CyberProof®
A UST Company

Chronicle

AI-powered incident response by CyberProof and Google

Reduce Incident Response Time From Hours to Minutes

8 ways CyberProof's nation-state trained experts help you mitigate risk and improve the cyber readiness of your enterprise with Google Chronicle's AI-powered security solutions

Maximize the Return on Investment on your current cybersecurity tools by working with CyberProof and Google Chronicle. By leveraging Google Chronicle's AI-powered solutions, CyberProof helps organizations gain continuous threat visibility to detect, investigate, and respond to threats faster and more effectively. The following illustrates how Google Chronicle is leveraged by CyberProof's experts to help you improve cyber readiness and effectively mitigate the risks of existing, new and evolving threats.

Managed XDR for Google

- Supercharge Google Chronicle SOAR's capabilities with CyberProof's expert teams to effectively contextualize alerts, automate response actions, and proactively notify client stakeholders of their cyber posture - improving their cyber readiness.
- Seamlessly integrate your existing operational workflows - providing consistent communication to multiple teams operating as a true extension of your cyber defense function.
- Chronicle users leverage generative AI to interact with and drill down into their security events.
- Coordinate multiple teams and processes that include SLAs and KPIs for continuous service improvement.
- Mitigate business impact with faster Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR).
- Prioritize potential threats in line with the changing attack surface according to a risk-based prioritization process.

Tailored Threat Intelligence

- Quickly identify emerging threats and exposures; with Google Chronicle, curated detections integrate with leading threat intel sources for real-time malware insights.
- Access a single view of enriched threat intelligence alerts.
- Implement actionable information including strategic and technical mitigation advice.
- Generative AI can speed up the pace of investigations and provide security insights and trends by pulling together and analyzing data from events, behavior anomalies, and more.

Threat Hunting

- Utilize insights from CyberProof's threat intelligence to define hunting hypotheses based on Incidents of Attack (IOAs) that are associated with the threat landscape and emerging threats - augmenting data from intelligence sources such as Mandiant, VirusTotal, and other vendors with insights from our in-house team.
- Identify serious threats that may have slipped through the security perimeter by learning about relevant incidents, dark web activity, and MITRE ATT&CK techniques.
- Continuously improve advanced analytics, detection rules, and response actions.
- Build custom and proactive hunting processes incorporating data gleaned from threat intelligence research, incident reports, and behavioral analysis techniques.

Cloud Security Transformation

- Build a security stack native to the Google Cloud Platform - including SIEM, SOAR, and threat intelligence capabilities.
- Leverage Big Data, ensuring the right security logs are collected for analysis and correlation.
- Reduce the cost of ingesting and storing volumes of cloud data.
- Mitigate the risk of cloud security transformation to future-proof your enterprise security.

Generative AI Innovation

- Leverage GenAI to organize and enrich alert data, providing meaningful and actionable information for SOC analysts.
- Reduce analysts' workload by creating custom queries and scripts that aid in detailed investigations and incident analysis.
- Provide concise and comprehensive information about the threat landscape, including threat actor activities and campaigns, as well as trending vulnerabilities.
- Create content such as incident summary reports, an overview of threat actors and their backgrounds, and information on attack patterns - by means of integration with a GenAI toolset.
- Combine threat intelligence with AI-powered detection and analytics to develop threat analytics rules proactively and initiate containment actions before they impact your network.
- Analyze and explain malicious code behavior, predict attacker activities and risk scenarios, and suggest threat mitigation actions.

Use Case Management

- Implement threat profiling, understand your security controls, and map the attack surface, control gaps, and vulnerabilities with CyberProof's unique approach to Use Case Management.
- Leverage the power of YARA rules and the Unified Data Model in Google Chronicle's use cases to help you detect, investigate, and respond to cyber threats with unprecedented speed and accuracy.
- Improve the targeting of responses; CyberProof's use case framework leverages Agile methodology to provide continuous improvement by minimizing gaps between threat detection and response capability.

Vulnerability Management

- Identify, assess, and mitigate security vulnerabilities through continuous scanning; meet reporting and regulatory requirements.
- Prioritize vulnerabilities based on real-world context: threat intelligence, risk prioritization, live threat feeds, real-time cloud posture management, and more.
- Approach vulnerability management as a process including patching, compensating controls, segmentation, segregation, and heightened diligence in security monitoring.
- Sharpen your vulnerability management capabilities with Google Cloud's ever-accessible data storage architecture.

Augment Your Security

- Bring in the skills your security team is missing; access hard-to-find expertise and experience with detection and response, threat hunting, digital forensics, incident response, and more.
- Adopt the flexible engagement model offered by CyberProof and Google; scale up or scale down as necessary.
- Maintain full control over all of your cybersecurity operations.
- Orchestrate the hundreds of the tools that you rely on to respond to potential incidents in minutes, not hours or days - through Google's automation capabilities.

Security Platform Management

- Provide custom, flexible parser development based on LogStash.
- Relieve the pressure on your team while maintaining in-house control.
- Maximize efficiency through integration of your Google Cloud and Google security solutions – or work with Google Chronicle with your existing stack.
- Maintain one source of truth for all threats and vulnerabilities; data science is central to Google Chronicle's security platform, enabling it to detect and respond to threats more quickly and effectively.
- Maintain faster, more effective operations that scale.
- Combine pro-active SecOps services like Attack Surface Management (ASM), Cloud Security Posture Management (CSPM), controls validation, and reactive detection and response through Google Chronicle.