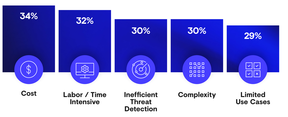
Secureworks

Top 5 Reasons to Replace Your SIEM with Secureworks® Taegis™ XDR

What are the most challenging attributes of SIEM for your organization?



1 Costs

Taegis XDR	VS	Legacy SIEM
Lowering Total Cost of Ownership • Cloud-native technology simplifies deployment, reduces maintenance costs, and decreases time-to-value. • Orchestration and investigation tools improve SecOps productivity. • Security analytics and applied threat intelligence reduce the need for supplemental security products.		**Total Cost of Ownership Reflects SIEM Complexity of Ownership** • On-Premises technology requires investment in hardware upfront and over time. • Additional licensing or 3rd-party products needed to enable orchestration features. • Additional security products and threat intelligence subscriptions required to generate high fidelity alerts.

Alert Fatigue is Growing

70% of security analysts investigate 10+ alerts each day (up from 40% last year)[2]

78% state that it takes 10+ minutes to investigate each alert (up from 64% last year)[2]

2 Labor & Time

Taegis XDR	VS	Legacy SIEM
Trust Your Alerts Reduce the volume of threat alerts with minimized false positives from powerful analytics so your team sees only the insights that matter		**Alert Fatigue** Detects high volume of alerts with no context provided, thus increasing the likelihood of missing breaches and increasing the time and resources to investigate them.

The Ability to Detect Unknown Threats is a Necessity

80% An average of 80 percent of successful breaches are new or unknown "zero-day attacks"[3]

2X New or unknown zero-day attacks are expected to more than double in the coming year[3]

3 Threat Detection

Taegis XDR	VS	Legacy SIEM
Detect Sophisticated Threat Recognize adversaries by their behavior, be alerted to unknown and emerging threats, and quickly report if your organization has been hit in the past with an attack just discovered		**Alert Fatigue** • IoCs and basic rules are not sufficient for detecting modern threats • Bolt-on analytics engines add complexity and cost

Security Pros Reveal Top Three Challenges of SIEM Complexity

38.5% Administration[4]

32% Deployment[4]

29.5% Operations[4]

4 Complexity

Taegis XDR	VS	Legacy SIEM
Simplifies Security Operations • Consolidation of multiple security tools into a single threat detection and response solution • Since XDR is cloud native, implementation can be performed in days – not weeks		**Consequences of Complexity** Hard to find security experts will continue doing administrative platform management tasks required by most SIEMs instead of defending against threats

5 Use Cases

Taegis XDR	VS	Legacy SIEM
XDR has added SIEM uses cases: • Log collection and retention • Search & Reporting • Custom Use Case Support **And some not covered by legacy SIEMs:** • User Behavior Analysis • Cloud Security Monitoring • Effective Incident Investigation		**Primary SIEM Use Cases Include:** • Basic Security Monitoring • Compliance & Control Monitoring • Basic Search & Reporting As data volume grew and move to the cloud, SIEM tools have become less effective at covering use cases in this environment

[1] Enterprise Strategy Group The Impact of XDR in the Modern SOC, Nov 2020
[2] CriticalStart: The Impact of Security Alert Overload, Q2 2019
[3] Forrester Institute, The Third Annual Study on the State of Endpoint Security Risk, January 2020
[4] SUMO Logic: SIEM Complexity Challenges February 2020

See XDR in Action

Begin by visiting secureworks.com to learn more

Secureworks