Nth GENERATION

Compromise Assessment

Prevent Future Attacks by Determining if a Compromise Has Already Happened

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

Nth Generation's Compromise Assessment -powered by Cylance IP- **evaluates an organization's security posture to determine if a breach has occurred or is actively occurring**. Our Security experts 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 help **secure environments while swiftly identifying a compromise**, resulting in a preventative security approach.

.

Service Overview

An Nth Generation 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:

- Network host and application configuration
- User account activity
- Malware and persistence mechanisms

Scope of Investigation --►

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

◄ --

Coverage of IT Environment

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

197 days is the Mean Time To Identify (MTTI) data breach incidents.

Source: Ponemon Institute, 2018 Cost of a Data Breach Study

POWERED BY CYLANCE CONSULTING
A professional service group of BlackBerry Corporation

How It Works

Any organization can participate in a Compromise Assessment, regardless of whether they are currently using Cylance solutions or not. Our security experts will conduct assessments that include two main phases:

Phase 1 — Initial Assessment

In this phase, data collection scripts, CylancePROTECT and/or CylanceOPTICS are deployed throughout the entire environment leveraging existing software deployment software. These scripts and software assist in gathering key data that assists in searching for anomalous behaviors and conditions that are indicative of malicious activity or correlate to risks in the environment. The output from the scripts and software is then forwarded to the cloud for both manual and automated analysis to determine hosts of interest.

Phase 2 — Targeted Assessment

Targeted stand-alone executables are deployed to hosts of interest identified in Phase 1 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. Data is 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.

Deliverables

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

- Network host and application configuration
- User account activity
- Malware and persistence mechanisms
- Command and control activity
- Data exfiltration and sabotage
- The risk state of their environment
- Strategic and tactical recommendations for remediation

How confident are you in knowing whether or not your organization has been compromised?

Contact assessments@nth.com to learn how a Compromise Assessment can help you identify and eradicate security vulnerabilities.