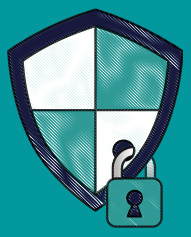
Compromise Assessment

Prevent Future Attacks by Determining If a Compromise Has Already Happened



CCS Group LIMITED

Benefits

- Proactively determine if a network has been compromised
- Identify areas of risk to better protect against a future attack
- Obtain results in weeks, not months
- Experience limited impact on system resources through a scalable and efficient process — launched through dissolvable scripts
- Receive assessment coverage of all operating systems

Accurate Compromise Assessments are Critical

Can an organization truly know whether or not it has been compromised? How easily can the extent of a breach be identified? Cyberattacks have become increasingly sophisticated and the sheer number of connected devices presents an unprecedented opportunity for threat actors.

CCS's Compromise Assessment evaluates an organization's security posture to determine if a breach has occurred or is actively occurring. The assessment can determine when, where, and how a compromise occurred, and provide tactical recommendations for preventing another attack.

By integrating artificial intelligence into tools and processes, our experts secure environments while swiftly identifying a compromise, resulting in a preventative security approach.

Service Overview

CCS's Compromise Assessment utilizes a proven methodology for identifying environmental risks, security incidents, and ongoing threat actor activity in a network environment. The assessment identifies ongoing compromises and uncovers the malicious access and usage of the environment.

The goal is to detect and stop any active security incidents quickly and quietly. The assessment is composed of three phases — with each phase more targeted — and addresses core problems such as:

- Data exfiltration and sabotage
- Command and control activities
- User account anomalies
- Malware and persistence mechanisms
- Network, host, and application configurations

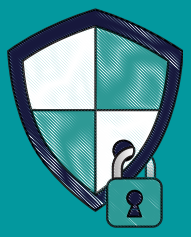
Scope of Investigation

Phase 1	Phase 2	Phase 3
File and Operating Audit	Network Logs Audit	Host Memory Analysis
Network Logs Audit	Host Memory Analysis	Host Disk Forensics
	Host Disk Forensics	Network Forensics

Get Started Today! **+1 (441) 294-3400** **www.ccs.bm**

Compromise Assessment

Prevent Future Attacks by Determining If a Compromise Has Already Happened



CCS Group LIMITED

Deliverables

At the conclusion of the assessment, a comprehensive report is provided to the executive team that details:

- A list of vulnerabilities detected
- The risk state of the environment
- Strategic and tactical recommendations for remediation

How confident are you?

Do you know whether or not your organization has been compromised?

Contact the CCS team to learn how a Compromise Assessment can help you identify and eradicate security vulnerabilities.

How It Works

Any organization can participate in a Compromise Assessment, regardless of which security solutions they are currently using. DigitalEra security experts will conduct assessments that include three main phases:

Phase 1 — Initial Assessment

In this phase, self-delegating and human readable scripts are pushed out to endpoints either through dissolvable scripts using the customer's existing software deployment or through a CCS agent.

These scripts assist in gathering key data that helps in searching for anomalous behaviors and conditions that are indicative of malicious activity or correlate to risks in the environment. The output from these scripts is then forwarded to the cloud for both manual and automated analysis to determine hosts of interest.

Phase 2 — Targeted Assessment

Targeted scripts are deployed to hosts of interest identified in Phase 1. Network logs are collected to gather more in-depth data and analysis related to the behaviors and activity previously identified. It is also determined whether the findings from Phase 1 were false positives or indicate malicious activity.

Script output is again forwarded to the cloud for analysis; however, it includes forensic artifacts to facilitate the validation that attacks have taken place or are underway. Containment strategies and other options moving forward are identified and communicated to the organization.

Phase 3 — Forensic Assessment

If, according to internal corporate policies, certain computers require retention for legal or other purposes, or if more scientific/technical analysis is necessary, then activities will include a full bit-by-bit disk copy of those computers, including memory dump, for related analysis.

As with Phase 2, any new information is utilized to identify additional systems of interest from the Phase 2 database, and subsequent analysis is then conducted.