CYLANCE CONSULTING

Incident Containment and Malware Analysis

Immediately Prevent and Contain Incidents

Benefits

- Instant agentless analysis for Linux®, Mac®, and Microsoft Windows®
- Dedicated machine learning technology and services
- Analysis tools that identify the scope of incidents within hours, not days, weeks, or months
- Immediate resolution for quicker and less expensive incident response

87% of respondents reported incidents in the past 12 months.

Source: Incident Response Capabilities in 2016: The 2016 SANS Incident Response Survey | June 2016

Whether you already have an incident response process in place, or need to augment or build one, Cylance Consulting is your partner for immediate help. Cylance Consulting's approach is to stop the active threat while applying proprietary processes and tools that quickly diagnose the environment and rectify the situation.

Active incidents need active protection. Waiting for mid-tier providers or consulting firms to find the time to respond can cause further harm and drive up the total cost of a security incident. Cylance Consulting's Incident Containment and Malware Analysis Services are designed to **provide instantaneous access to Cylance security**. Our world-class team has decades of experience working with enterprises to mitigate risk immediately.

Service Overview

Incident Containment and Malware Analysis Services are designed to protect your business during an incident without relying on the lengthy process of investigation, testing, analysis, remediation, and solution implementation. Using proven methodology for approaching comprehensive incident containment, Cylance Consulting helps your organization:

Understand Current Threat and Client Objectives

- How was the issue detected?
- What data has been collected?
- What is the profile of the security threat?
- Has anything been done so far to mitigate the solution?
- Prioritize all goals
- Recover from data loss
- Identify the attacker
- Determine the attack vector

Contain Malware and Potentially Unwanted Programs (PUPs)

- Deploy malware containment tool
- Analyze and contain PUPs

Collect Evidence

- Collect and document evidence
- Follow chain of custody procedures consistent with law enforcement standards

Analyze the Attack and Malware

- Determine the attack vector
- Identify the extent of the compromise
- Establish a timeline for the incident
- Analyze malware, forensics, and logs
- Provide access to an expert malware analyst/incident containment agent
- Analyze static, behavioral, network, and exploits
- Conduct advanced persistent threat analysis to determine if the threat was targeted or generic

About Cylance Consulting

- World-renowned experts work synergistically across our practice areas to deliver consistent, fast and effective services around the world
- Incorporates artificial intelligence into tools and processes to more efficiently and effectively secure the environment to PREVENT attacks from happening
- Utilizes multiple techniques to collect information, assess data, provide a risk profile, recommend actions, and highlight notable strengths for an organization
- Techniques are designed to not impact your operations in any way
- Integrated practice areas: ThreatZERO™ Services, Incident Containment and Compromise Assessments, Red Team Services, Industrial Control Systems Security, IoT and Embedded Systems, and Training

Contain the Incident

- Contain the incident before moving forward with any additional testing or reporting
- Do more than just try to understand issues – work to prevent them

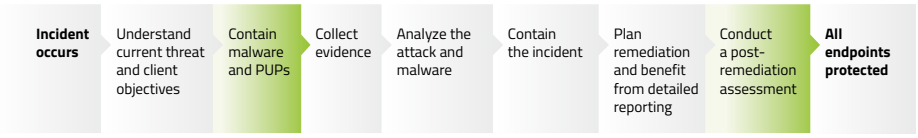
Plan Remediation and Benefit from Detailed Reporting

- Provide status reports to management to communicate details of the attack
- Develop detailed remediation plans for moving forward
- Assist with implementation of remediation recommendations
- Benefit from detailed reports of all findings from the incident investigation - reports are appropriate for management, technical staff, insurers, and litigators

Conduct a Post-Remediation Assessment

- Test all systems once remediation is complete to ensure there are no lasting effects of the incident

The Cylance Consulting Approach



Contact Cylance Consulting or your technology provider to discuss your Incident Containment, Incident Response Retainer, and Malware Analysis needs.

+1-877-97DEFEND
proservices@cylance.com
www.cylance.com/consulting

CYLANCE