Have Your SIEM... and Augment It Too

3 achievable use cases when you add Chronicle to your SecOps infrastructure

Many security operations teams are not quite ready to ditch their legacy SIEMs. But they still crave stronger visibility, scale and speed to adequately address the modern hybrid threat landscape.

Instead of ripping and replacing, what if you choose to deploy a modern SIEM to sit alongside your traditional version–and in the process introduce enhanced value to the entire SOC stack?

It's called augmentation, and here are three memorably titled use cases for adding the cloud-native Chronicle SIEM to achieve greater detection, investigation, and response outcomes.

01

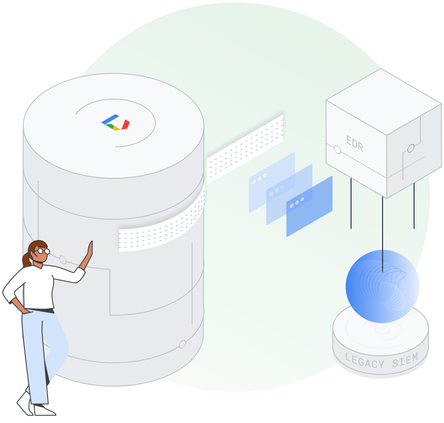
The "Cover All Your Bases" Use Case

The rapid adoption of the cloud and IoT means more security telemetry and the need to ingest breach-indicating server logs like DNS/DHCP. Chronicle SIEM can be used to analyze voluminous and more demanding data sources with sub-second search across petabytes of data, while your legacy tool is used to capture more traditional SIEM data sources.

02

The "Hoarding is Rewarding" Use Case

You love your EDR tool. In fact, you consider the data it produces to be the single source of truth for every device living across your network. Unfortunately due to high cost, there may be times when your existing legacy SIEM cannot retain your EDR data for an extended period. Chronicle SIEM allows you to ingest and store endpoint telemetry at least 10-times longer–and correlate with broader enterprise signals for greater visibility and deeper analytics.



03

The "Automation Station" Use Case

Response time is the difference maker in any unfolding security incident. Yet many organizations lack automation and orchestration capabilities, resulting in delayed and manually intensive efforts to respond to threats. Integrating SOAR with Chronicle SIEM, as part of a SecOps suite of solutions, outfits your team with automated playbooks, case management and team collaboration that can result in faster and more effective response.

When it comes to security solutions, going the "less is more" route isn't an overnight process. Nor is your SecOps transformation. Occasionally adding a single tool can offer far more value than subtracting one. These three Chronicle augmentation use cases are proof that a modern SIEM can free you from costliness and complexity as you take on today's adversaries.