Trellix

DATA SHEET

Root Cause Analysis (RCA)

Understand the Why. Fix the Root. Secure the Future.

Benefits

- Reduces likelihood of repeat incidents
- Strengthens control effectiveness and monitoring
- Improves cybersecurity maturity
- Enables evidence-based decision making
- Ensures regulatory and audit alignment

Key Deliverables

- Incident Timeline Reconstruction
- Root Cause Identification Report
- Contributing Factors Analysis
- Technical Analysis Artifacts (logs, forensics, malware, IOCs)
- Remediation Recommendations (short- and long-term)
- Stakeholder Briefing & Executive Summary
- Lessons Learned Workshop

Outcome

- Discovery of the true origin of the incident
- Documentation of control failures and risk exposure
- Prioritized recommendations to prevent recurrence
- Readiness for regulator, insurer, or board-level scrutiny

Overview

Trellix Guardians' Root Cause Analysis (RCA) service helps organizations understand *_why_* a cybersecurity incident occurred, beyond simply *_what_* happened. By examining the technical, procedural, and organizational causes behind an incident, we deliver insights that empower clients to eliminate vulnerabilities at their source.

This service is ideal for clients who have experienced a breach, outage, or security failure and need a structured investigation to identify causes, contributing factors, and actionable improvements.

Whether triggered by a ransomware event, insider breach, or unknown compromise, Guardians RCA service provides clarity and assurance that the root cause has been addressed, enabling clients to recover stronger, smarter, and more secure.

When Should You Consider a Root Cause Analysis?

- After a confirmed cyber incident (e.g., ransomware, data breach)
- If a prior compromise assessment or IR uncovered threats
- When regulators, auditors, or insurers request formal RCA
- To understand why a major outage or system(s) failure occurred
- As part of the post-incident "lessons learned" process

Our Methodology

Our methodology is structured to uncover the root cause of a cybersecurity incident through evidence-driven analysis, timeline reconstruction, and causal investigation. We collect and preserve digital artifacts, map the incident against known threat behaviors, and identify the underlying technical and organizational failures.

Copyright © 2025 Musarubra US LLC

Optional Add-On Services

- **Compromise Assessment**
  Identify signs of advanced threats or lateral movement beyond the immediate incident scope
- **Incident Response Retainer**
  Access rapid containment and investigation services with priority SLAs
- **Threat Hunting Engagement**
  Proactive hunt for hidden threats based on intelligence and hypotheses
- **Post-Incident Red Team Exercise**
  Validate the effectiveness of remediation and test detection capabilities
- **Security Architecture Review**
  Assess network, endpoint, and cloud infrastructure design and security controls
- **MDR (Managed Detection and Response) Integration**
  Add 24/7 monitoring, triage, and threat detection to your environment
- **Compliance and Regulatory Support**
  Assistance aligning recommendations with industry frameworks and regulatory expectations (e.g., GDPR, PCI DSS etc.)

The process concludes with tailored remediation guidance and collaborative debrief to drive continuous improvement and long-term resilience. Below is the flow of our methodology:

Scoping and Engagement Initiation

- Define affected systems, timeline, business impact, and objectives

Evidence Collection and Preservation

- Acquire logs, endpoint telemetry, network artifacts, and forensic images

Incident Timeline and Kill Chain Mapping

- Reconstruct attacker actions using tools like Trellix, proprietary tools etc., and map to MITRE ATT&CK and NIST 800-61

Root Cause Identification

- Apply structured analysis techniques such as the 5 Whys and Fault Tree Analysis to isolate causal factors

Contributing Factor Analysis

- Assess weaknesses across technology, people, and process that enabled the incident to progress

Remediation and Control Improvement Plan

- Provide tactical and strategic guidance to mitigate root causes and prevent similar events

Reporting and Executive Debrief

- Deliver a formal RCA report and conduct a lesson learned session for leadership and stakeholders

For more information or to schedule a consultation, please contact us at Guardians@Trellix.com

Copyright © 2025 Musarubra US LLC