FORTINET

SOLUTION BRIEF

FortiGuard Compromise Assessment Service

Executive Summary

In reading today's headlines, we often learn that attacks have been underway in companies for years at a time without being detected. It might seem inconceivable, but without comprehensive visibility and the necessary staffing to monitor and comprehend alerts, attackers can easily fly under the radar. When this happens, they can lie dormant, waiting for the opportunity to escalate privileges, move laterally, and take their actions on objectives—all while "blending in" in an attempt to look like typical network traffic. IT and security teams may not have the resources or skills to conduct regular threat hunting to ensure something hasn't been missed and determine if the network is breached.

Enterprises often turn to outside help to answer the question, "Have we been breached?" They look to security professionals with deep experience and an adept eye for handling threats and active incidents. The FortiGuard Incident Response (IR) team conducts compromise assessments to do just that: threat hunt, gather, stack, and analyze data, and conduct deep forensics analysis to answer this question. The assessment can alleviate enterprise concerns, and the IR team will recommend prioritized, swift actions if a breach is found.

> "With many things shifting in the environment, it's easy to make a mistake. And you can get 'configuration drift'—your settings were good, but three days later so much has happened, and something has changed in the IT environment."[1]

Have You Been Breached but Don't Know It Yet?

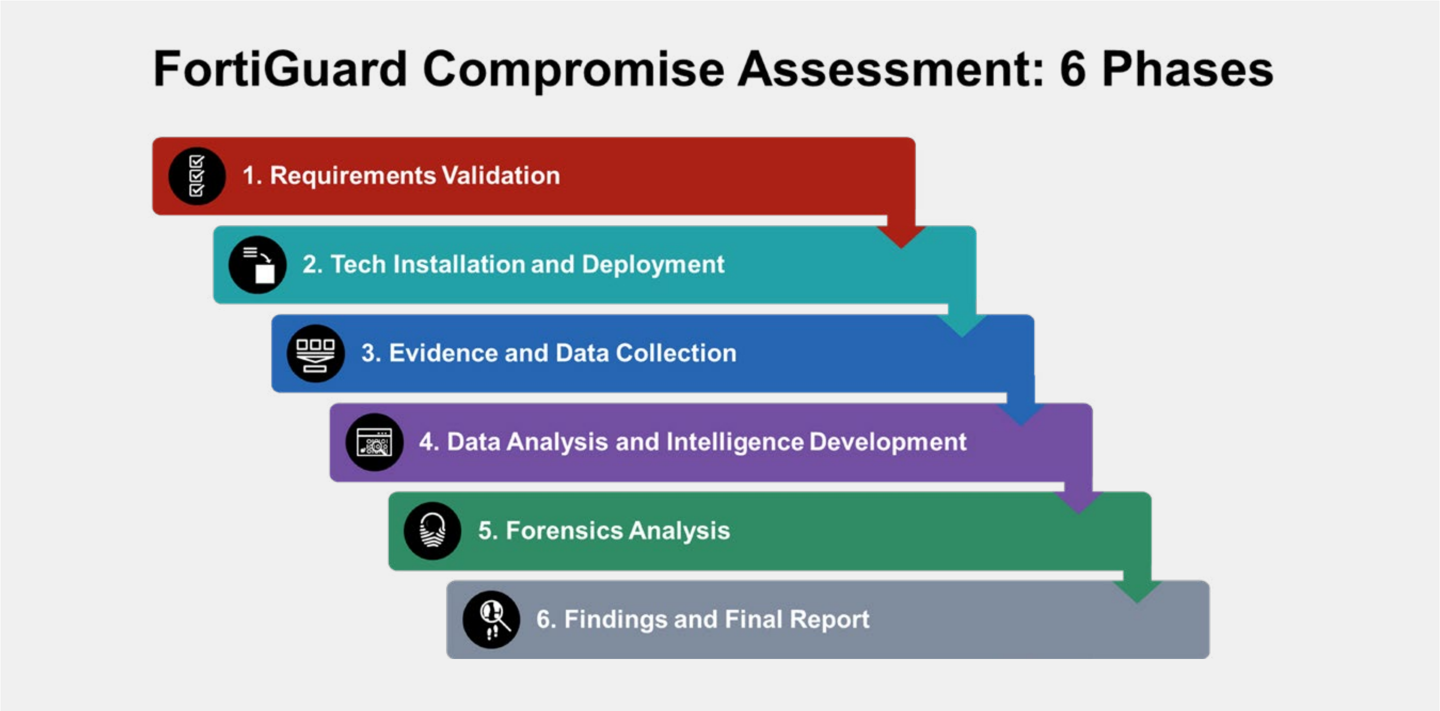
Enterprise growth, the adoption of new technologies and services (cloud, mobile, and others), the addition of partners, and new operating paradigms mean constant and substantive change. Add to that the evolution of attacker techniques to leverage legitimate business applications—hiding their tracks among authorized network traffic—and it's more challenging than ever to identify threats. Without skilled staff to recognize and act on that anomalous behavior at any time, 24×7, or to threat hunt to identify historical network breaches, it can be difficult to catch threat actor behavior.

Determine if You've Already Been Breached

The FortiGuard Compromise Assessment provides a way for enterprise teams to answer the question, "Have I been breached?" Using a six-phase process that culminates in a comprehensive report of all findings and recommendations, the assessment helps your team know if, when, and how an attack happened and what to do about it.

The six assessment phases enable inputs from the customer to define the goals and guide the inquiry for researching historical and live data to kick off the threat hunting. Throughout the process, the FortiGuard IR team delivers a weekly status update that contains the following:

- Summary of activities completed
- Deployment status of tools
- Issues requiring attention and plans for the next reporting period
- Key findings


FortiGuard Compromise Assessment: 6 Phases
1. Requirements Validation
2. Tech Installation and Deployment
3. Evidence and Data Collection
4. Data Analysis and Intelligence Development
5. Forensics Analysis
6. Findings and Final Report

Deep-Dive Data Collection, Analysis, and Forensics

The three key collection and analysis phases that result in the IR team extracting indicators of compromise (IOCs) and building a detailed attack timeline include:

Real-Time and Historical Data Collection

Using a centralized database or data lake, live and historical data is collected from different platforms, including:

- Endpoint data
- Network data
- Cloud data
- Security controls data
- External attack surface and adversary-centric data

The data lake indexes, processes, and correlates all the collected data. Using inputs from the organization's data—such as that from any SIEM solution or logs and other tool outputs, in addition to incoming data from the deployment of FortiGuard tools—the data lake extends telemetry and visibility across endpoint, network, cloud, and security controls, essentially creating an extended detection and response (XDR) solution.

The IR team collects and analyzes data in transit, including any behavior or evidence in memory, disk, or network. The IR team can then track back suspicious events on both network and endpoints to help identify "patient zero" and how malware may have spread across the network.

Data Analysis and Intelligence Development

During this phase, the IR experts "stack" the data, filtering and extracting only data of interest that may lead to suspicious behavior or abnormal activity. This helps threat hunters look for behaviors of compromise (BOC). Once hunting begins, each BOC is reviewed carefully with both manual and intelligence-driven analysis to prove its positivity.

Using threat intelligence from FortiGuard Labs Threat Intelligence Services, the IR team also performs BOC lookup in this phase. Each behavior contains a single IOC that can be used during the search operation. If something useful is found, the IR team proceeds to the next phase, which is deep-dive forensics. Otherwise, manual analysis of the behaviors continues to determine the outcome.

Deep-Dive Forensics

In this final research and analysis phase, the IR team can start to create a picture of what is and was happening and where in the environment through deeper forensics analysis. In this phase, the IR team focuses on forensics of all relevant, suspicious data from which they extract related IOCs. If an attack exists, this phase may involve advanced investigation to extract IOCs and build an attack timeline. It can include any or all the following:

- Malware forensics
- Memory forensics
- Network forensics
- Windows forensics
- MacOS and Linux forensics

It takes organizations 128 days on average to detect a breach—a delay that can be extremely damaging and costly.[2]

Your Final Compromise Assessment Report

To conclude the investigation, the IR team aggregates the results of their analysis to develop a final report. The report details the security incident findings, if applicable, and provides recommended remediation actions and recommended technical support.

A typical compromise assessment report contains the following components:

- Executive Summary
  - High-level narrative that explains the work performed, what was assessed, what was found, and what it means to the business
- Deployment Summary
  - Summary of the number of sensors, agents, and solutions deployed, duration of traffic monitored, and the scope
- Detailed List of All Findings
  - Detailed description of identified malicious activity, compromised infrastructure, at-risk data, and general observations
- Remediation Recommendations
  - Actionable recommendations to increase your security posture*

*These recommendations are provided in addition to any automated remediation performed by the FortiGuard IR team and related tools throughout the assessment.

Assessment Outcomes, Benefits, and Value

The FortiGuard Compromise Assessment provides organizations with a clear and decisive answer to the question, “Are we breached?” It provides all the information needed in case there is a compromise so that an organization understands the extent of the situation, any immediate action required, and threats to the enterprise’s data or business operations. This deep-level investigation can help augment your team’s capabilities as they attend to daily tasks and provides helpful insights for enterprises to consider before embarking on new projects, investing in new technologies, or making other key business decisions, all of which could potentially be impacted by a breach.

[1] “Cybersecurity Solutions for a Riskier World,” ThoughtLab, May 2022.

[2] Ibid.

www.fortinet.com

March 23, 2023 2:06 PM
2029872-0-0-EN