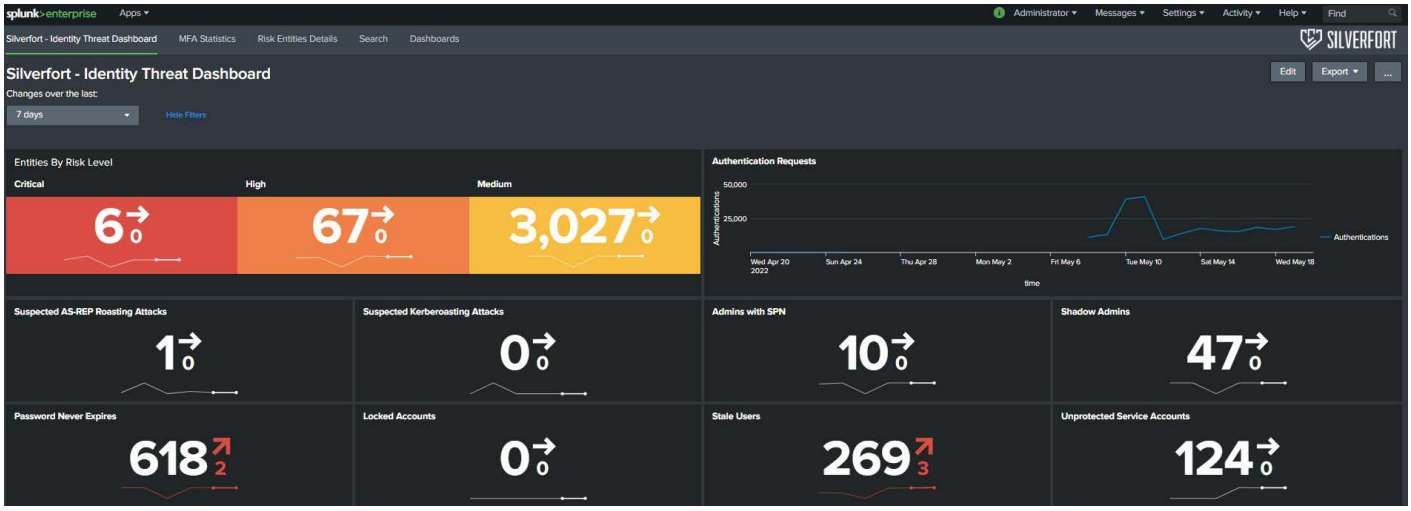
Actionable Threat Detection
Get concrete alerts of identity threats such as lateral movement, Pass the Hash, Kerberos, and more.

Automated Risk Analysis
Leverage Silverfort's ability to autonomously score the risk of each user and resource in the environment.

Optimized Investigation
Accelerate investigation time with granular forensic data on users, protocols, machines, and apps.

Consistent SOC Experience
Provide SOC teams with a native Splunk app in their security eco-system for a familiar user experience.

Security Focused Dashboards
Automate all security data and events with enriched and in-depth graphs and dashboards.



The Silverfort App for Splunk Dashboard
This detailed dashboard offers a complete picture, based on system logs, and highlights authentication spikes and trends.