FORTIS By Sentinel

Advancing Your Protection

Incident Response
Compromise Assessment

A high level forensics evaluation designed to identify current and past threat activity.

Sentinel's compromise assessment uses lightweight scripts coupled with AI-based tools to identify anomalies and correlate them to root causes. These indicators of compromise (IOCs) answer the question, "Are we (or have we previously been) compromised?" If no compromise is detected, our focus shifts to identifying any risks detected in your systems.

FOCUS AREAS

When attempting to identify a compromise, Sentinel's expert technical analysts investigate the following areas:

- Data Exfiltration & Sabotage
- Command & Control (Botnet) Detection
- User Account Activities
- Malware & Persistence Tools
- Network, Host, & Application Configurations
- Privilege Escalations
- Risks & Vulnerabilities

AREAS OF EXPERTISE

Compromise assessments can be performed for any or all of the following technologies.

- **Client & Server Endpoint Devices**
- **Cloud Email Platforms**
- **Network Edge Devices**
- **Perimeter Web Servers**
- **Active Directory**

GET STARTED

If you are interested in learning more about our compromise assessments, please contact Sentinel or your existing Sentinel Account Manager today.

Sentinel Technologies
1.800.769.4343
Sentinel.com/Solutions/FortisBySentinel
(24/7/365) Incident Response Hotline:
(844).297.4853