Company Profile: Global healthcare industry leader

Security Analytics Challenges

A US based healthcare sector market leader was contending with constantly growing security telemetry volumes. Over the years, growth of infrastructure and new security tools had significantly expanded the aggregate log volume their SOC needed to access for investigations.

Meanwhile low and slow (APT) threats warranted longer retention periods with quick or hot access but queries were already taking too long. Scaling their existing on-premise SIEM solution would imply higher license costs as well as more infrastructure to buy, deploy and manage. The deployment of a modern EDR, valuable for its rich telemetry but voluminous in its logging output, drove them to start identifying new solutions to address their security analytics challenges and needs.

Key Challenges

- Growing log volumes
- Existing SIEM TCO
- Analyst caseload
- Time to remediation
- EDR telemetry value

Chronicle Security Analytics Platform

The security team evaluated existing market leaders and emerging technologies based on architectural, economic and functional criteria. Chronicle was selected by the team for its clear advantages around:

TCO	Fixed cost pricing for all security telemetry including future growth No infrastructure procurement, deployment, tuning costs 1 year of built-in retention in hot state
SCALE	Auto-scaling SaaS offering built on core Google infrastructure
SPEED	Seconds to search an entire year of security telemetry (>500 TB)
ANALYTICS	Continuous and automated IoC matching with all telemetry Purpose built security investigation views (Assets, Users, IoCs)

> **We chose Chronicle for its productivity gains, economic advantages, and its speed and depth of security investigations**

Security Impact and Outcomes

Time to Remediation (TTR)	Previously, SOC burnout led to a shift in the primary metric from TTR to caseload. The speed and SOC optimized interface of Chronicle has enabled not just a return to TTR but an introduction of a 15 minute limit on case investigation time.
SOC Workload Balance	In the organization's 2-tier structure, previously the smaller subset of L2 analysts had to take on a disproportionate number of cases. With Chronicle, major threat categories like phishing have been fully operationalized into the hands of L1 analysts, freeing up limited L2 resources to focus on advanced threats such as healthcare and retail fraud.
SOC Budget Optimization	The license cost of security analytics is now fixed and predictable and encompasses future data growth as well. Since Chronicle is a SaaS offering, this benefit also extends to associated infrastructure costs. Additionally, the productivity gains optimize operational (personnel) budget.
Return on Security Investment (RoSI)	Chronicle has increased the return on other security investments such as EDR and web proxies. Now these high volume data sources are retained for a full year and instantly accessible for analysis. Similarly, the threat intelligence platform (TIP) investment is maximized through continuous, retroactive matching against all security telemetry.