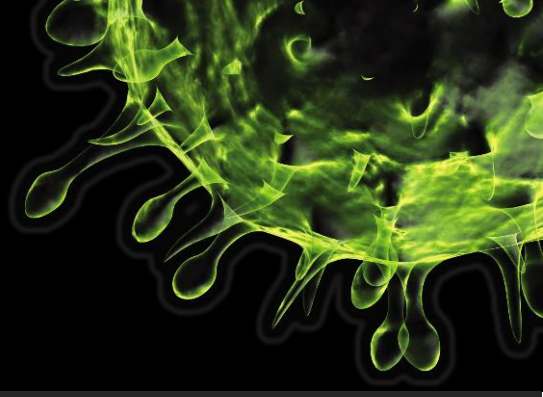
Deloitte.

Cyber Compromise Assessment



THE PROBLEM

Use of advanced malware by sophisticated attackers is becoming an increasing threat to organisations today as it enables them to remain undetected. Advanced malware can operate 'under the radar' and remain undetected and potentially lead to reputational damage, data loss, theft, regulatory fines and operational disruption.

Research has shown attacks that have prolonged access typically extend across the supply chain, and a correlation between extended access and the likelihood of a disruptive outcome.

Using Deloitte's **Cyber Compromise Assessment (CCA)** on your estate will help identify if there is a current or indicators of a past compromise of your network - utilising the latest threat intelligence and detection techniques.

201
Average days to identify a breach^

70%
Attacks that involve lateral movement*

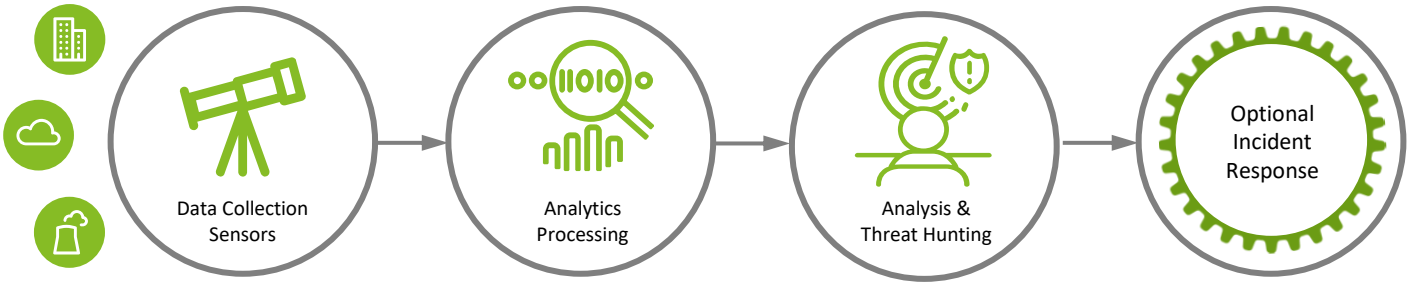
50%
Attacks leveraging supply chain*

31%
Victims experience destructive outcomes*

Advanced malware can operate **under the radar** and remain undetected

OUR SOLUTION

The approach is designed to be light-touch, with simple and temporary monitoring installations. With a typical end-to-end duration of approximately seven to nine weeks, dependent on the nature of any incidents identified and the remediation activities undertaken.



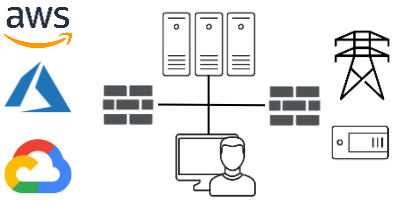
^ Deloitte Beneath the surface of a cyberattack, 2018
* Carbon Black Global Incident Response Threat Report, 2019

PEACE OF MIND

The CCA not only identifies past or current compromises – it also assists in the validation that your existing controls are effective in preventing and detecting a compromise, provides perspective on your cyber maturity vs. your industry peers, and recommendations on improvements that can be made.

We apply our industry experience and heritage in business risk and advisory to identify appropriate systems and segments to include in the CCA scope - understanding the relationship between business systems, platforms and protocols unique to industries and technology allows Deloitte to tailor each engagement to deliver maximum value while minimising business disruption.

Inspection points for sensors include traditional network taps and client endpoints – with further capability to target cloud (AWS, Azure and GCP), IT/OT boundary, OT network (passive detection and threat monitoring) and analysis of an existing data lake (Splunk, Hadoop, Elastic).



Using a combination of open source and proprietary technology, data from the deployed sensors is ingested and processed to identify alerts and events for further investigation and/or consideration for recommendations.

In addition to analysis of the analytic processing alerts, Deloitte applies our sector specific threat intelligence to pro-actively hunt for evidence of threats in the client environment.

In the event that actual compromise is discovered, Deloitte can provide incident response services which may include malware analysis, incident investigation, forensic data collection services.

Contact Us

Ho Siew Kei
Executive Director
Deloitte Business Advisory Sdn Bhd
sieho@deloitte.com
+603 7610 8040

Azlan Mohamed Ghazali
Director
Deloitte Business Advisory Sdn Bhd
amohamedghazali@deloitte.com
+603 7610 8497