COMPROMISE ASSESSMENT

Managing cyber threats across your organisation

Cyber attacks leading to high-profile data breaches have steadily increased with the ever-growing number of connected devices and sophistication of threat actors. Given such a large opportunity for threat actors, and despite growing security investments, companies struggle to identify whether they have been compromised. Understanding whether your organisation has been breached and identifying methods to reduce risk is critical to preventing cyber threats.

OBJECTIVES

A Cyber Citadel Compromise Assessment helps you determine environmental risks, security incidents and ongoing threat activity in your network environment. A set of core objectives underpin the threat activity hunt, as follows:

- Malicious files and activity
- Unusual ports, protocols, or malformed data packet transmissions
- Unusual data transmission levels from a host or to a specific destination
- Sensitive data leaving the network, such as PII, personal data or credit card information
- Command and control communication and backdoors
- Suspicious changes in behaviour on the database and application servers
- Indicators of the presence of any file-less malware.

OVERVIEW AND BENEFITS

A Compromise Assessment combines Cyber Citadel's extensive experience, proprietary technology and behavioural analytics with industry-leading threat intelligence to evaluate an organisation's security posture.

A comprehensive assessment by Cyber Citadel helps avoid financial and reputation loss to a business by increasing preparedness and identifying ways to minimise risk, including the following key benefits:

- Provides a robust analysis of ongoing or previous compromises and breaches
- Provides risk assessment by identifying vulnerabilities in security architecture, system security misconfigurations, improper policy violations and human error
- Provides increased situational awareness on systematic risk of exposure
- Increases an organisation's preparedness for future intrusions
- Reveals insights into the motivations of a threat actor
- Delivers MITRE's ATT&CK model to help characterise and describe post-compromise behaviour
- Provides comprehensive reporting of the assessment and guidance on remediation

6 Months

Average time for a company to detect a data breach.

Source: ZD Net

31%

Percentage of organisations that have experienced cyber attacks on operational infrastructure.

Source: Cisco

4%

Percentage of global annual turnover that companies can be fined for GDPR non-compliance.

Source: EU Commission

APPROACH

The Cyber Citadel team deploys various technologies to search and analyse logs for evidence of attacker activity, monitor network traffic, analyse endpoints, and inspect mail. Clients choose the correct combination of technologies appropriate to their environment.

Log Analysis

Logs from various applications, infrastructure, and security hardware are collected to identify any malicious activity by conducting a log inspection. Note: There are various log formats which are difficult to normalise, logs have limited coverage, and queries can be expensive, so therefore the security personnel must be very experienced.

Network Analysis

Strategic monitoring takes place to detect compromise activity, such as unauthorised remote access, malware command and control communication, and data theft.

Endpoint Analysis

Real-time detection of malicious activity is provided, including malware and other procedures and techniques, by carrying out a

detailed Endpoint Inspection. In an INFOCYTE HUNT architecture, surveys are adopted at endpoints via existing remote management protocols and dissolve in minutes. There are tools known as 'poor hunt tools' due to low false-positive alerting and low false negatives.

Email Analysis

Assessment of inbound and outbound emails is carried out through email inspection. The email attachments can be passively scanned to look for malware and other activities used for an intrusion

CORE ADDRESSABLE PROBLEMS

- Exfiltration, Corruption, Disruption
- Command and Control
- User Account Anomalies
- Malware and Persistence
- Network, Host and Application Configurations

ASSESSMENT PHASES

At the beginning of the project a **planning** phase takes place in order to devise the course of action. It develops an understanding of the compromise assessment as per the requirements and system architecture of the client. Since the context of the assessment is imperative, it is very important to agree a clear scope with the customer before proceeding.

Next, in the **preparation** phase, a strategy is developed to implement the compromise assessment processes. The compromise **assessment** phase is then carried out. All nodes of data communication are scanned including email, endpoints, networks, attachments, logs, and software. The compromise assessment concludes with the **discovery** of various vulnerabilities, unpatched data points, endpoint assessments and other potential gateways of intrusion, such as email.

Once the vulnerabilities are detected, a forensic state **analysis** (Forensic Triage) is carried out utilising the data stack and the hunt analysis method by reviewing all running processes and loaded modules. It involves a review of all autorun entries, locations, all execution and forensic artefacts. This analysis is used to identify any evidence of host manipulation. Additionally, there are some methods known as the collection methods, which are real-time monitoring (Sysmon and EDR or ELK), on-demand collection (periodic or one time by Forensic Triage) and query by specific question, or searches for IOC's (real-time by OS Query and for non-real time by EDR). It is important that the assessor does not rely on the existing data/logs in the environment to maintain efficacy and input their own primary data. It must be agentless security, and must concentrate on endpoints/servers. There are some recommendations which utilise on-demand/forensic-triage type collections. It is important to note the query/IOC searches are not appropriate for comprehensive, proactive assessments.

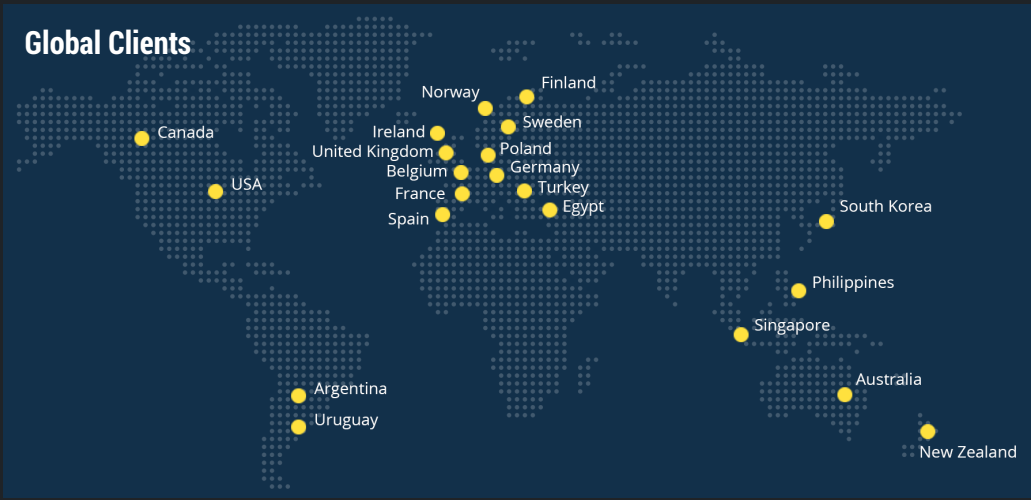
The Compromise Assessment concludes with comprehensive **reporting**. If a compromise is detected, our reporting breaks down the complex information into a clear chain of actionable intelligence. We highlight the areas of compromise and provide guidance on remediation activities to optimise your team's response time. Even if our assessment does not find any threat activity, we will identify steps your company can take to improve your resiliency and breach readiness.

GET IN TOUCH

info@cybercitadel.com

Cyber Security. It's time to get real.

www.cybercitadel.com



SYDNEY

Level 25, Tower 3
300 Barangaroo Ave
Barangaroo
NSW 2000
+61 2 8318 0290

MELBOURNE

Level 14, The Dome
333 Collins Street
Melbourne
Victoria 3000
+61 3 8592 0580

AUCKLAND

Partners Life House
33-45 Hurstmere Road
Takapuna
Auckland 0622
+64 9 940 2250

CHICAGO

+1 312 940 8388

LONDON

+44 203 677 0000