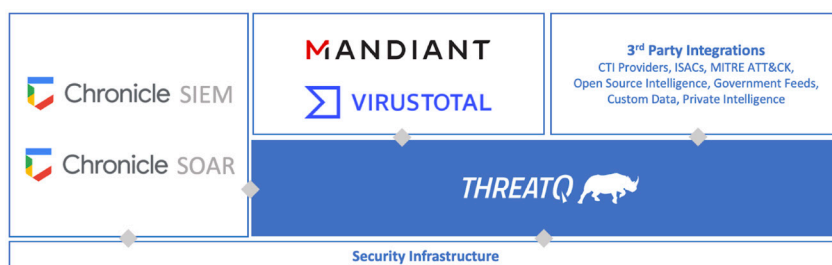


THREATQ™ AND GOOGLE CLOUD SECURITY

MAKING THREAT INTELLIGENCE ACTIONABLE AND MAXIMIZING ROI

Together, ThreatQuotient and Google Cloud Security solutions offer a comprehensive approach to leveraging and utilizing threat data. This combination improves the efficiency and effectiveness of security operations with actionable threat intelligence.



THREATQ BY THREATQUOTIENT™

ThreatQuotient's solutions make security operations more efficient and effective. The ThreatQ data-driven security operations platform is both open and extensible, supporting the integration of disparate threat intelligence and security technologies into a single security infrastructure, automating actions and workflows so that tools and people can work in unison. Empowered with continuous prioritization based on their organization's unique risk profile, security teams can focus resources on the most relevant threats, and collaboratively investigate and respond with the aim of taking the right actions faster.

GOOGLE CLOUD SECURITY INTEGRATIONS

Chronicle SIEM

Chronicle SIEM (Security Information and Event Management) delivers modern threat detection and investigation at unprecedented speed and scale, at a predictable price point. Chronicle SIEM features cloud-scale security analytics, context rich investigation, lightning speed search, and an advanced detection engine.

Chronicle SOAR

Chronicle SOAR (Security Orchestration, Automation and Response) enables modern, fast and effective response to cyber threats by combining playbook automation, case management, integrated threat intelligence, and collaboration in one cloud-native, intuitive experience.

Mandiant

Mandiant Threat Intelligence gives security practitioners unparalleled visibility and expertise into threats that matter to their business right now. Mandiant threat intelligence is compiled by over 380 security and intelligence professionals across 29 countries, and collected directly from the frontlines spending over 200k hours per year responding to attacks. All to help organizations of all sizes to be more proactive and understand the adversary and their tactics, techniques and procedures. So, organizations can be more proactive in setting and adjusting their security strategy.

VirusTotal

VirusTotal is the richest and most actionable crowdsourced threat intelligence suite on the planet. With over 70 antivirus scanners, URL/domain blocklisting services and a myriad of tools to extract signals from indicators, it equips security teams with comprehensive context and a cutting edge investigative workbench to proactively protect their networks from cybersecurity threats.

INTEGRATION HIGHLIGHTS

Combine Google Cloud Security intelligence with private threat data and context, making it more relevant and actionable to an organization

Accelerate deployment and integration of Google Cloud Security products within the organization through the use of the ThreatQ integration marketplace

Make threat intelligence contextual, tailored and actionable to specific security missions

Provide user-configurable intelligence scoring to eliminate noise at the integration level

Offer visibility beyond the typical attack lifecycle, adding context and priority to global threats with MITRE ATT&CK

Improve ability to prioritize and remediate security alerts, and patch security vulnerabilities

Deliver granular reports to help align security programs and resources against your most likely threats and actors

Helps security teams respond efficiently when investigating a threat

Make Threat Intelligence Actionable across other tools in the environment

INTEGRATION USE CASES:

Detection Triage and Investigation Enablement

Receive detection events to alert analysts of threats directly affecting your infrastructure, allowing them to conduct investigations, identify a threat actor, and discover mitigation tactics.

Incident Validation and Prioritization

Determine which incidents are likely to pose a risk to the enterprise and prioritize those with the highest potential for negative impact on the business.

Incident Analysis

Answer questions about the who, what, why, when and how of attacks. Determine if attacks are still in progress and identify their effects.

Containment and Remediation

Disrupt attacker communications. Remove malware and reverse changes. Eliminate vulnerabilities.

Hunt Missions

Uncover previously undiscovered attacks related to current incidents or to threats targeting the enterprise's industry, geographical locations, applications, etc.

Dissemination of Prioritized Threat Intelligence

Prioritize and disseminate high confidence indicators to your SIEM for higher fidelity detections and alerts.

Threat Intelligence Sharing - Global Distribution Network

Share intelligence from Mandiant and other CTI providers, open source intel, government feeds, Mitre ATT&CK, and analysts input across a distribution network to companies across the globe.

ABOUT THREATQUOTIENT™

ThreatQuotient improves security operations by fusing together disparate data sources, tools and teams to accelerate threat detection and response. ThreatQuotient's data-driven security operations platform helps teams prioritize, automate and collaborate on security incidents; enables more focused decision making; and maximizes limited resources by integrating existing processes and technologies into a unified workspace. The result is reduced noise, clear priority threats, and the ability to automate processes with high fidelity data. ThreatQuotient's industry leading data management, orchestration and automation capabilities support multiple use cases including incident response, threat hunting, spear phishing, alert triage, vulnerability prioritization and threat intelligence management. ThreatQuotient is headquartered in Northern Virginia with international operations based out of Europe and APAC. For more information, visit www.threatquotient.com.

ABOUT GOOGLE CLOUD

Google Cloud accelerates every organization's ability to digitally transform its business. We deliver enterprise-grade solutions that leverage Google's cutting-edge technology – all on the cleanest cloud in the industry. Customers in more than 200 countries and territories turn to Google Cloud as their trusted partner to enable growth and solve their most critical business problems.