



Detect, Hunt, Respond

We live in a digital world, but the current economics of storing and processing enterprise security data have made it not only expensive, but nearly impossible to compete against cyber crime. Organizations are looking to improve their ability to address potential cyber threats in a smarter, faster, and more cost-effective manner.

Chronicle is Google's cloud-based security telemetry platform capable of ingesting petabytes of data to quickly perform analytics and identify signals of threats at Google-speed through a predictable cost model based on number of users, not volume of data.

Deloitte's industry leading Cyber practice is collaborating with Chronicle to provide cloud native security analytics for organizations to identify threat signals across people, processes, and technology.

Why Chronicle



Threat actors are becoming more sophisticated. Cyber threats are growing in number and complexity through cloud, third-party providers, Internet of Things (IoT), and more.



Alerting is increasingly becoming coupled with proactive hunting. Modern threat detection requires proactive threat hunting in addition to security monitoring correlation & alerting, coupled with automation.

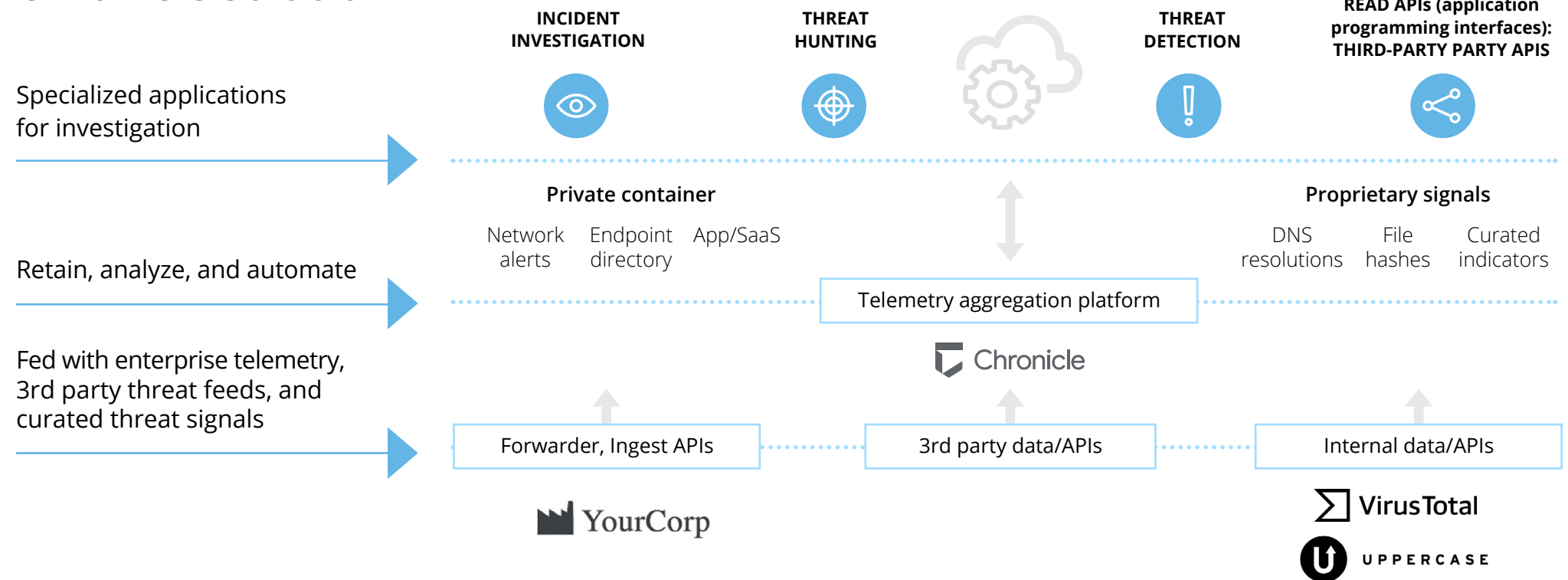


Shortage of cybersecurity talents and skill sets. Limited cyber talent may cause SOC (Security Operations Center) staff to often be overworked and undertrained for the challenges they face.



Constantly increasing data storage in a cost-effective manner. SOCs consume more and more data to detect threats but are expected to increase efficiencies and reduce costs such as storage.

Chronicle Solution



Multi-petabyte threat analytics platform

Applies planet-scale computing and analytics to secure client networks and their customers' data

Cloud-based

Chronicle operates on Google Cloud's scale and speed as its underlying security platform to facilitate security analytics

High volume detection, investigation, and hunting

Data model enables real-time asset and threat intelligence analytics for investigations coupled with YARA-L customized rule writing

Google-speed hunting and continuous threat evaluation

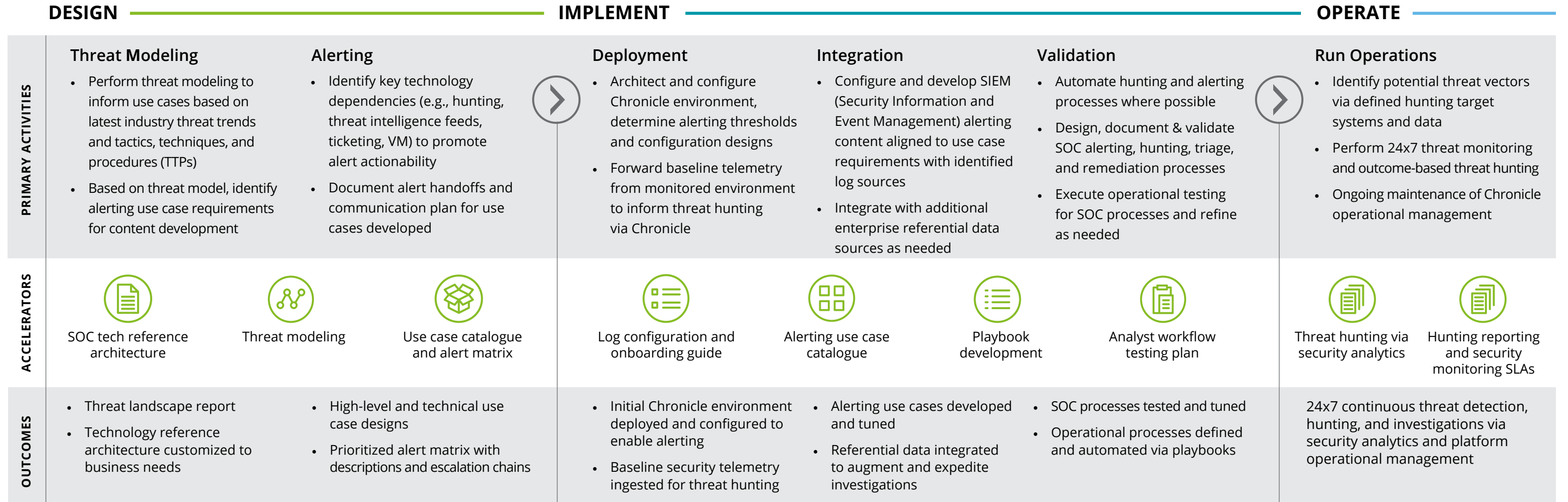
Real-time searches against petabytes of data with no proprietary search syntax coupled with automated, retroactive threat intelligence








A Google Cloud Specialization indicates the strongest signal of proficiency and experience with Google Cloud.

Our Approach to Chronicle Implementation

Deloitte brings technical and industry experience to guide clients on their journey to detect sophisticated threats in an efficient, analytically-driven, continuously improving model that spans across people, processes, and technology.



Deloitte and Chronicle Solution Benefits

- 
Business risk focused
 by bringing together business, technology, and security insights to rapidly identify cyber threats
- 
Instant intelligence
 by correlating indicators of compromise against 1+ years of security telemetry coupled with highly flexible syntax (YARA-L)
- 
Rapid investigations
 by improving quality and sophistication of SOC analysis via instant searching against petabytes of data
- 
Continuous improvement
 by evolving to a proactive intelligence lead integrated across operational groups
- 
Predictable cost with scalability
 for analyzing enterprise security telemetry with no penalty for additional devices via cloud-based solution

Start the conversation



Arun Perinkolam
Principal
Deloitte & Touche LLP
aperinkolam@deloitte.com



Christopher Trollo
Senior Manager
Deloitte Services LP
ctrollo@deloitte.com



Sachin Verma
Senior Manager
Deloitte & Touche LLP
sacverma@deloitte.com



Alexi Wiemer
Manager
Deloitte & Touche LLP
awiemer@deloitte.com

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see <http://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.