COMPROMISE ASSESSMENT

Capture. Analyse. Report.

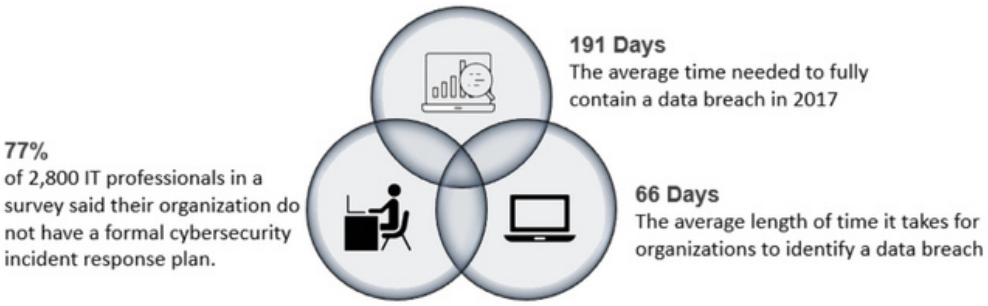
NETWORK INTELLIGENCE
Global cybersecurity provider

Compromise Assessment

Are you confident that your organization has not fallen victim to a compromise that you don't know yet?

Recent research has shown that organizations typically take upwards of 200 days to realize that they have been victims of an advanced attack.

High-profile data breaches in the news represent only a fraction of the intrusion activity carried out globally. Knowing whether your organization has been breached and identifying ways to reduce risk is crucial to preventing your organization from becoming the next major data breach headline.



SERVICE OVERVIEW

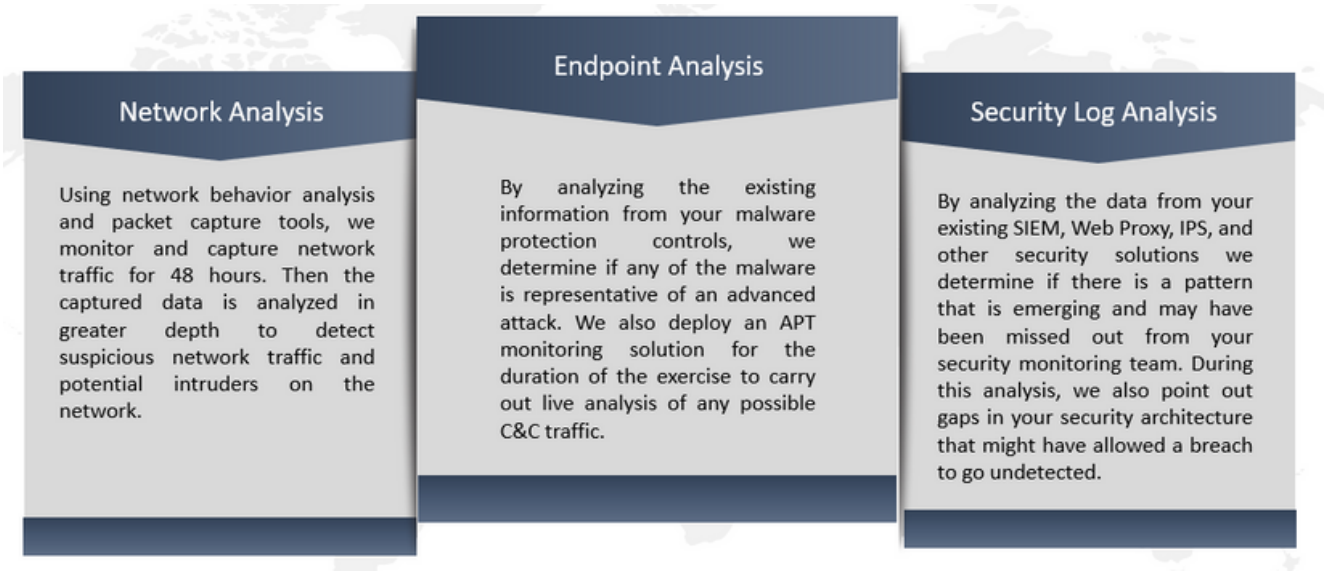
Network Intelligence's Compromise Assessment service focuses on capturing, analysing and detecting suspicious traffic, malicious activities, compromised systems, and the possible presence of an attacker or backdoor within the corporate network.

If, during the assignment, the presence of a significant breach is detected, which goes beyond the standard garden-variety malware, a more detailed analysis of the malware, its nature, the control gaps that allowed the breach to take place in the first instance, and remedial actions to correct breach and prevent it from recurring, are suggested.

APPROACH AND METHODOLOGY

Analysis of network, endpoint, and log data:

This is the first step when conducting a compromise assessment service which tries to monitor, capture and analyze the network, endpoint and log data for approximately 48 hours.



Identification of compromised systems

Based on the analysis of network, end-point and security log data, we try to identify systems which may have been compromised or which were compromised in the past. A more detailed analysis is then carried out of the malware and the specific modus operandi used by the attackers to penetrate into your network.

Analysis of attacker activity

As part of this assessment, we also seek to determine how much and what data may have been compromised. Our team will also advise whether it is worth pursuing the case with local law enforcement, or it might be better to simply contain the attack, determine the financial and regulatory impact from it, and move to plug the lapses that led to the attack occurring in the first place.

Deception Technology

Deception technology provides the innovation required to easily execute an active defense. By deploying decoys throughout the network, companies achieve efficient detection for every threat vector and every phase of attack. Utilizing high-interaction decoys and lures, deception solutions deceive attackers into revealing themselves, thereby closing detection gaps on threats that have evaded other security controls. By partnering with Attivo's ThreatDefend Deception and Response Platform, we are able to deliver unparalleled visibility into threats inside your network and into attacker lateral movements and tactics.

Report of findings

After completion of this activity, we would provide a detailed report of our observations, security gaps, and recommendations how these are to be addressed. These recommendations would cover the technology controls at the endpoint, network, perimeter and application levels. They would also address process gaps if it is concluded that this is an attack which the existing security mechanisms should have picked up. As mentioned earlier, we would also try to determine the data that has been lost by the organization.

ABOUT NETWORK INTELLIGENCE

We are a global cybersecurity provider founded in 2001 with more than 600 team members working out of our New York, Singapore, Dubai and Mumbai offices. We offer services across 6 broad spectrums - Assessment, BCMS, GRC, Professional Services, MSSP & Trainings. We serve customers across industry verticals such as Banks and Financial Services, Technology and Media, Oil & Power, Airlines, E-commerce, Retail, etc. We believe that cybersecurity is not a destination, it is a journey and we partner with our clients to address the dynamic cybersecurity threat landscape.

TO KNOW MORE ABOUT OUR COMPROMISE ASSESSMENT SERVICE: CLICK HERE

US | Singapore | India | UAE | Netherlands

info@niiconsulting.com

www.niiconsulting.com