splunk>

CASE STUDY

Travis Perkins PLC Adopts Analytics-Driven SIEM to Enable Hybrid Cloud Transition

Travis Perkins

Executive summary

Travis Perkins PLC is a British builders' merchant and home improvement retailer with 2,000 outlets and 28,000 employees. In 2014 the organization embarked on a "cloud-first" journey; however, its existing security information and event management (SIEM) solution couldn't provide the necessary security insights across a hybrid environment. Travis Perkins PLC reviewed the alternatives available and selected Splunk Cloud, Splunk Enterprise and Splunk Enterprise Security (ES) as its SIEM. Since deploying the Splunk platform, Travis Perkins PLC has seen benefits including:

- Improved visibility over hybrid infrastructure
- Gained ability to detect and respond to complex cyberthreats
- Reduced IT costs due to more efficient resourcing

Why Splunk

Faced with challenging market conditions during the recession, Travis Perkins PLC de-prioritized investment in technology. Recently, with business conditions improving, the company went through a strategic review of all technology infrastructure and adopted a cloud-first approach to reduce costs and increase flexibility. As Travis Perkins PLC rolled out a number of cloud services including G Suite from Google Cloud, Amazon Web Services and Infor CloudSuite, it quickly became apparent that its existing SIEM wasn't capable of providing the required insights into security events across a complex hybrid environment. Having reviewed alternatives including offerings from HP, IBM and LogRhythm, Travis Perkins PLC selected Splunk Cloud, Splunk Enterprise and Splunk ES to provide a single view of security-relevant activity.

Building security from the ground up

Travis Perkins PLC used the opportunity presented by the Splunk ES implementation to improve the security awareness of all individuals in IT, rather than focusing just on the security team. Employees in the IT operations teams now have access to specific dashboards and alerts so they can act as first responders to potential threats, instigating immediate action before escalating to the dedicated security team where necessary. As a result, Travis Perkins PLC has developed a highly effective and lean security operations center (SOC), without needing to invest the considerable resources this might usually require.

Industry

- Retail

Splunk Use Cases

- Security
- Fraud

Challenges

- Introduction of a cloud-first strategy required a new SIEM solution
- Complex mixture of on-premises legacy systems and cloud services meant it was difficult to gain overall infrastructure visibility
- Significant volume of advanced cyberattacks constantly threatened the business

Business Impact

- Enabled a lean SOC, with all IT operations staff empowered as cyberattack 'first responders'
- Intrinsic risk score-based correlation has improved the ability to detect and respond to significant threats
- Security incident investigation time reduced from three weeks to three hours

Data Sources

- Amazon Web Services
- Operating System logs (including Windows, Red Hat Linux, Ubuntu)
- FireEye
- Cisco Network Security
- Cloudlock
- ServiceNow
- Forcepoint
- Sophos

Splunk Products

- Splunk Cloud
- Splunk Enterprise
- Splunk Enterprise Security

Automating threat defense

With 24,000 employees based across the U.K. using a variety of devices to access corporate data, it has become crucial for Travis Perkins PLC to automate a large part of its cybersecurity. With Splunk ES, Travis Perkins PLC now calculates risk scores on different threat activities based on previously correlated data or alerts from the company's existing security solutions. With the business facing a particular problem with phishing emails, if an infected client is identified through correlation searches in the Splunk platform, it produces an automated alert. The relevant teams then react using a preset playbook response. The swimlanes in Splunk ES provide a holistic view into an asset or user and dramatically reduce the time it takes for security incidents to be investigated and resolved.

Enhancing security with machine learning

Travis Perkins PLC is planning on extending the capabilities of its lean SOC with additional insights driven by the Splunk platform's growing machine learning capabilities. Faced with a growing number of threats across the cybersecurity spectrum, Travis Perkins PLC will look to use machine learning to improve the quality of its existing alerting, reducing the number of false positives. Machine learning capabilities such as pattern recognition and anomaly detection will further enhance the effectiveness of the lean SOC model, while providing the highest level of protection across the business.

"Replacing our previous SIEM with Splunk Enterprise Security has dramatically improved our ability to effectively monitor and secure our complex hybrid environment. At the same time, using Splunk Cloud has helped ensure we have the flexibility we need to respond to the evolving threat landscape."

Nick Bleech, Head of Information Security
Travis Perkins PLC

"Replacing our previous SIEM with Splunk Enterprise Security has dramatically improved our ability to effectively monitor and secure our complex hybrid environment," says Nick Bleech, head of Information Security at Travis Perkins PLC. "At the same time, using Splunk Cloud has helped ensure we have the flexibility we need to respond to the evolving threat landscape."