proofpoint.

EMAIL SECURITY SPLUNK INTEGRATION

ACCELERATE RESPONSE WITH A CONSOLIDATED VIEW OF ADVANCED THREATS

Enhanced visibility into email activity, threats and data exfiltration is now available as a part of our partnership with Splunk. The Email Security App for Splunk offers a single dashboard view and reporting to help you pinpoint security issues and respond quickly. It works in conjunction with our Email Security Technical Add-On (TA) to enrich the data the TA provides so it is more actionable and visual.

REQUIREMENTS FOR ENABLING EMAIL SECURITY TECHNOLOGY ADD-ON (TA)

- Proofpoint Email Protection version 8.0 or above
- Splunk Enterprise version 6.4 or above
- Splunk Common Information Model (CIM) Add-on version 4.8 or above

REQUIREMENTS FOR PROOFPOINT EMAIL SECURITY APP FOR SPLUNK

- Proofpoint Email Protection version 8.0 or above
- Splunk Enterprise version 6.4 or above
- Splunk Common Information Model (CIM) Add-on version 4.8 or above
- Proofpoint Email Security Add-On for Splunk 1.0.7 or above
- Proofpoint TAP SIEM Modular Input 1.0.1 or above

Security teams that are standardized on the Splunk Platform for threat research and incident response can act faster with Proofpoint email security information displayed within the Splunk interface. An at-a-glance view of security events and affected users allow security teams to save time responding to security incidents. With security information all in one place, security teams can quickly stop the spread of an attack. (Figure 1)

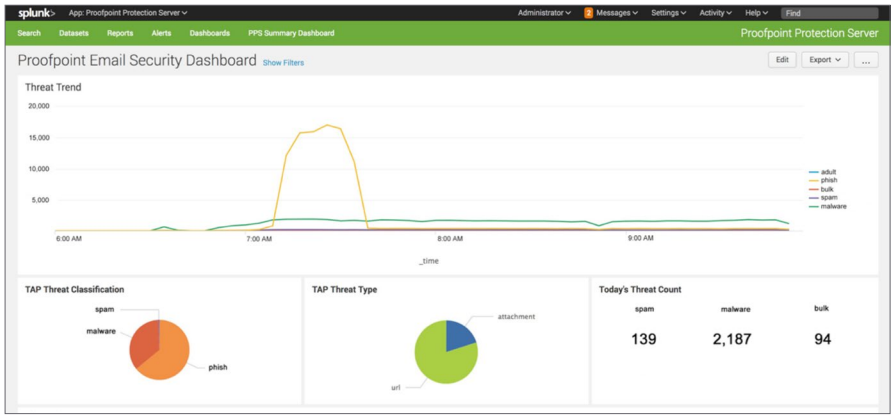

Figure 1 Email Security Dashboard

Email Security app integration with Splunk delivers security teams complete visibility into today's advanced threats including, ransomware, business email compromise (BEC), impostor, and credential phishing attacks. (Figure 2)

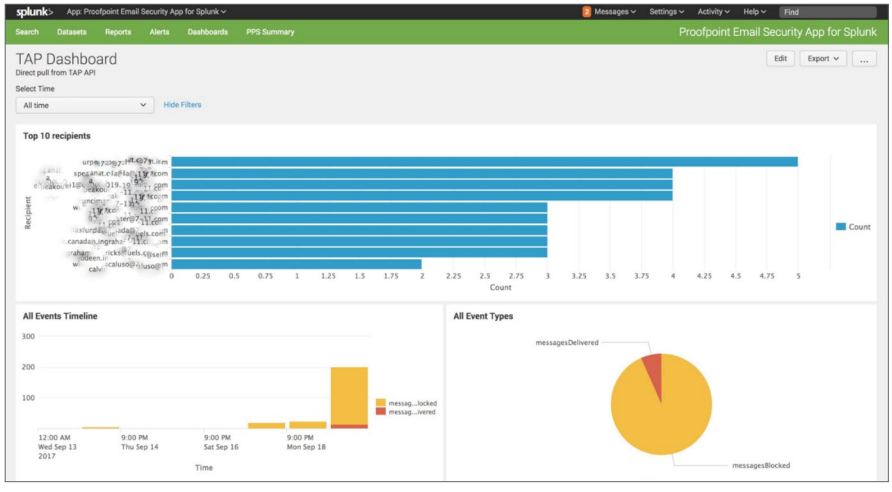

Figure 2 TAP Dashboard

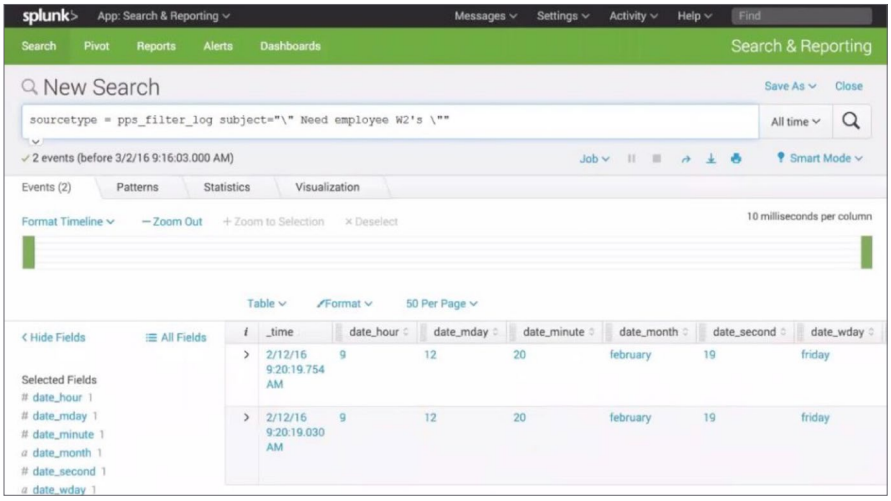

Figure 3 Sample search using Email Protection TA

Consolidate reporting with email security data feeds automatically correlated with Splunk Enterprise and Splunk Enterprise Security reporting as well as other sources. This helps security teams' zero-in on malicious insiders and other difficult to detect activity. Admins can create customize queries to search and analyze email logs with other sources of data (Figure 3).

The Email Protection TA requires the Splunk CIM Add-on and is available for download on Splunkbase.
The Email Security App is available for download on Splunkbase.

ABOUT PROOFPOINT
Proofpoint, Inc. (NASDAQ:PFPT), a next-generation cybersecurity company, enables organizations to protect the way their people work today from advanced threats and compliance risks. Proofpoint helps cybersecurity professionals protect their users from the advanced attacks that target them (via email, mobile apps, and social media), protect the critical information people create, and equip their teams with the right intelligence and tools to respond quickly when things go wrong. Leading organizations of all sizes, including over 50 percent of the Fortune 100, rely on Proofpoint solutions, which are built for today's mobile and social-enabled IT environments and leverage both the power of the cloud and a big-data-driven analytics platform to combat modern advanced threats.