Reservoir Labs

Rich Network Metadata for Splunk Enterprise Security (ES)

Multiply effectiveness of cyber alerts and investigations with seamless CIM integration

THE CHALLENGE

You don't need more data, or even more dashboards. You need the right data, organized in such a way that host, network, threat intelligence and other sources can easily be evaluated and cross-correlated. That's why you invest in Splunk® and tools that provide broad contextual awareness of events, actions, and assets that integrate with Splunk and Splunk ES out of the box, accurately, in minutes.

SOLUTION BENEFITS

R-Scope is an advanced threat detection network sensor that transforms raw network packets into rich Metadata.

- Metadata is normalized to the Splunk Common Information Model (CIM).
- Metadata integrates with Splunk ES sensors, sources, assets, identities, and threat intelligence.
- Metadata directly populates Splunk ES dashboards.
- Metadata provides critical context and correlation for Splunk ES alerts, risk analysis, and investigations.
- Metadata enriches Splunk operational intelligence.

You can also customize R-Scope to conduct intelligent packet capture, carve files of interest, and alert directly on uniquely-concerning events.

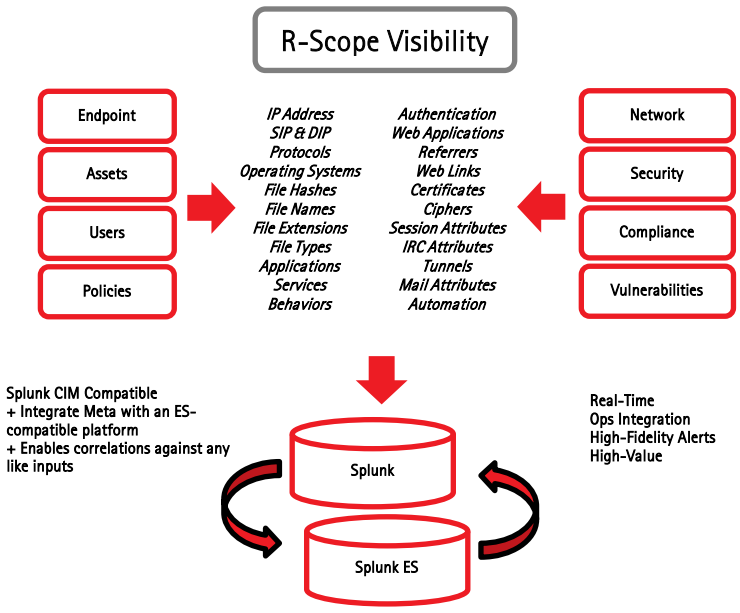
The Reservoir Technology Add-ons (TA) and Forwarders for Splunk and ES Security are packaged directly with R-Scope.

RESERVOIR LABS R-SCOPE SOLUTION OVERVIEW

R-Scope® is an enterprise-ready network appliance that leverages Bro to deliver real-time network visibility, situational awareness, and event detection at the speed of today's enterprise. R-Scope appliances seamlessly integrate with Splunk, Splunk ES, and the balance of your IT operations, equipping your teams with easy-to-use tools to defend against rapidly evolving cyber threats.

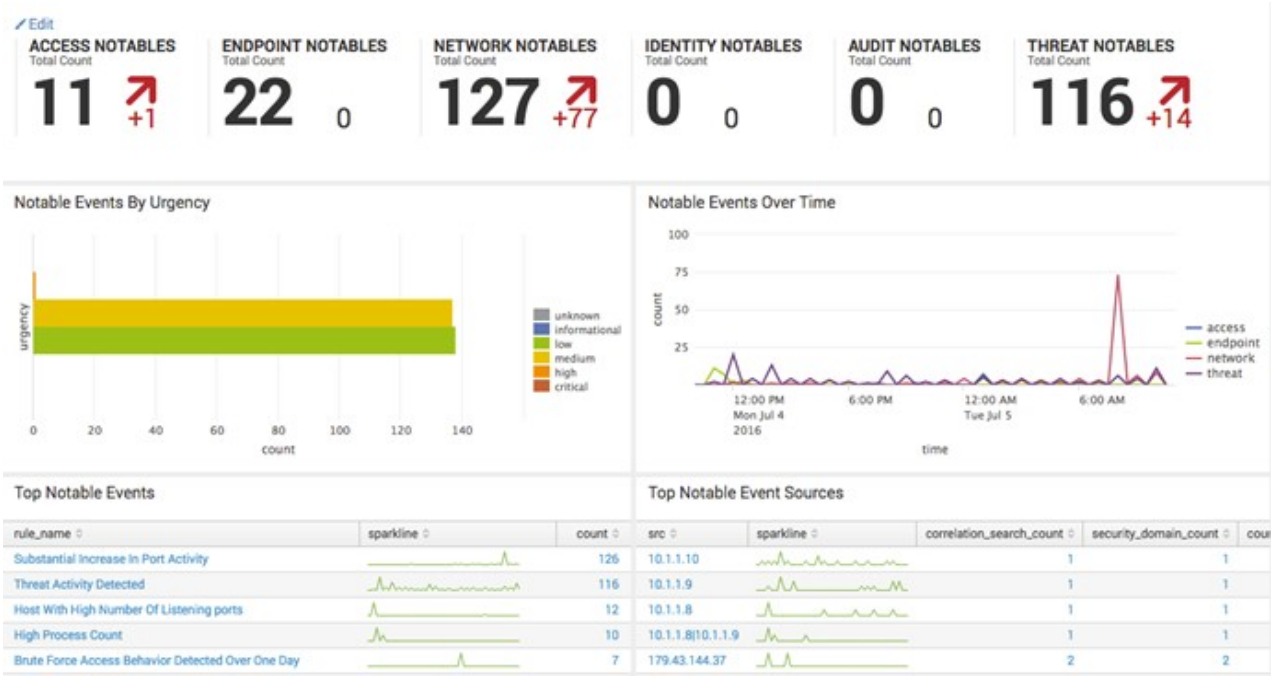
Splunk ES is a premium security solution that provides insight into machine data generated from security technologies such as network, endpoint, access, malware, vulnerability and identity information. Combining R-Scope's metadata and behavioral analytics with Splunk ES allows security professionals to proactively hunt for threats that traditional security solutions miss; to proactively identify security and policy violations that compromise security posture; and to build custom analytics to automate alerts.

BRIDGING THE GAP: LINKED DATA



Reservoir Labs

SPLUNK ENTERPRISE SECURITY (ES) DASHBOARD WITH R-SCOPE METADATA



splunk>

Splunk Inc. (NASDAQ: SPLK) is the market-leading platform that powers Operational Intelligence. We pioneer innovative, disruptive solutions that make machine data accessible, usable and valuable to everyone. More than 11,000 customers in over 110 countries use Splunk software and cloud services to make business, government and education more efficient, secure and profitable.

Join thousands of passionate users by trying Splunk solutions for free: http://www.splunk.com/free-trials

250 Brannan Street
San Francisco, CA 94107
(415) 848-8400
www.splunk.com

Reservoir Labs

Reservoir Labs is a privately held technology and solutions company headquartered in New York City that's earned the trust and respect of commercial and government clients as well as top-tier researchers around the globe. Our team of experts develop novel technologies to address the advanced security needs created by an evolving threat landscape.

Contact Reservoir Labs for a free trial license: sales@reservoir.com.

632 Broadway, Suite 803
New York, NY 10012
(212) 780-0527
www.reservoir.com