CYLANCE CONSULTING

Incident Response Readiness Assessment

Put Your Incident Response Plan to the Test

Incident response is a multi-faceted discipline and can be a very complex process when dealing with complicated attacks. Incident response demands a myriad of capabilities that typically require resources from various operational units of an organization, including human resources, legal counsel, IT and security professionals, corporate security, business managers and users, and the help desk.

In an effort to ensure that key personnel have been identified and the appropriate IT and security technologies are brought together in a cohesive manner, Cylance Consulting's Incident Response Readiness Assessment (IRRA) helps **analyze your current response program and identify gaps or weaknesses to assist in avoiding pitfalls during a real-world incident**. The IRRA provides an opportunity to ensure that the documented processes followed, and current controls are effective for responding to a future security incident. Utilizing industry best practices, our IR experts will **review how existing controls and processes enable your organization to quickly detect and contain security incidents**.

Service Overview

Discovering broken processes in an existing incident response plans during a critical incident is never something any organization wants to encounter. To avoid this pitfall, Cylance Consulting will assess key areas of the organization's documentation and response capabilities, which include:

- Policies, Standards, Procedures, and Guidelines
- System and Network Diagrams
- Network and Endpoint Technologies
- Incident Response Plans and Playbooks
- Incident Response Capabilities
- External Response Capabilities
- Insurance Contracts

The IRRA lowers costs, prioritizes technology solutions, and focuses efforts to reduce the impact and time to containment in the case of a security incident.

Incident Response Readiness Assessment Phases and Duration*		
Phase 1	Documentation Review & Interviews	2-3 weeks depending on scope
Phase 2	Incident Response Readiness Assessment Development	2-3 weeks depending on scope
Phase 3	Reviews, Revisions, and Final Presentation	1-2 weeks depending on scope

**Schedule is an example time frame and may vary.*

Benefits:

- Provides an impartial view and baseline into detailed aspects of an organization's incident response and security technology strategy
- Identifies opportunities for improvement and provides recommendations for enhancing the response activities and security technology posture of the organization
- Provides a set of detailed requirements and measurable routine analysis that the organization can report up through the various layers of management
- Provides recommendations where security automation and orchestration technologies can be utilized, aimed at lowering costs across the organization

> "Sadly, most IR plans fail to deliver on this promise. For companies that have one—and according to one recent survey, one in three organizations don't—they are bare-bone, poorly set out and rarely involve any other lines of business (LOB) aside from the InfoSec and IT teams."

Source: CIO from IDG, 10 Steps for a Successful Incident Response Plan

Deliverables

At the conclusion of the engagement, Cylance Consulting provides results from the IRRA in a custom report:

- Formal Incident Response Readiness Assessment Report detailing positive findings and opportunities for improvemen for existing processes and technologies
- Formal Incident Response Readiness Assessment Executive Presentation

Evaluate your organisation's preparedness for a cyber attack. Contact Cylance Consulting or your technology provider to discuss an Incident Response Readiness Assessment.

About Cylance Consulting

- World-renowned experts combine subject matter experts from different practice areas to deliver consistent, fast, and effective services around the world
- Incorporates artificial intelligence into tools and back end data analysis processes to more efficiently and effectively secure the environment and *prevent* attacks
- 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 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 Education

BlackBerry

CYLANCE

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

MKTG 19-2026-20190716