CYLANCE CONSULTING

Malware Assessment

Prevent Future Malware from Entering the Network

Today's malware is highly sophisticated, targeted and complex. With malware at the root of so many security breaches, a malware assessment is a vital component of any incident response program. It helps responders understand the extent of a malware-based incident and to rapidly identify additional hosts or systems that could be affected.

A Malware Assessment from Cylance® Consulting can help organizations **identify and remediate all malware in the environment** as well as provide strategic and tactical recommendations to **ensure a preventative posture against a future compromise**.

Service Overview

The primary focus of a Malware Assessment is to evaluate the maturity and capabilities of your organization's security tools to detect malware in the environment. The objectives of the assessment include:

- Identification and remediation of all malware in the environment
- Discovery of the presence of active or past malware campaigns
- Development of Indicators of Compromise (IOCs) to prevent future infections
- Efficacy assessment of anti-malware detection tools

Depending on what was found during the assessment, Cylance Consulting may move into a full incident response and/or forensics engagement. A Security Tools Assessment may also be conducted to evaluate the organization's maturity based on tool capabilities.

Deliverables

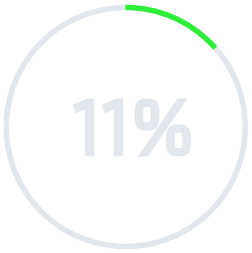
Cylance Consulting will furnish a comprehensive report detailing:

- All malware, adware and potentially unwanted programs (PUPs) identified
- Analysis and assessment of the current antivirus solution including other malware detection solutions in place
- Reverse engineering of malicious binaries
- Containment and remediation strategies

Prevent future malware-based incidents with a comprehensive assessment of your current environment. Contact Cylance Consulting or your technology provider to discuss your malware detection history.

Benefits:

- Reveal the functionality of the malicious code including its capabilities, intent, attack vector, motivation, and tactics
- Identify impacted systems and any changes the malware may have made to affected systems
- Ensure a more swift and effective response and containment
- Reveal technical indicators that can be used to spot additional infections and compromised resources
- Prevent future malware-based incidents of similar nature



The cost of malware attacks has increased by 11% over the year and is considered the most expensive attack type for organizations.

Source: 2019 The Cost of Cybercrime Study, Accenture Security

BlackBerry
CYLANCE

+1-877-973-3336
proservices@cylance.com
www.cylance.com/consulting