The rise of cybersecurity analytics and operations platforms

From the boardroom to the SOC, enterprises are searching for cybersecurity analytics and operations solutions that improve both efficacy and efficiency.

The analytics and operations challenge

The rapidly evolving threat landscape makes it difficult to keep up with trends.
The changes in the regulatory environment.
The increasing volume of security alarms.
The gaps in tools and processes which hinder understanding the entire cybersecurity picture.

From the boardroom to the SOC, enterprises are searching for cybersecurity analytics and operations solutions that improve both efficacy and efficiency.

Analyzing and operations program objectives

When asked to identify their security analytics and operations objectives, large organizations point to:

- Advancing the ability to detect and remediate attacks: 34%
- Improving operational efficiency: 27%
- Reducing the amount of time for incident detection and remediation: 27%
- Integrating external threat intelligence with internal security data collection and analysis: 26%
- Adding custom functionality that sits above existing security tools: 19%
- Contributing factors include: 19%
- The loss of time and personnel when dealing especially with internal cyber interspers: 18%

The bigger truth

Enterprises seek to improve their ability to detect and remediate attacks, reduce response times, and integrate and consolidate information to provide the big picture view. Threat intelligence provides a foundation for improving risk management and efficacy. Additional gains in efficiency can be realized with automation and orchestration.

Learn more

www.threatq.com/esgresearch

The threat intelligence continued to be a foundational element of strong cybersecurity operations and analytics.

The top four intelligence objectives include:

- Improving risk management: 33%
- Establishing a central threat intelligence service to guide smaller organizational units: 25%
- Using threat intelligence to automate remediation: 23%
- Including threat intelligence as part of every business activity for making a different in the wild: 22%

Automation and orchestration

To improve productivity and accelerate incident detection and response, organizations are looking toward security automation and orchestration.

The top four priorities cited include:

- Integrating external threat intelligence with internal security data collection and analysis: 35%
- Adding source functionality that integrates existing security tools: 30%
- Automating basic remediation tasks: 29%
- Correlating and contextualizing security data from multiple tools: 28%

The analytics and operations challenge

72% find cybersecurity analytics and operations MORE difficult than it was 2 years ago. Contributing factors include:

- The rapidly changing threat landscape makes it difficult to keep up with threats: 26%
- The changes in regulatory environment: 19%
- The increasing volume of security alarms: 19%
- The gaps in tools and processes which hinder understanding the entire cybersecurity picture: 18%