Trellix

DATA SHEET

Comprise Assessment

Protect Defend Respond

Key Deliverables

- **Compromise Detection Report**: Comprehensive analysis of security threats found within your environment.
- **Incident Timeline & Forensics Summary**: Timeline of suspicious activities and forensic insights.
- **Remediation Roadmap**: Actionable steps to mitigate identified risks and improve security defenses.
- **Executive Summary Presentation**: High-level overview of findings and strategic recommendations.
- **Post-Assessment Support**: Advisory services for implementing security enhancements.

A Cybersecurity Compromise Assessment is a proactive investigation designed to detect hidden threats, active breaches, and vulnerabilities in your organization's IT environment. This assessment provides critical insights to identify unauthorized access, malware infections, and other security threats before they cause significant damage.

When do you need a Compromise Assessment?

A Compromise Assessment is essential if your organization suspects a security breach or unauthorized access, experiences unusual network activity or data anomalies, or has recently been targeted by a phishing attack or ransomware event. It is also crucial when verifying the effectiveness of security controls, preparing for an audit or regulatory compliance assessment, or operating in a high-risk industry such as finance, healthcare, government, or retail, where cyber threats are prevalent.

Methodology

Our Trellix Guardians Team follows a structured approach to identify and mitigate threats affectively:

- Pre-Engagement Consultation
- Threat Intelligence Analysis
- Network & Endpoint Forensics
- Malware and Advanced Persistent Threat (APT) Detection
- Data Integrity & Exfiltration Analysis
- Findings & Recommendations Report

Contact our Guardians team for further information at: Guardians@Trellix.com