REPLICA PARTNER PROFILE

Secure Environments for Autonomous Security Operations

Safely Automating High-Risk Steps in SecOps

How Torq Powers the AI SOC

Torq is the enterprise AI SOC platform transforming how organizations triage, investigate, prioritize, and respond to threats. Built as an AI-native platform (not bolted on AI), Torq AI Agents plan, reason, and take action across the complete threat management lifecycle.

Security teams use Torq to ingest and normalize security events spanning across SIEM, EDR, identity, cloud, and collaboration tools, filtering out noise to prioritize actual threats. The platform connects to what teams already have to automate the full alert lifecycle, from enrichment and triage through investigation and response. Teams deliver faster results while keeping agentic transparency and control, without increasing risk by running high-stakes steps on production networks.

Torq turns fragmented security tooling into a unified, AI-driven operations layer. Its autonomous SecOps model reduces response times, standardizes workflows, and shifts analysts from repetitive execution into the judgment and decision-making roles where human expertise matters most. Teams set the terms: dial autonomy up for high-confidence, low-severity alerts; keep humans in the loop for critical incidents — calibrated to severity, confidence, and business context.

The combination of AI-native orchestration and adjustable control makes Torq a natural fit with Replica: Torq orchestrates the full workflow with explainable AI reasoning, and Replica provides the isolated, policy-enforced environments where the riskiest investigative steps can safely happen.

Industry

Security Operations Automation

Value Delivered

- **Reduced Risk & Exposure**
  Keeps high-risk SecOps activity isolated from production systems and data, while Torq's explainable AI reasoning gives teams full visibility into why each action was taken.
- **Accelerated Incident Response**
  Torq automates triage, enrichment, and case management across the full alert lifecycle, with Replica providing ready-to-go secure workspaces when investigations require isolation.
- **Enabled Autonomous SecOps**
  Torq's agentic AI handles the execution layer end-to-end. Replica ensures the riskiest steps happen safely. Together, they deliver repeatable, autonomous operations with human oversight where it matters.

Use Cases: Automated, Isolated SecOps

Phishing and identity investigations

For phishing, account takeover, and access-abuse cases, Torq can automatically collect context from email gateways, identity platforms, and EDR tools, then open or update a case.

As soon as deeper investigation is needed, the workflow can route the analyst into a Replica environment tailored for phishing and identity analysis, preloaded with the right tools and policies.

Analysts safely open links, inspect payloads, and validate remediation paths without touching their primary devices or corporate networks, while Torq tracks progress and triggers downstream actions.

Malware, hunting, and high-risk cloud reviews

In malware and threat-hunting workflows, Torq orchestrates the detection, enrichment, and initial classification of events, then hands off to Replica for the most sensitive investigative work.

Analysts detonate samples, pivot through suspicious infrastructure, or review risky cloud assets inside Replica environments with managed attribution and strict controls.

Torq closes the loop by capturing findings, updating the case, and driving remediation across EDR, firewalls, IAM, and ticketing systems. The result is a closed, automated loop from alert to response, with isolation built in at every high-risk step.

> *Torq shows what's possible when AI-driven SecOps meets a secure environment platform built for high-risk work. Joint customers get the speed of automation and the assurance of isolation in the same motion.*

Kris Schroeder
Co-founder & CEO
Replica Cyber

Results

- Torq playbooks auto-launch Replica labs, standardizing isolated investigations by default.
- Tier-1 phishing and malware handled end-to-end, never touching production systems.
- SecOps engineers ship new automations safely, without new VDI or networking projects.

Scaling High-Risk Work Together

Over time, Torq and Replica can make the handoff from automation to secure execution almost invisible to analysts. On the near-term roadmap, we're exploring direct "Open in Replica" actions from Torq alerts and cases, so a file or link can be investigated in an isolated workspace with a single click. We're also working with Torq's Socrates AI agent to automatically create Replica environments preloaded with the right tools and threat context for each case.

The goal is simple: every high-risk task should land in the right secure workspace without extra clicks or custom projects.

Torq is the enterprise AI SOC platform transforming how enterprises manage risk. Using adaptive agentic reasoning and automation, Torq identifies, prioritizes, and remediates critical threats at machine speed, slashing MTTI and MTTR while amplifying productivity. Global leaders like PepsiCo, Procter & Gamble, Siemens, Telefónica, and Virgin Atlantic trust Torq to power the next generation of AI-driven security operations.
For more information, visit torq.io.

Replica helps teams execute high-risk work without expanding their attack surface. Founded by counterintelligence experts, trusted by Fortune 100 institutions, and backed by 20+ patents, Replica delivers secure, isolated environments for investigations, threat operations, and sensitive initiatives—behind an anonymized surface with full observability and control.
Learn more at replicacyber.com.