

Chronicle Foundations







Transform Security Operations with Google Chronicle SIEM and SOAR



OVERVIEW

Google Chronicle is a game-changing security analytics platform that empowers organizations to fortify their security posture, streamline operations, and swiftly detect and respond to threats. Onix's Chronicle Foundations solution accelerates the design and deployment of Google Chronicle by implementing Chronicle best practices in 3-4 weeks using rules, configurations, alerts, and dashboards developed by Onix. By leveraging the power of Google's infrastructure and threat intelligence, along with this foundation solution, Chronicle offers unparalleled capabilities to protect your organization and secure your digital assets.

DELIVERABLES

- 
Document Business and Technical Requirements
 Our team assesses your current security environment (logs, SLAs, KPIs) to understand use cases and success criteria.
- 
Chronicle SIEM Data Ingestion (50 sources)
 Design, configure, and test ingestion environment (based on sources identified in the business requirements phase).
- 
Chronicle SIEM Threat Detection (50 rules)
 Design and build threat detection rules including top rules from Google to detect malware, ransomware, and Mitre attacks.
- 
Chronicle SIEM Alerting & Reporting (10 each)
 Setup and configure alerts and design and build reporting dashboards
- 
Chronicle SOAR Playbooks (10 Playbooks)
 Setup top 8 playbooks including brute force, phishing, ransomware, C&C traffic, and insider threats.
- 
Chronicle SIEM and SOAR Testing
 Test data ingestion, validate data integrity, test alerting, analyze dashboards, and test playbooks.

CUSTOMER VALUE

- Enhanced threat detection and response reducing MTTD and MTTR potentially saving millions of dollars in potential incident costs.
- Streamlined security operations with a unified platform that scales and provides automation to reduce toil.
- ingest and analyze 3x more security telemetry compared to other SIEMs without experiencing performance degradation.

BUSINESS OUTCOMES

- Accelerate business transformation and maximize threat coverage.
- Eliminate security blind spots and expand automation.
- Improve investigation and response to cloud-based threats.
- Reduce security costs.

