CYLANCE™

CONSULTING

INCIDENT RESPONSE AND MALWARE ANALYSIS

Immediately Prevent and Contain Incidents

Every second of delay after a breach can result in further harm. IT staff is forced to drop everything to initiate a lengthy chain of discovery, analysis, verification and solution implementation, all while under crisis. As time ticks by, the damage continues.

Active incidents need active protection. Incident Response and Malware Analysis Services from Cylance® are specifically designed to protect your business during an incident without relying on a lengthy process of investigation, testing, analysis, remediation and solution implementation. Cylance's world-class Consulting team has decades of experience working with enterprises to mitigate risk immediately.

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

The Cylance Difference

When seconds count, waiting for mid-tier providers or large consulting firms to find the time to respond can cause further harm and drive up the total cost of a security incident. Get the security and dedicated response your organization deserves:

- 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 that leads to quicker and less expensive incident response

Why Do I Need An Incident Reponse Retainer?

When you are the victim of a cyberattack, you should have someone you can call for help. If you rely on mid-tier providers or large consulting firms, you could be waiting for days. If you have an incident reponse retainer with Cylance's Consulting team, you will get an immediate response:

- Instantaneous access to Cylance security experts
- Pre-negotiated terms and conditions
- Prioritized, effective response

Cylance's Approach to Incident Response

Cylance's Consulting team has developed a proven methodology for approaching comprehensive incident response:

Understand the 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 situation?
- Prioritize all goals
- Recover from data loss
- Indentify 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

Attack and malware analysis

- Determine the attack vector
- Identify the extent of the compromise
- Establish a timeline for the incident
- Malware, forensic and log analysis
- Access to an expert malware analyst/incident response agent
- Static, behavioral, network and exploit analysis
- Advanced persistent threat analysis to determine if the threat was targeted or generic

Incident containment

- Most companies will just try to understand the issues
- Cylance will actually contain the incident before moving forward with any additional testing or reporting

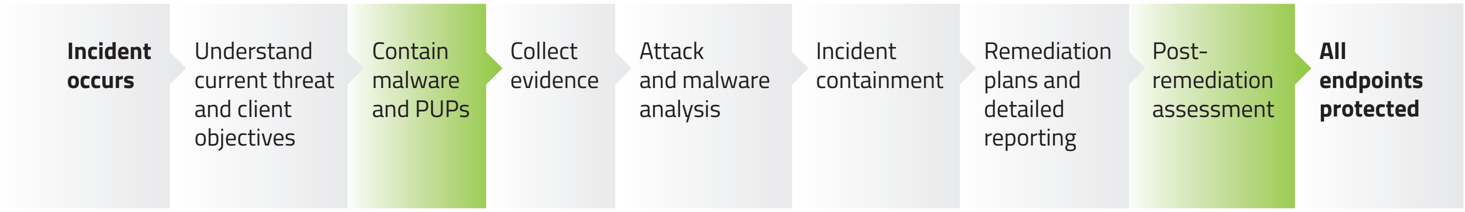
Remediation plans and detailed reporting

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

Post-remediation assessment

- Once all remediations is complete, Cylance will test the systems again to ensure that there are no lasting effects of the incident

The Cylance Consulting Approach


Incident occurs
Understand current threat and client objectives
Contain malware and PUPs
Collect evidence
Attack and malware analysis
Incident containment
Remediation plans and detailed reporting
Post-remediation assessment
All endpoints protected

About Cylance:

Cylance is the first company to apply artificial intelligence, algorithmic science and machine learning to cybersecurity and improve the way companies, governments and end-users proactively solve the world's most difficult security problems. Using a breakthrough predictive analysis process, Cylance quickly and accurately identifies what is safe and what is a threat, not just what is in a blacklist or whitelist. By coupling sophisticated machine learning and artificial intelligence with a unique understanding of a hacker's mentality, Cylance provides the technology and services to be truly predictive and preventive against advanced threats. For more information, visit cylance.com

+1 (877) 97DEFEND
proservices@cylance.com
www.cylance.com
18201 Von Karman Ave., Suite 700, Irvine, CA 92612