Setting up dashboards and reporting in ES

After data is in and some basic configurations are complete, it's time to start looking at dashboards and reports.

1. Identify and investigate security incidents.
   1. Use the Security Posture dashboard to monitor enterprise security status
      ▪ View a high-level overview of the notable events in your environment over the last 24 hours.
      ▪ Identify the security domains with the most incidents, and the most recent activity.
   2. Use the Incident Review dashboard to investigate notable events
      ▪ View the details of all notable events identified in your environment.
      ▪ Triage, assign, and review the details of notable events from this dashboard.

2. Accelerate your investigations with security intelligence.
   1. Use the Risk Analysis dashboard to assess the risk scores of systems and users across your network and identify particularly risky devices and users posing a threat to your environment
   2. Use the Protocol intelligence dashboard to provide network insights that are relevant to your security investigations.
      ▪ Identify suspicious traffic, DNS activity, email activity, and review the connections and protocols in use in your network traffic.
   3. Use the Threat intelligence dashboard to provide context to your security incidents and identify known malicious actors in your environment.
      ▪ Use the threat intelligence sources included in Splunk Enterprise Security and custom sources that you configure.
   4. User activity dashboards allow you to investigate and monitor the activity of users and assets in your environment.
   5. Web intelligence dashboards help you analyze web traffic in your network and identify notable HTTP categories, user agents, new domains, and long URLs.

   1. Access domain dashboards display authentication and access-related data, such as login attempts, access control events, and default account activity.
   2. View endpoint domain dashboards for endpoint data relating to malware infections, patch history, system configurations, and time synchronization information.
   3. View network domain dashboards for network traffic data provided by devices such as firewalls, routers, network intrusion detection systems, network vulnerability scanners, proxy servers, and hosts.
   4. Identity domain dashboards display data from your asset and identity lists, as well as the types of sessions in use.

• Docs: Overview of incident review in Splunk Enterprise Security
• Docs: Security posture dashboard
• Docs: Introduction to the dashboards available in Splunk Enterprise Security
• Blog: Modifying the incident review page

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.
Blog: What's new with Splunk Enterprise Security 6.6?