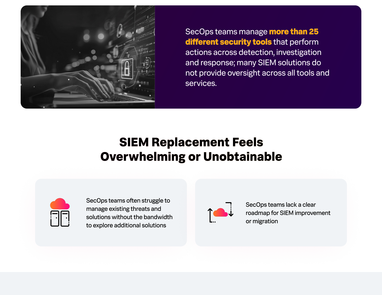
SIEM Replacement Assessment

Situation

Challenges in Modern SIEM Solutions

Traditional SIEM solutions haven't stepped up to serve the challenges faced by modern SecOps teams. SIEM solutions are business critical functions, making transitions and updates a daunting task. Moreover, there is not a clear blueprint to making this transition while maintaining a strong security posture.

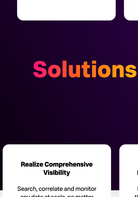
Traditional SIEM solutions limit security efforts and open the organization up to new threats.



Challenges

Lack of Innovation Heightens Security Risks

Security teams employing traditional or alternative SIEM solutions are static players in an arena with innovative bad actors and threats.



SecOps teams manage **more than 25 different security tools** that perform actions across detection, investigation and response; many SIEM solutions do not provide oversight across all tools and services.

SIEM Replacement Feels Overwhelming or Unobtainable

SecOps teams often struggle to manage existing threats and solutions without the bandwidth to explore additional solutions

SecOps teams lack a clear roadmap for SIEM improvement or migration

Implications

52%

of organizations report suffering a recent data breach

9

weeks is the average dwell time a bad actor penetrates - meaning that the average MTTD is about 2.24 months

88%

of organizations face talent challenges, impacting their security operation management

Solutions

Splunk Enterprise Security is the market-leading SIEM and security analytics solution trusted by SOCs around the globe. Its powerful capabilities enable you to realize comprehensive visibility, empower accurate detection with context, and fuel operational efficiency.

Realize Comprehensive Visibility

Search, correlate and monitor any data at scale, no matter where it resides.

Empower Accurate Detection with Context

Reduce noise, detect more threats, and identify risk with advanced detection technologies.

Fuel Operational Efficiency

Unify threat detection, investigation and response with seamless integration with Splunk SOAR.

Replacing Your Traditional SIEM Doesn't Have to Be Overwhelming

Splunk Professional Services experts support the replacement of traditional SIEM products across the globe with a framework for identifying the critical steps and timelines of the significant stages in a replacement project with a customized migration plan.

Identify use cases to be implemented in your new environment

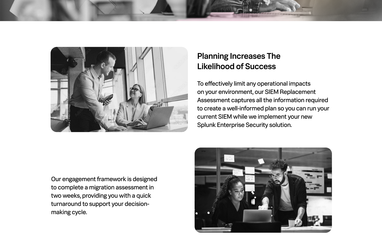
Develop a dual environment data feed plan

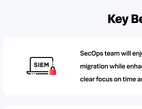
Evaluate data sources and map data requirements to use cases

Provide a customer network architecture recommendation for the new Splunk environment

Evaluate custom integration requirements (workflows, ticketing, etc.)

Conduct integration planning for existing Splunk instances already running in your organization





Planning Increases The Likelihood of Success

To effectively limit any operational impacts on your environment, our SIEM Replacement Assessment captures all the information required to create a well-informed plan so you can run your current SIEM while we implement your new Splunk Enterprise Security solution.

Our engagement framework is designed to complete a migration assessment in two weeks, providing you with a quick turnaround to support your decision-making cycle.

Key Benefits

SIEM

SecOps team will enjoy a clear, navigable solution for SIEM migration while enhancing their existing security posture with clear focus on time and financial investment to accomplish

Your team will receive recommendations to enhance security presence and can ask questions to Splunk subject matter experts

After our assessment, you can choose to implement your transition on your own or with our help

Let Splunk Professional Services Help You

Learn more