

# **Deloitte.**





### 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**

Specialized applications for investigation

Retain, analyze, and automate

Fed with enterprise telemetry, 3rd party threat feeds, and curated threat signals









### THREAT DETECTION

READ APIS (application programming interfaces): THIRD-PARTY PARTY APIS



indicators

#### Private container

Network Endpoint App/SaaS alerts directory

Forwarder, Ingest APIs

**YourCorp** 

Proprietary signals

DNS File Curated

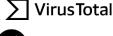
resolutions hashes

Telemetry aggregation platform



3rd party data/APIs

Internal data/APIs





# 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

### **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.

DESIGN — OPERATE

#### **Threat Modeling**

- Perform threat modeling to inform use cases based on latest industry threat trends and tactics, techniques, and procedures (TTPs)
- Based on threat model, identify alerting use case requirements for content development

#### Alerting

- Identify key technology dependencies (e.g., hunting, threat intelligence feeds, ticketing, VM) to promote alert actionability
- Document alert handoffs and communication plan for use cases developed

### Deployment

- Architect and configure
   Chronicle environment,
   determine alerting thresholds
   and configuration designs
- Forward baseline telemetry from monitored environment to inform threat hunting via Chronicle

#### Integration

- Configure and develop SIEM (Security Information and Event Management) alerting content aligned to use case requirements with identified log sources
- Integrate with additional enterprise referential data sources as needed

#### Validation

- Automate hunting and alerting processes where possible
- Design, document & validate SOC alerting, hunting, triage, and remediation processes
- Execute operational testing for SOC processes and refine as needed

#### **Run Operations**

- Identify potential threat vectors via defined hunting target systems and data
- Perform 24x7 threat monitoring and outcome-based threat hunting
- Ongoing maintenance of Chronicle operational management



SOC tech reference architecture



Threat modeling



Use case catalogue and alert matrix



Log configuration and onboarding guide



Alerting use case catalogue



Playbook development



Analyst workflow testing plan



Threat hunting via security analytics



Hunting reporting and security monitoring SLAs

24x7 continuous threat detection, hunting, and investigations via security analytics and platform operational management

- Threat landscape report
- Technology reference architecture customized to business needs
- High-level and technical use case designs
- Prioritized alert matrix with descriptions and escalation chains
- Initial Chronicle environment deployed and configured to enable alerting
- Baseline security telemetry ingested for threat hunting
- Alerting use cases developed and tuned
- Referential data integrated to augment and expedite investigations
- SOC processes tested and tuned
- Operational processes defined and automated via playbooks

### **Deloitte and Chronicle Solution Benefits**



PRIMARY

**ACCELERATORS** 

#### **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 subsid-iary 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.