crest(data)

CASE STUDY

SECURITY OPERATIONS · GOOGLE SECOPS SOAR

Leveraging Exposure Management Data Through Integration with Google SecOps SOAR

175+	5,500+	60%	1,000+
Global customers served	Projects delivered	Typical cost savings delivered	Talented professionals

Executive Summary

THE OPPORTUNITY

The customer wanted to consolidate its security posture by making **Continuous Exposure Management (CEM) data** genuinely useful — streamlining threat detection, investigation, and response. Their analysts lacked full context and visibility into asset relationships and attack paths, response was slowed by manual remediation steps, and integration friction appeared whenever teams tried to use that data within Google SecOps SOAR.

This case study describes how **Crest Data built a comprehensive integration between the customer's CEM platform and Google SecOps SOAR** — bringing attack-path data and exposure insights directly into security operations workflows. It sharpens threat detection, adds deeper incident context, and drives more effective remediation through automated workflows, advanced entity enrichment, risk scoring, and breach-point management.

About the Customer

The customer is one of the **fastest-growing cybersecurity firms in the world**, specializing in continuous exposure management and helping enterprises see and close the gaps attackers exploit.

They deliver transformative capabilities including **External Attack Surface Management, Exposed Credentials Management, and security controls management** — and much more across the exposure lifecycle.

CUSTOMER PROFILE

INDUSTRY
Cybersecurity — Continuous Exposure Management

PROFILE
One of the fastest-growing security firms globally

CORE PLATFORM
CEM — attack paths & exposure insights

CRITICAL NEED
Faster, context-rich detection & response

The Customer Challenge

CONTEXT & WORKFLOW GAPS

The customer faced critical problems that significantly hampered their ability to **strategically manage security threats** — limiting how effectively their analysts could detect, prioritize, and respond to exposures.

Limited context. Analysts lacked comprehensive visibility into asset relationships and attack paths during investigations.

Manual workflows. Remediation actions required manual intervention across multiple platforms.

Prioritization difficulties. Without proper context, teams struggled to rank which vulnerabilities and exposures posed the greatest risk.

Platform dependencies. Teams on non-Google SIEMs hit integration friction when trying to leverage exposure data in Google SecOps SOAR.

> Organizations needed a way to bring the customer's **attack-path data and asset information directly into Google SecOps SOAR** — enhancing detection, investigation, and response regardless of the underlying SIEM platform.

The Proposed Solution

INTEGRATION CAPABILITIES

Crest Data delivered a **seamless connection between the customer's CEM platform and Google SecOps SOAR**, letting security teams act on attack-path data and exposure insights right inside their operations workflows.

Data Enrichment

Retrieves detailed information for each identified entity — **critical scores, risk factors, and attributes**.

Risk Calculation

Weighted scoring determines overall risk in the customer's context, with customizable weights for **nine risk factors**.

Breach Point Management

Flags entities in alerts as potential breach points, with sophisticated filtering across **20+ parameters**.

Automated Playbooks

Ready-to-use playbooks extract entity data from alerts and **intelligently filter** by the risk-scoring algorithm.

Visualization Widgets

Six specialized widgets turn complex exposure data into intuitive, actionable security insight.

Universal SIEM Compatibility

Consistent enrichment across **Google SecOps SIEM and third-party SIEMs** alike.

The solution can be easily migrated to the Content Pack once it reaches general availability.

The Crest Difference

BEYOND BASIC CONNECTIVITY

Strategic Solution Design

We don't just connect APIs — we **architect intelligent security workflows**. Purpose-built visualization widgets, cross-platform enrichment, and comprehensive SOAR playbooks deliver true operational value well beyond basic connectivity.

Deep Google SecOps Expertise

A profound understanding of **how security teams actually use these platforms** ensures the integrations we build are not just technically sound, but intuitively useful and highly effective in real-world operations.

Any
SIEM, one layer

SIEM-AGNOSTIC BY DESIGN

Consistent exposure enrichment, whatever the SIEM

Attack-path context and risk scoring flow into Google SecOps SOAR whether the team runs Google SecOps SIEM or a third-party platform — no rip-and-replace required.

About Crest Data

AI-FIRST · SECURITY-LED

Crest Data is a data and AI-first product engineering and technology solutions provider with deep expertise across cloud and AI, cybersecurity, observability, data analytics, and workflow automation. With **1,000+ experts** and a track record of **5,500+ successful projects across 175+ global customers** — backed by partnerships with AWS, Google, Microsoft, Datadog, Dynatrace, ServiceNow, and NetApp — Crest Data delivers outcome-focused solutions that strengthen security, improve platform reliability, and enable sustainable digital growth.

PUT YOUR EXPOSURE DATA TO WORK

Turn exposure insights into automated SOAR response.

Talk to Crest Data's Google SecOps experts about cross-platform enrichment, risk scoring, and ready-to-use playbooks tuned to your security operations.

Talk to Our Experts →

www.crestdata.ai/contact

SCAN TO EXPLORE

crest(data)

USA · CA
3031 Tisch Way #602
San Jose, CA 95128

INDIA · AHMEDABAD
CDS House, SG Road
Makarba, Ahmedabad 382210

INDIA · PUNE
Amar Madhuban Tech Park
Baner, Pune, MH 411045

+1 (408) 551-0051 info@crestdata.ai www.crestdata.ai