Proofpoint Managed SIEM

Enhance the security of your Splunk environment

Key Benefits

- Enhanced detection for deeper visibility. Identify hidden threats using indicators of compromise from our emerging threat intelligence.
- Intelligent threat hunting for proactive responses. We research the bad actors and look for evidence in your environment. By yielding in-depth insights into contextual factors such as target scope, timing, and other aspects, we enable proactive response and remediation.
- 24x7 monitoring and detection. We deliver quick-turn optimisation of your environment. And our threat hunting team will support your SIEM program with round-the-clock monitoring and a fast mean time to remediate response.
- Expert security engineering. Our engineering team is world class and ensures the health of your Splunk environment.

This solution set is part of Proofpoint's integrated Human-Centric Security platform, mitigating the four key areas of people-based risks.

Proofpoint Managed SIEM gives you access to a team of experts whose sole focus is to detect, analyse and mitigate threats. The service delivers enhanced threat protection for Splunk environments. With it, you can shift some of the workload associated with security information and event management (SIEM) and gain advanced threat-hunting capabilities.

Proofpoint Managed SIEM helps ease the everyday challenges that your IT and infosec teams face when they try to manage large volumes of alerts and respond to them quickly. Without our service, these tasks can be overwhelming. And the problem is only getting worse with the addition of new detection technologies and the rising number of alerts that they bring with them. This can lead to alert fatigue, even if your teams apply best practices, runbooks and the latest tools and analytics.

Simplify Security Operations

Splunk customers who use Proofpoint Managed SIEM benefit in many ways, including:

- **Improved detection.** Unlike other services that simply operate off alerts that other SIEM solutions provide, Proofpoint Managed SIEM enhances detections with intelligence and threat indicators. This allows us to see threats others don't.
- **Threat hunting and pivoting.** Our security portfolio footprint spans many detection vectors, a powerful machine learning- and artificial intelligence-powered threat graph of more than 1 trillion nodes as well as more than 100 threat researchers. This breadth and depth let us not only detect threats, but also connect the dots between what might seem to be disconnected events.
- **24x7 threat protection.** A global team of security and threat detection professionals delivers Proofpoint Managed SIEM. Our experts are based in security operations centres around the world. And they identify, triage and, investigate threats for our customers around the clock.

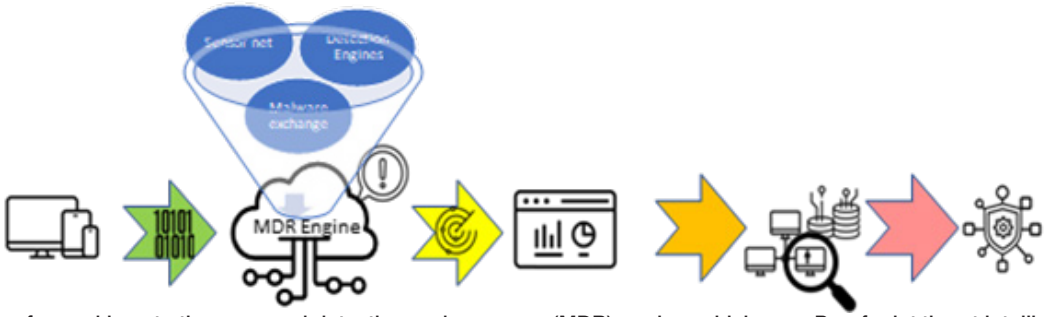

Figure 1: Sources forward logs to the managed detection and response (MDR) engine, which uses Proofpoint threat intelligence to create enhanced alerts. Our team triages, analyses and prioritises the alerts, then it conducts correlational analyses and proactively hunts threats to contain and respond to them.

Enrich Splunk Logs With Proofpoint Threat Intelligence

Proofpoint threat intelligence enriches logs from your network to identify threats that might have been missed and create new Proofpoint alerts. When alerts are raised, we triage and investigate them further. Details of the threats – such as key users, high-value targets and patterns of attack – are identified for prioritisation and mitigation. We evaluate the threats for advanced threat hunts when needed.

The Proofpoint team uses a streamlined approval workflow to remediate active threats quickly. The workflow also ensures that your organisation's security resources are released and available to work on more important or strategic security projects.

Advance Threat Detection for Your Organisation

Proofpoint enhances traditional SIEM capabilities with advanced detection based on industry-leading technologies and services. It delivers:

- **Unrivalled experience and proactive expertise.** Proofpoint threat intelligence allows us to be proactive as we protect you. Our worldwide sensor network and our team of threat analysts and researchers deliver threat-hunting and correlation across multiple platforms. Our experts are also forward-looking. They build defences that are tailored to your needs. They are also based on industry best practices and the latest Proofpoint products updates.
- **Continuous, cost-effective security operations.** Hiring, training, and retaining security staff is a challenge. This is even more true when it comes to specialty knowledge such as incident identification and response. Our managed services gives you access to our team of experts, who are always available to you. This helps you keep to a minimum the time, money, and resources that you must dedicate to address localised staffing challenges.
- **Regular reporting and executive-level insights.** We provide metrics that can give you valuable insights into security trends, identify opportunities for new security focus, and help you make informed decisions.

Proofpoint Managed SIEM integrates these capabilities to provide effective defence. Our team helps to ensure the health of your environment. And we optimise rule configuration in Splunk to detect threats accurately. This includes implementing system upgrades, patches, and tuning as needed. We combine advanced detection, prioritisation, and high-priority threat resolution with rapid mitigations. In short, our team delivers security engineering at its best. Let us help you reduce your security gaps and overall attack surface.

LEARN MORE

For more information, visit **proofpoint.com**.