

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

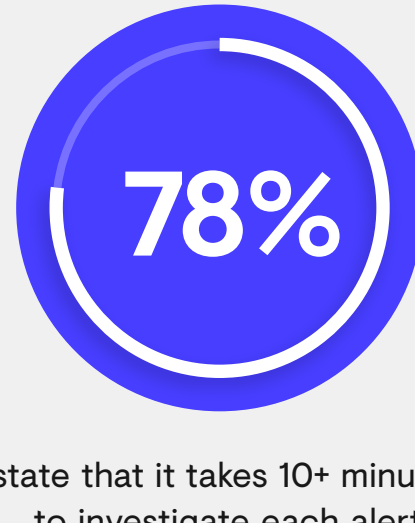
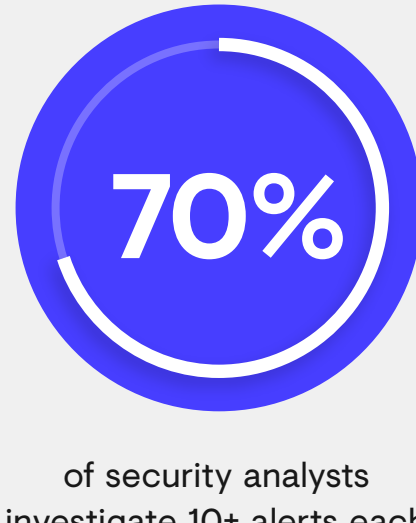
What are the most challenging attributes of SIEM for your organization?



1 Costs

Taegis XDR	VS	Legacy SIEM
<p>Lowering Total Cost of Ownership</p> <ul style="list-style-type: none"> 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. 		<p>Total Cost of Ownership Reflects SIEM Complexity of Ownership</p> <ul style="list-style-type: none"> 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.

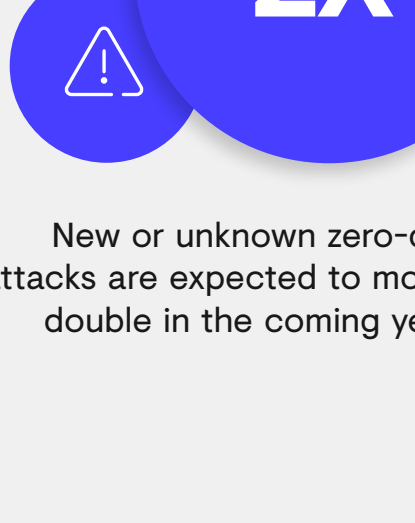
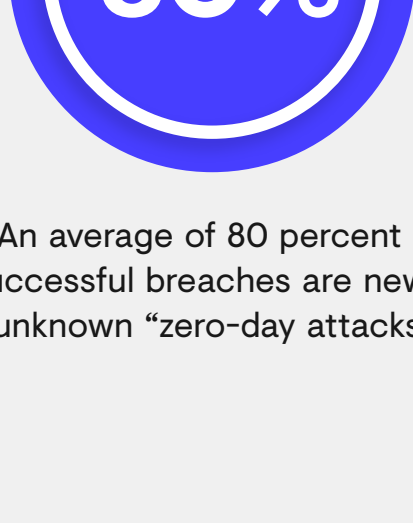
Alert Fatigue is Growing



2 Labor & Time

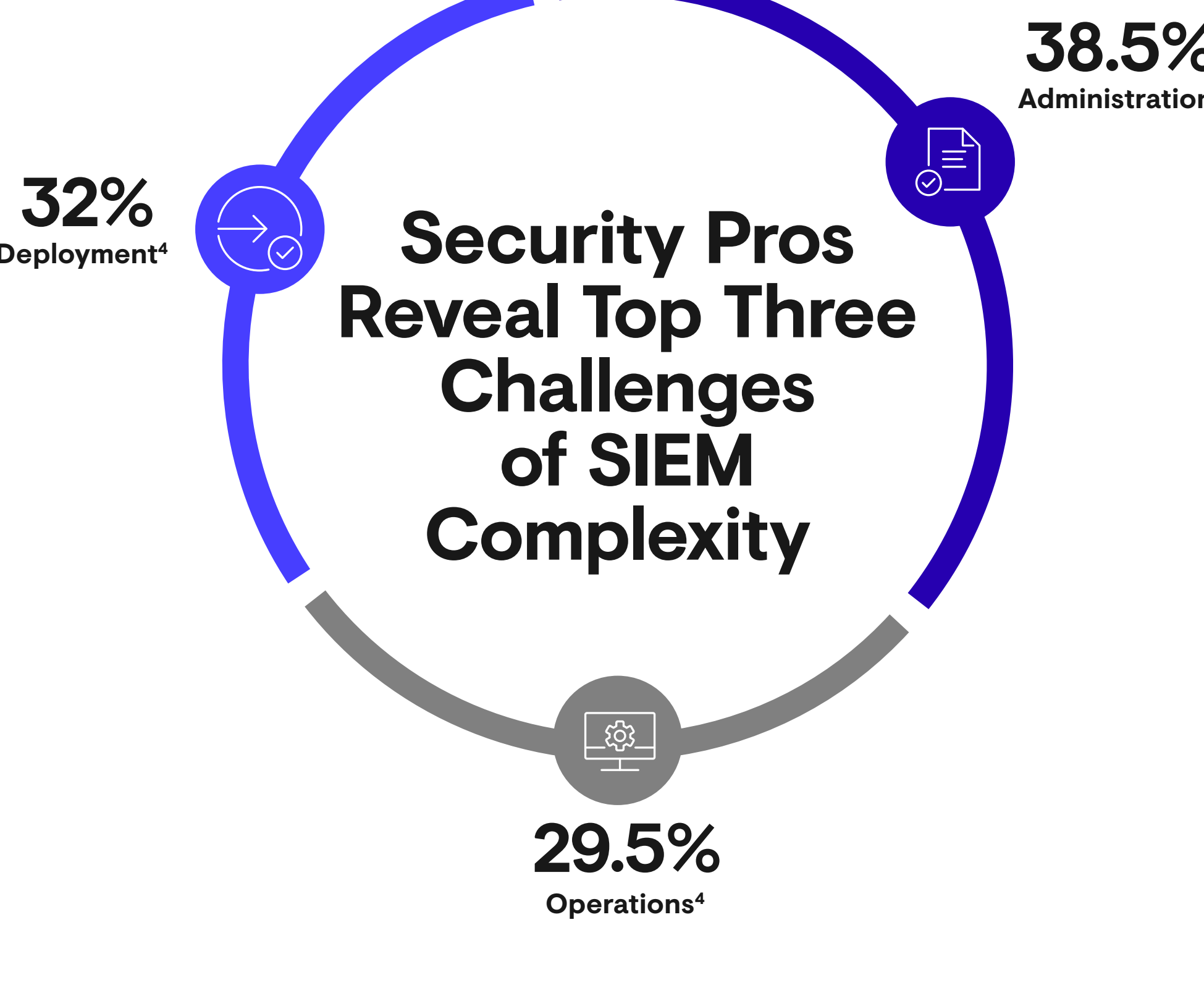
Taegis XDR	VS	Legacy SIEM
<p>Trust Your Alerts</p> <p>Reduce the volume of threat alerts with minimized false positives from powerful analytics so your team sees only the insights that matter</p>		<p>Alert Fatigue</p> <p>Detects high volume of alerts with no context provided, thus increasing the likelihood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

The Ability to Detect Unknown Threats is a Necessity



3 Threat Detection

Taegis XDR	VS	Legacy SIEM
<p>Detect Sophisticated Threat</p> <p>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</p>		<p>Alert Fatigue</p> <ul style="list-style-type: none"> IoCs and basic rules are not sufficient for detecting modern threats Bolt-on analytics engines add complexity and cost



4 Complexity

Taegis XDR	VS	Legacy SIEM
<p>Simplifies Security Operations</p> <ul style="list-style-type: none"> 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 		<p>Consequences of Complexity</p> <p>Hard to find security experts will continue doing administrative platform management tasks required by most SIEMs instead of defending against threats</p>

5 Use Cases

Taegis XDR	VS	Legacy SIEM
<p>XDR has added SIEM uses cases:</p> <ul style="list-style-type: none"> Log collection and retention Search & Reporting Custom Use Case Support <p>And some not covered by legacy SIEMs:</p> <ul style="list-style-type: none"> User Behavior Analysis Cloud Security Monitoring Effective Incident Investigation 		<p>Primary SIEM Use Cases Include:</p> <ul style="list-style-type: none"> Basic Security Monitoring Compliance & Control Monitoring Basic Search & Reporting <p>As data volume grew and move to the cloud, SIEM tools have become less effective at covering use cases in this environment</p>

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 Ponemon Institute, The Third Annual Study on the State of Endpoint Security Risk, January 2020
⁴ SUMO Logic: SIEM Complexity Challenges February 2020