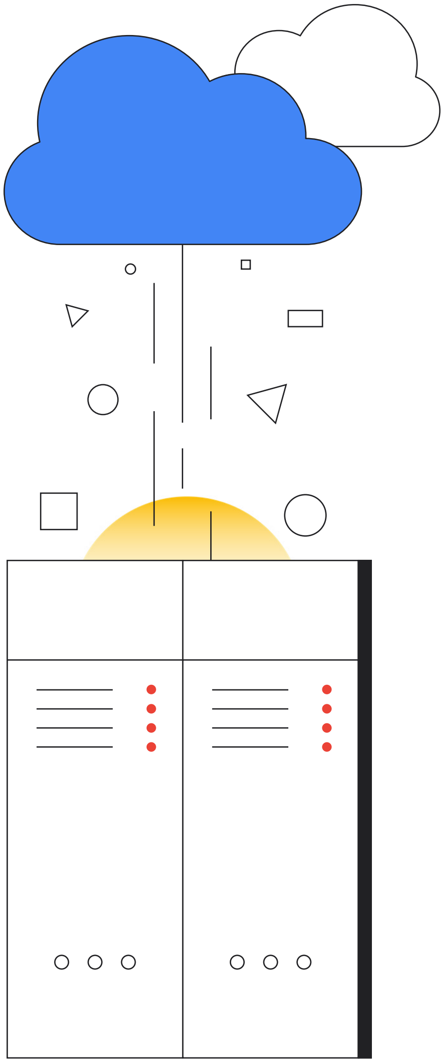
How Chronicle SIEM can help augment your SOC stack

Anton Chuvakin | Dave Herrald

Google Cloud

White paper

Table of Contents



How Chronicle SIEM can help augment your SOC stack

Introduction

This paper will evaluate using Google Chronicle SIEM to augment other comparable tools already deployed in your environment. We will review drivers for introducing additional detection capabilities, recommend joint architectures and best practices, and discuss common problems and how to avoid them.

This paper is for both Chronicle SIEM customers and those looking to address some limitations of your existing SIEM. Current Chronicle SIEM customers can use this to plan the optimal joint architecture for their needs and circumstances.

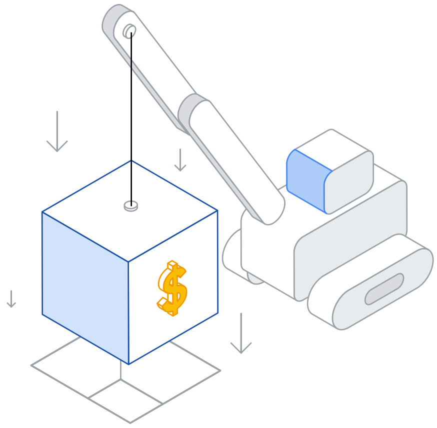
Why augment?

- Cost savings due to license, hardware and maintenance costs of reduced data volumes flowing into a volume-priced SIEM
- Higher cost savings for data retention and search (Chronicle SIEM keeps one year of data for no extra price and no per gigabyte costs)
- Dramatically higher search performance without a corresponding cost increase
- Improved security visibility due to EDR and other high volume telemetry being collected and analyzed
- Longer data retention especially for EDR and cloud data sources
- Improved threat intelligence matching especially for retroactive matching of intel versus security telemetry
- Expanded and new use case coverage for SOC such as deeper EDR data analytics or cloud threat detection.

Ultimately, augment is about eliminating existing SIEM blind spots without breaking the bank. So, why would a security organization decide to introduce a new tool to its security stack? Especially one that, at first glance, performs a task similar to existing tools? Most security leaders would rather consolidate tooling than expand it.

Still, there are powerful reasons to augment existing detection and response functionality with Chronicle SIEM. After all, the mission of the security operations center (SOC) is to protect an organization from security threats by rapidly detecting and responding to attackers in the most effective way that mitigates the most harm. If the addition of a tool can demonstrably improve the organization's ability to fulfill this mission at a reduced total cost, then it is worthwhile.

Lower cost



Some security organizations think of tool reduction/consolidation in very literal terms. For example, some will only consider a new tool if it replaces another. However, leaders should instead evaluate whether the benefits of augmenting detection capabilities help them achieve the SOC mission. For example, suppose an organization can save millions of dollars by using two tools instead of one. In that case, an additional tool may not be such a concern for most leaders, even if it leads to some additional complexity. Anyhow, transforming the SOC may require more than a better SIEM and a modern SOAR.

New use cases

This motivation for augment occurs when there's a way to gain significant additional capabilities and where the value of those capabilities outweigh the associated incremental cost and complexity. Such value typically comes from the Chronicle SIEM per-employee pricing model, and its powers of data retention, scale, search performance, data quality, embedded threat intelligence, and overall detection approach.

Further, it may happen when a new tool addresses the use cases that the old tool does not address, while the tool that addresses all use cases in one shot either doesn't exist or is too pricey.

New telemetry sources

More specific to the domain of security operations, the situations where certain data sources cannot be collected by the original tool or data cannot be retained for a required retention period such as a year or even multiple years. For example, this means that a particular data set (VPN logs or EDR data) needs to be kept useful for a year while the existing tool cannot do that. More precisely, there are industry examples where one security tool vendor charges as much for seven-day retention of telemetry data as another charges for a year.

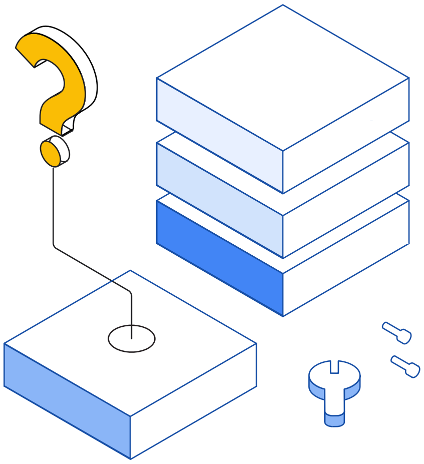
Note that when they say that the tool cannot do that, it does not always mean that it is technically impossible, sometimes it means that it is economically implausible. For example, a particular tool may theoretically be configured to use a large amount of hardware to search petabytes of security data in seconds. However, if the cost of such hardware amounted to a nine-digit number, all companies would consider it impossible, despite the theoretical technical capabilities of the tool.

Summary

As a result, augment your SIEM with Chronicle SIEM when it delivers value, reduced cost, or expanded new use case coverage for your SOC or detection and response team.

How to augment?

How do you evaluate if your situation is a good case for augmenting your existing toolset with Chronicle SIEM?



Is your current detection and response tool set delivering on the entirety of required use cases, from detection to alert triage to investigation and response and threat hunting?

If the answer is “yes,” perhaps there is no immediate need for another tool. However, for many organizations the current answer is “no” or at least “not entirely.” Hence they should consider deploying Chronicle SIEM alongside the other tools they use for detection and response.

Note that sometimes the answer to this is “yes” but the cost growth curve is unsustainable. This means that another tool may still be of value, especially if it is simple and won’t cause an unacceptable increase in complexity.

The existing tool may, in theory, deliver on the use cases required, but not on the speed required for delivering the tasks, such as during large-scale incident response. Examples may include ransomware response where minutes or even seconds count. Quantitative speed differential delivers the qualitative differences–a difference between successful and failed outcomes, in fact.

As another scenario, is your current tool failing to collect all the data needed? Is the tool slow because there is no way to scale it, either practically or economically? In this case augmenting with Chronicle SIEM is a good answer as well.

Summary

If any of the following is true, augment needs to be considered:

- Does your SIEM address all current and planned use cases cost-effectively?
- Does your SIEM address the current use cases but at an unsustainable cost?
- Does your SIEM address the current use cases but future scaling is not assured?

Augment use cases

Let's consider the augmentation scenarios that arise in the field. In many situations, Chronicle SIEM is selected as either a threat hunting tool, incident response tool or detection and response tool–or all the above. This means that another SIEM handles tasks like compliance reporting, and perhaps some others. (Chronicle SIEM has partners that can cover those needs as well.)

These tools would coexist and will need to be integrated in order for the detection, reporting, and hunting missions to be successful. The organizations that need to achieve excellence in each of the use cases, without breaking the bank, will select the approach of augmenting their existing SIEM with Chronicle SIEM.

The question of data sources that would feed Chronicle SIEM, another SIEM, or both comes up a lot. For example, if Chronicle SIEM is used for security incident response, there is almost no data source that can be disqualified from inclusion.

Naturally, in many augmentation scenarios where Chronicle SIEM co-exists with another tool, evolution leads to another tool being discontinued while Chronicle SIEM takes on more and more responsibilities. For example, for some clients who started using Chronicle SIEM for incident investigation and hunting while using another tool for detection transition to using Chronicle SIEM for all the tasks while limiting the old tool to specific niche uses.

Augment architectures

What are the practical architectures for augmenting your detection response tool with Chronicle SIEM?

Log routing to two SIEMs

If Chronicle SIEM is chosen to support investigation and hunting use cases, the tool needs access to a broad set of data. In this case, it would make sense to send all the data to Chronicle SIEM and the subset to the tool used for other purposes as shown in Figure 1. Note that it is not always easy to send logs to multiple destinations. Some sources can be configured for multiple destinations. In many cases, however, a specially configured forwarder, a streaming event platform like Apache Kafka or Google Cloud Pub/Sub, or a third-party log routing service must be implemented.

A SOAR platform such as Chronicle SOAR or another tool is used to unify the querying activity across multiple SIEM tools.

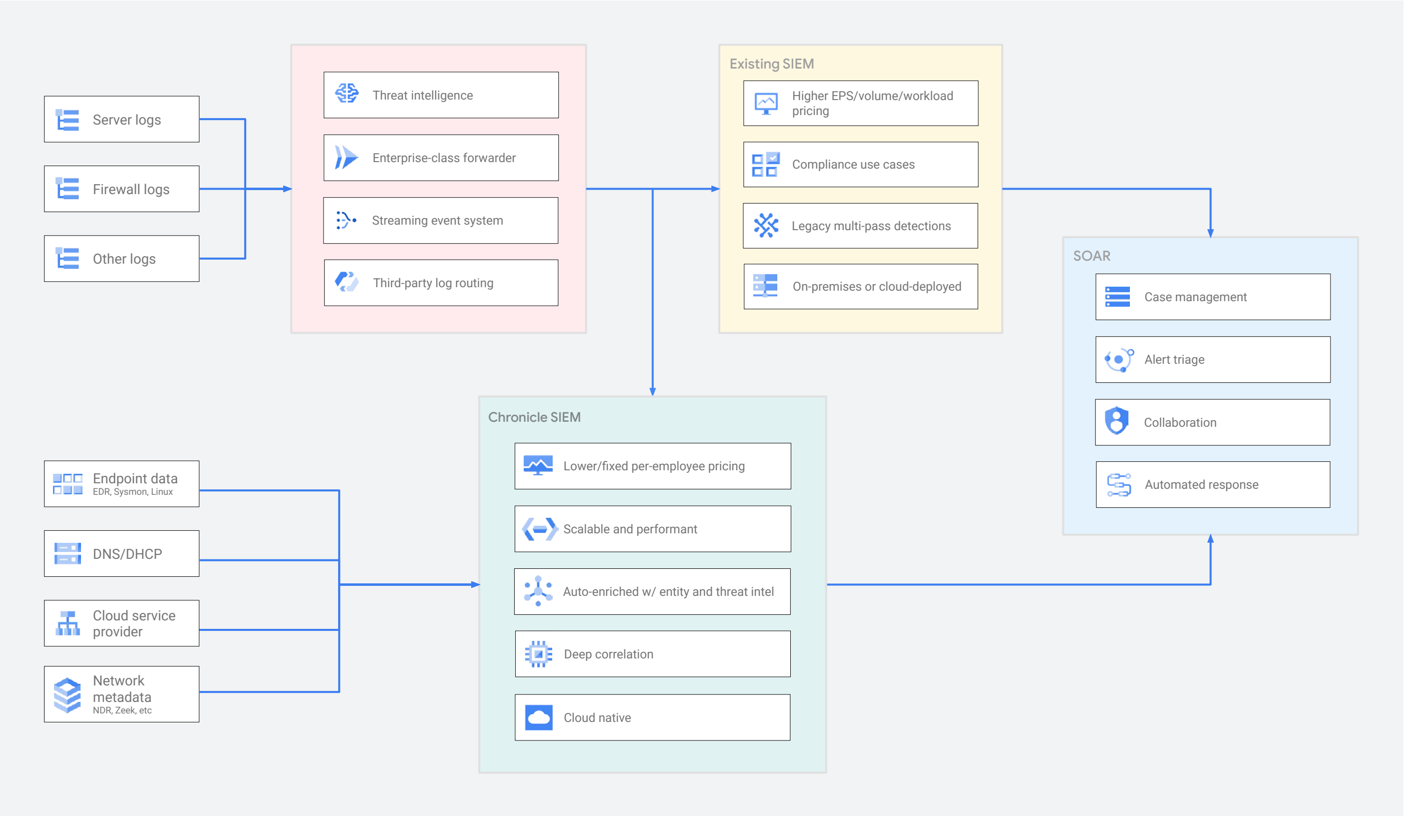


Figure 1

A complete SIEM and a focused SIEM

If Chronicle SIEM is utilized for detection and investigation as well as hunting while the traditional tool is used for compliance reporting, the situation is similar. Chronicle SIEM needs access to the entire data set while a subset may go to the legacy tool.

For some augmentation scenarios, Chronicle SIEM is used to analyze voluminous and demanding data sources while the other tool is used for more traditional SIEM data sources. In this case, it makes sense to split the collection into two tools. Naturally, that brings the challenge of access to the entirety of data. Deploying a security orchestration, automation, & response (SOAR) solution such as Chronicle SOAR that can make API calls to both SIEM tools is typically the answer here as shown in Figure 2.

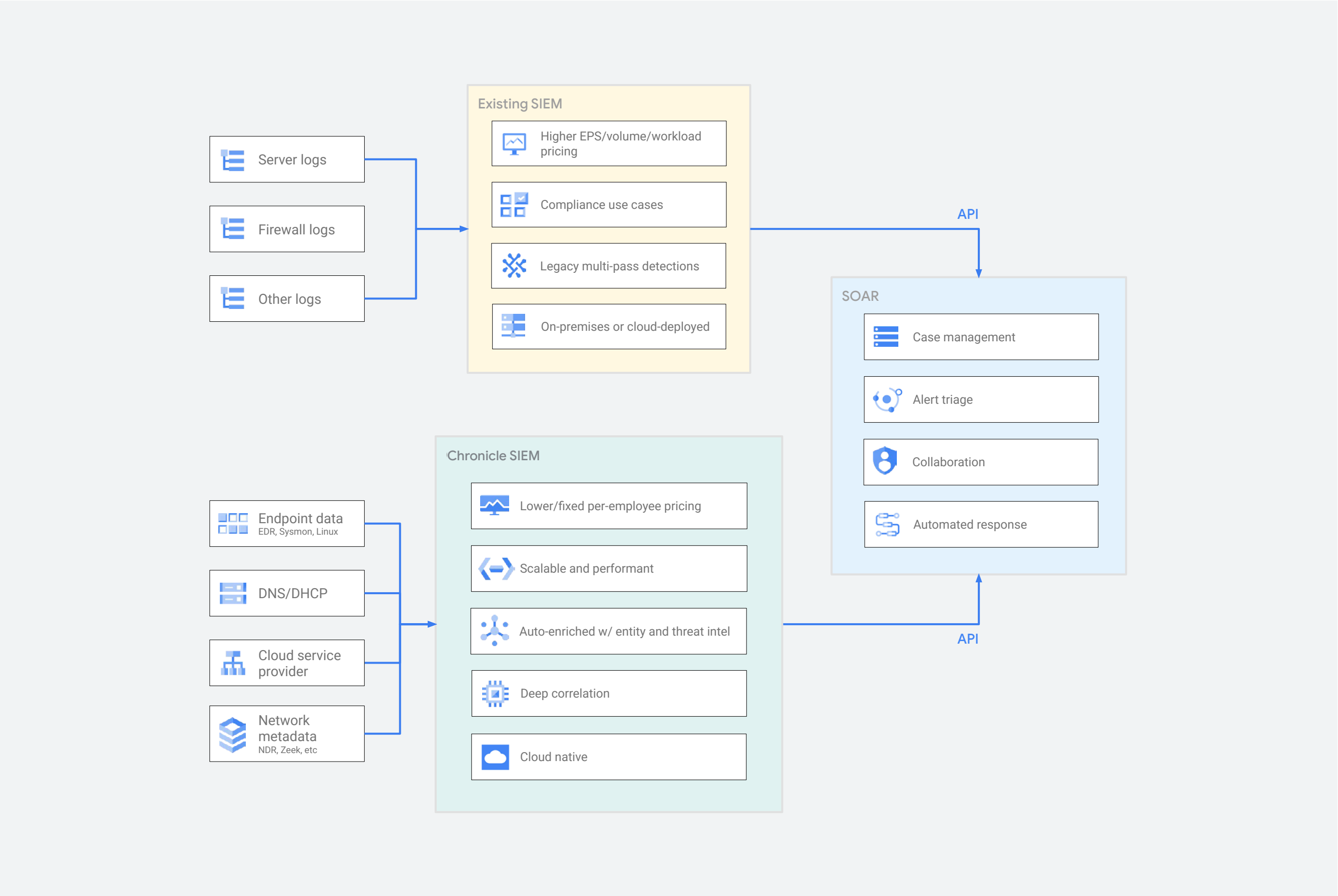


Figure 2

Send logs through one SIEM to another

SIEM passthrough is also an option. In this architecture, raw data and/or alerts collected in the existing tool are sent along to Chronicle SIEM as shown in Figure 3. This is a compelling design, however it comes with many caveats. Investment in log ingest infrastructure/configuration is preserved, as is existing detection content. While SIEMs generally are optimized to ingest and process data, they often perform poorly when exporting raw data at scale.

If the existing SIEM is deployed in a public cloud, exporting large amounts of raw data may result in unexpected data egress costs. In the face of these challenges, some customers may choose to only send alerts to Chronicle SIEM. The use of SOAR for case management, alert triage, collaboration, etc. is recommended in all scenarios. Some customers may decide against integrating SOAR with their legacy SIEM depending on their unique circumstances.

There are many other factors that influence SIEM augmentation architecture. For example defense industry customers may have significant requirements for segmentation of data, and are therefore willing to build and manage more complex topologies. Another factor to consider is data residency for global organizations. The architectures depicted in this section represent just a few examples, however many other permutations are possible. Naturally, this architecture choice has flaws due to the second SIEM getting the data via an intermediary, thus increasing the chance of data errors and missing data.

In summary, the above three augment architectures cover most situations where Chronicle SIEM augments the value for a customer by being used with another SIEM tool.

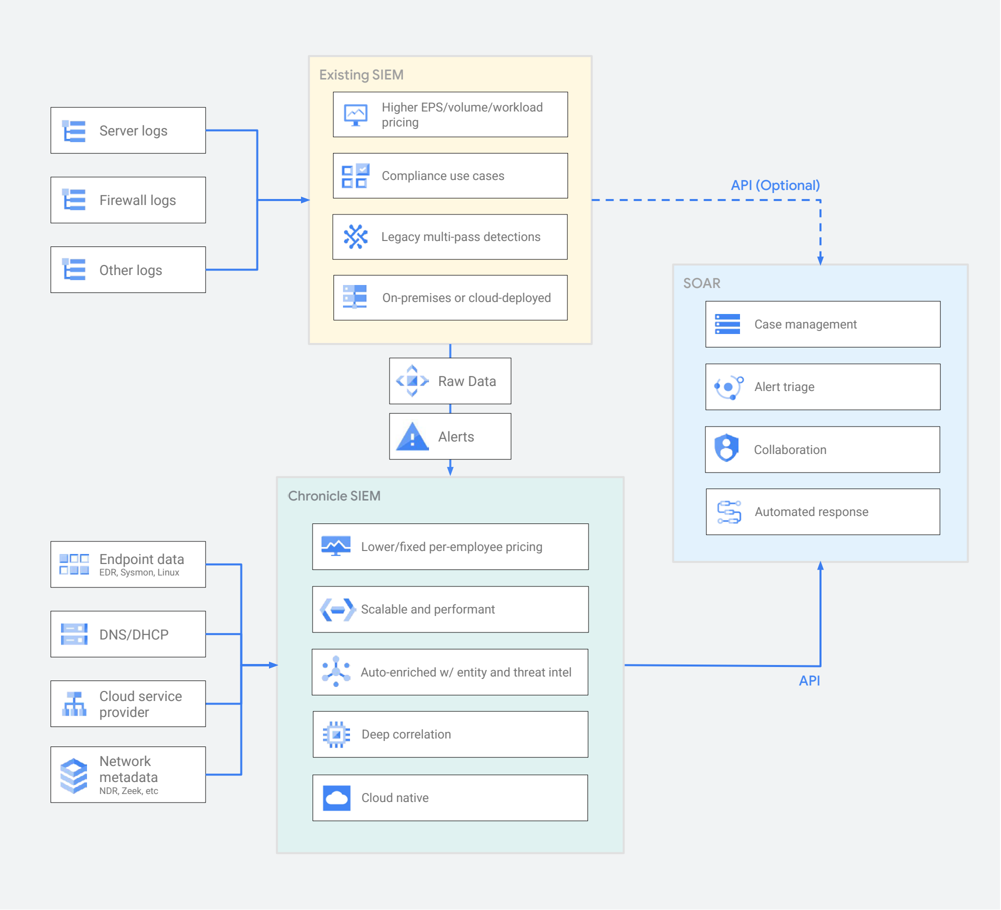


Figure 3

What to watch for

What are the critical pitfalls to watch for while deploying Chronicle SIEM in your SOC alongside another similar tool?

Data collection pitfalls may materialize. Some of the data sources do not support being sent to multiple destinations. In some cases sending logs to a different destination can cause increased cloud service provider egress costs. In this case, additional costs and complexity arise. All the situations when data access becomes more difficult when you're adding another tool are very possible.

To mitigate this, decide where the logs go based on the use cases and log routing capabilities. For some logs, one can use a third party tool to send the logs to two sources even if there is no native support for this.

Split data needed for one use case. While deploying the architecture of Chronicle SIEM and another tool, a challenge where data exists in multiple sources may arise. For example, while chasing a threat actor using threat hunting, it may turn out that a certain data set isn't available in Chronicle SIEM, but is located in another tool.

To mitigate this, use a SOAR that can query multiple SIEM tools (and perhaps even some context and enrichment sources directly) and thus unify the data needed for solving a problem.

Multiple workflows add complexity. As we pointed out, complexity is the main risk with scenarios involving multiple SIEM tools. To streamline the workflows involving multiple data repositories, the proverbial data lake house scenario, it is possible that yet another tool would be needed—typically an SOAR that can query multiple repositories

To mitigate this, a SOAR such as Chronicle SOAR is also a big part of the answer. By keeping the workflows in a SOAR, one can avoid the challenge of swivel chairs and multiple screens needed for the same task.

Detection content duplication. If both tools are used for threat detection, the question of detection content repository would come up. In the future, we can use multi-vendor detection languages such as sigma to plan detection across tools. For example, when Chronicle SIEM is used together with EDR, some detections are running inside the EDR vendor tool chain while others are around inside Chronicle SIEM. The risk of conflicting results may also arise based on the analysis approach or implementation.

There is no universal way to mitigate this, but a careful planning of what is the optimal detection chokepoint for each threat type add much needed sanity for this situation. For example, detecting cloud threats can be performed inside the native tool such as GCP Security Command Center while an EDR tool is used to detect traditional client and server threats. The SOAR is again used as a deconfliction layer for many detections.

Source of record. The presence of multiple detection tools can give rise to confusion about which system is the official source of record. A detection in one tool may not appear in the other, leading to confusion and wasting time. Compliance requirements may dictate that one system be considered the source of record for audit purposes. Still, the need to have “detection in depth” and cover the same threat scenarios with multiple controls may lead to keeping multiple detection approaches such as EDR, NDR and SIEM.

To mitigate this, lean toward the architecture where one of the SIEM tools does contain a complete copy of the data with all context, while another is used for specific use cases.

Google Cloud

Action plan

Short-term recommendations

- Review your detection and response practices and activities.
- Evaluate your detection and response tools and identify gaps and weaknesses in current detection use case coverage.
- Look for gaps in your detection use cases, especially gaps that exist due to inability to collect and retain telemetry data
- Look for data that is not being collected in support of security use cases especially due to costs and other challenges.

Medium-term recommendations

- Look for cloud detection scenarios that may not be addressed by existing tools.
- Review choices for a joint, augmented architecture to address the gaps identified.
- Evaluate the need for SOAR capability to address the use cases, especially if data would be spread over multiple repositories.
- Run proof of concept of Chronicle SIEM on your data.
- Review Autonomic Security Operations vision and blueprint.

In many augmentation scenarios, Chronicle SIEM exists alongside another tool. Evolution may lead to that tool being phased out while Chronicle SIEM takes on more and more responsibilities. For example, for some clients who started using Chronicle SIEM for incident investigation and hunting while using another tool for detection transition to using Chronicle SIEM for all the tasks while limiting the all tool to specific niche uses.

Thanks for reading!

For more information, visit chronicle.security

Google Cloud