Executive Summary:
The Business Value of Google Security Operations

Michelle Abraham
Research Director,
Security and Trust, IDC

Matthew Marden
Research Vice President,
Business Value Strategy Practice, IDC

The security information and event management (SIEM) platform is the central analytics tool for the security operations center. Telemetry and log data from other security tools are brought into the SIEM so that it can be correlated, and new understanding can be gained when it is analyzed together rather than in separate silos.

Bringing the data together makes investigations easier, helping identify more adversary activity and increasing the efficiency of the security team. This in turn lowers the probability of large-scale attacks because teams detect adversary activity earlier and can stop threat actors before they take down an entire system.

SIEMs are complex security platforms with many data connectors and numerous options for detection rules. The rules must be tuned to the organization's specific environment to reduce false positive alerts so security teams can focus on detecting and investigating critical incidents. In addition to tuning, developing and running automated playbooks can greatly improve the efficiency of security teams by offloading mundane tasks in order to have time to focus on those that call for their expertise. Security teams need to make sure they are receiving the full value from their SIEM, taking advantage of all the capabilities.

IDC interviewed organizations using Google Security Operations (formerly known as Google Chronicle) to understand its impact on their security capabilities and operations. According to study participants, Google Security Operations enables them to analyze and correlate far more data, which leads to improved security outcomes and efficiencies for the staff responsible for analyzing and engineering security data.

Business Value Highlights

- **$13.50 million** higher revenue per organization per year
- **7 months** to payback
- **407%** three-year ROI
- **283%** higher data ingestion volumes
- **87%** more potential threats identified
- **85%** more capacity for data logs
- **60%** reduced likelihood of a major security incident
- **42%** more efficient security operations teams

IDC calculates that interviewed Google customers will realize average annual benefits worth $4.29 million per organization ($104,500 per 1,000 endpoints covered) by:

- Significantly improving threat identification and resolution capabilities, thereby limiting the likelihood of suffering serious security incidents
- Helping security operations teams work more efficiently by providing high-quality insights about threats and correlation and allowing them to spend less time on monitoring activities
- Capturing higher revenue by moving with greater speed and confidence to address business opportunities and customer needs
- Enabling ingestion of significantly more data and data logs by separating data volumes from incremental costs

While this IDC study demonstrates the tangible benefits for study participants of using Google Security Operations, the more intangible value of peace of mind can be as important. As an interviewed CISO at an EMEA automotive-related company with annual revenue of $5 billion to $10 billion explained: *"Our cybersecurity teams deal with issues faster with Google Security Operations, but they also identify more issues. The real question is 'How much safer do I feel as a CISO with Google Security Operations versus my old platform?' and I would say 100 times safer."*

Read the full white paper

Produced by: IDC Custom Solutions
Business Value Executive Summary, sponsored by Google Cloud
January 2024 | IDC #US51386223