Google Cloud

Deloitte.

The Evolution of the SOC

At the heart of many enterprise security teams, the Security Operations Center (SOC) stands ready to protect the business. Combining people, processes, and technology, it manages and enhances the security posture of the organization.

The SOC is staffed with security analysts and engineers responsible for technical operations, troubleshooting, and to guard against bad actors who are intent on accessing corporate infrastructure and data.

As the threat landscape continues to evolve, so must the SOC. Yet, even decades in, scalability challenges remain a constant:

- Ever-expanding attack surfaces
- Too many alerts from too many tools
- A limited supply of talented security experts

The next generation SOC

Task automation has made a big difference for the SOC, helping security teams overwhelmed by the sheer number of alerts, false positives, and other high-volume / low-value work.

The modern day SOC will shift from task to decision automation. This logical next step will reduce the volume of noise and the tools needed for threat detection. Decision automation uses artificial intelligence (AI) to help automate how the environment is monitored and how events, once detected, are triaged.

Orchestration, the ability to pull all telemetry and workflows into fewer views, is another means by which the modern SOC will minimize distractions so personnel can focus on analysis and investigation.

Technologies to help scale

Efficiencies within the SOC can also be realized from technologies such as Chronicle, a threat detection platform that automatically finds threats in real-time and at scale.

Chronicle supports massive data ingestion and storage, alleviating traditional cost and scaling limitations, and broadening the lens for anomaly and machine learning (ML) / AI-based detection. With data stored and analyzed in one place, security teams can investigate and detect threats more efficiently.

With Chronicle, the SOC is able to make better use of verbose data sources such as EDR/XDR, DNS, and NGFW. By not having to compromise on source selection from Security Information and Event Management (SIEM) platform licensing restrictions, the SOC can streamline parsing and ingest functions, shifting its focus from data management to threat detection.

A path forward

With the security landscape evolving rapidly, sourcing skilled cyber specialists can remain a challenge. Re-thinking the SOC workforce model is an important first step.

As new risks emerge, the SOC must continually refine how it works, focusing on three areas of innovation:

1. **Automation to reduce busy work**
2. **Orchestration to reduce distraction and increase efficiencies**
3. **Next generation monitoring platforms to extract value from large stores of relevant and critical data**

This modern approach can help liberate security teams from mundane and routine work, so they can dedicate their expertise and time to the most challenging scenarios.

Chronicle collaborates with Deloitte to provide cloud-native security analytics and monitoring for organizations to hunt and identify threat signals across people, processes, and technology.

Chronicle
now part of Google Cloud

For more information, read the whitepaper or contact us:

- Philip Bice
  Global Manager, Service Providers Partnerships and Channel at Google Cloud
- Ryan Lee
  Alliance Manager at Deloitte Services LP

As used in this document, “Deloitte” means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.