

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 or the CylancePROTECT® agent
- Receive assessment coverage of all operating systems



The number of data breaches involving stolen or weak passwords has risen from 50% to 81% during the past three years.

Source: 2017 Verizon Data Breach Investigations Report (DBIR)

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.

Cylance® Consulting’s Compromise Assessment **evaluates an organization’s security posture to determine if a breach has occurred or is actively occurring.** Cylance Consulting 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, Cylance experts secure environments while swiftly identifying a compromise, **resulting in a preventative security approach.**

Service Overview

A Compromise Assessment utilizes a 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 System Audit	Network Logs Audit	Host Memory Analysis
Network Logs Audit	Host Memory Analysis	Host Disk Forensics
	Host Disk Forensics	Network Forensics

..... Coverage of IT Environment

About Cylance Consulting

- World-renowned experts work synergistically across our practice areas to deliver consistent, best-in-class services anywhere in the world
- Incorporates artificial intelligence into tools and processes to more efficiently and effectively secure the environment to *prevent* attacks from happening
- Utilizes multiple techniques to collect information, assess data, provide a risk profile, recommend actions, and highlight notable strengths for an organization
- Techniques are designed to not impact the client's operations in any way
- Integrated practice areas: ThreatZERO™ Services, Incident Containment and Forensics, Red Team Services, Industrial Control Systems Security, IoT and Embedded Systems, and Training

How It Works

Any organization can participate in a Compromise Assessment, regardless of whether they are currently using Cylance solutions or not. Cylance 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 the CylancePROTECT 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.

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 in knowing whether or not your organization has been compromised? Contact Cylance Consulting or your technology provider to learn how a Compromise Assessment can help you identify and eradicate security vulnerabilities.