CYLANCE CONSULTING

Merger and Acquisition Security Assessment

Gain Critical Insight into Potential Security Risks

Benefits

- OS-agnostic assessment across all server and workstation devices on the network without network taps, agents, or monitoring of egress points
- Gain full insight into any potential vulnerabilities on the endpoint, including any previous or actively occurring breaches
- Identifies both known and unknown threats across the environment with the goal of moving the environment into a preventative posture from cyberattack
- Leveraging methodologies that include artificial intelligence to provide the fastest results in the industry
- Identifies the shortcomings and resources needed for the security infrastructure to meet industry-recognized best practices



80% of respondents said cybersecurity issues have become highly important in the M&A due diligence process

Source: Testing the Defenses: Cybersecurity Due Diligence in M&A | West Monroe 2016

The importance of cybersecurity-related issues throughout the M&A process has increased significantly due to a rise in corporate data breaches and related potential liabilities. Data security issues can lead to large financial losses and can be indicators of risk exposure related to compliance concerns and the organization's reputation in the marketplace.

Cylance® Consulting's Merger and Acquisition Security Assessment helps organizations address this uncertainty by allowing M&A participants (including third-party legal firms) to **demonstrate expert due-diligence in the determination and preventative reduction of cyber risk.** Armed with information about the security posture of a possible acquisition, companies planning to acquire another can **plan fixes for identified vulnerabilities, use the information to aid decision-making whether to proceed with the acquisition, and may help negotiate a lower purchase price.**

Service Overview

Cylance Consulting helps organizations obtain a security baseline of the pending acquisition to reveal the critical information needed to gauge viability and value. Our methodologies leverage artificial intelligence and apply scripts that are quick and lightweight to obtain fast results.

A Merger and Acquisition Security Assessment is comprised of:

Compromise Prevention Assessment

A Compromise Prevention Assessment utilizes a methodology for identifying environmental risks, security incidents, and ongoing threat actor activity in a network environment. The assessment identifies ongoing compromises and uncovers the malicious access and usage of the environment. The goal is to detect and stop any active security incidents quickly and quietly.

The assessment addresses core problems such as:

- Data exfiltration and sabotage
- Command and control activities
- User account anomalies
- Malware and persistence mechanisms
- Identification of potential threats and/or vulnerabilities
- Network, host, and application configurations

About Cylance Consulting

- World-renowned experts work synergistically to deliver consistent, best-in-class solutions anywhere in the world
- Custom integration and rapid prototyping services are available to solve difficult and personalized challenges
- 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
- Integrated practice areas: ThreatZERO™ Services, Incident Containment and Compromise Assessments, Red Team Services, Industrial Control Systems Security, IoT and Embedded Systems, and Training

NIST Cybersecurity Framework (CSF) Gap Analysis

The goal of Cylance Consulting's NIST CSF Gap Analysis is to evaluate the policies, standards, and procedures implemented by the organization and how they align with the five core functions; identify, protect, detect, respond, and recover. Cylance Consulting's experts will identify positive practices, as well as areas for improvement.

Elements of consideration include:

- Policy, standards, and procedures
- Program management
- Human resources and organization
- Asset management
- Physical and environmental considerations
- Communications and operations
- Access control
- Information systems management
- Response plans and management
- Regulatory compliance

Deliverables

Cylance Consulting will furnish a comprehensive report detailing:

- Any compromises detected
- A list of vulnerabilities and potential threats
- Strategic and tactical recommendations for remediation
- Assessment findings and alignment of the security policies and procedures to the NIST CSF
- Remediation strategies to achieve compliance with the NIST CSF and industry best practices
- Instructions for developing a roadmap for continuous improvement and monitoring

The reality of the modern business environment is that every organization is vulnerable to cybersecurity problems. It is vital that a full security assessment takes place when considering M&A targets. Contact Cylance Consulting or your technology provider to discuss your data security needs.

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

CYLANCE™

©2017 Cylance Inc. Cylance® and CylancePROTECT® and all associated logos and designs are trademarks or registered trademarks of Cylance Inc. All other registered trademarks or trademarks are property of their respective owners.

20170504-1485