PacketWatch M&A

Overview

According to a survey[1] of close to 2800 decision-makers, 62% agreed that their company faces significant cybersecurity risk by acquiring companies. The same survey mentioned that Cyber Risk is their biggest post-acquisition concern.
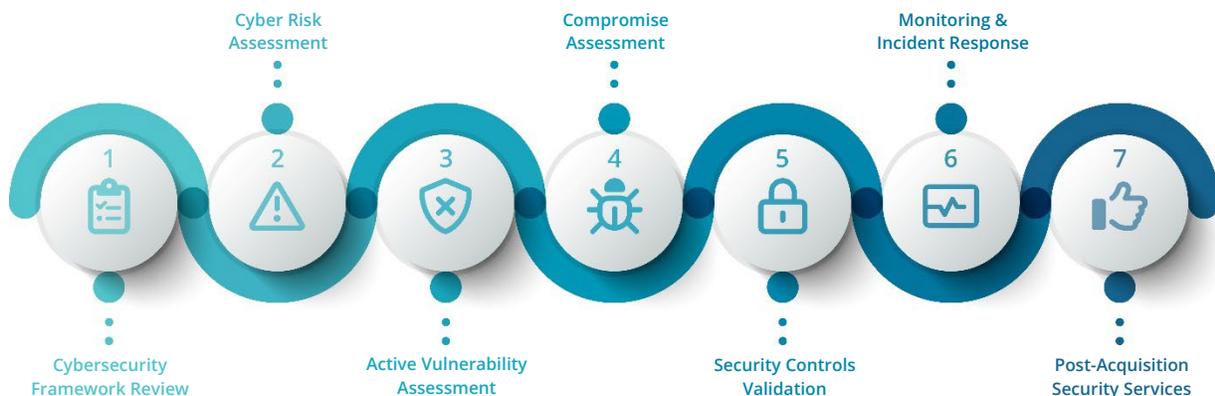
A Progressive Approach

PacketWatch has developed a comprehensive suite of cyber due diligence services that help buyers and sellers assess their security posture thoroughly. Since every situation is unique, our cost-effective approach adjusts to align with the size and scope of the transaction. However, when indicators of compromise are identified, the intensity and cost of the due diligence process increase. Up to seven due diligence steps may be implemented, and several additional cybersecurity services.

Why PacketWatch?

Our highly skilled experts and threat hunters use a proprietary software platform to analyze client networks at the packet-level to find and remediate cybersecurity risks others may have missed.

Benefits

- Helps buyers and sellers better understand their security program and posture

- Provides a complete security intelligence profile from multiple data sources

- Scans for vulnerabilities and tests controls to validate that they mitigate & eradicate risks

- Scours your network for advanced persistent threats and anomalous behaviors

- Monitors your network to identify abnormal activities and hunt for threats

1	2	3	4	5	6	7

Cyber Risk Assessment (2)
Compromise Assessment (4)
Monitoring & Incident Response (6)

Cybersecurity Framework Review (1)
Active Vulnerability Assessment (3)
Security Controls Validation (5)
Post-Acquisition Security Services (7)

PacketWatch M&A Cyber Due Diligence

1 Cybersecurity Framework Review

Using an industry-standard cybersecurity framework, we'll interview key members of the organization's IT and cybersecurity teams to evaluate, score, and compare the company's overall security posture with industry peers.

2 Cyber Risk Assessment

We'll look at the organization from the perspective of an attacker. Our experts will scan threat intelligence sources and the Dark Web to identify any exposed corporate data or user credentials that could be used to design a malicious attack campaign.

3 Active Vulnerability Assessment

We'll scan the organization's systems and networks, looking for known vulnerabilities, weaknesses, loopholes, and backdoors. Our experts will recommend ways to remediate weaknesses and harden systems to prevent malevolent activities.

4 Compromise Assessment

We'll thoroughly analyze the organization's network infrastructure with our proprietary, packet-level technologies. Our experienced threat hunters will look for indicators of compromise, as well as policy violations and misconfigurations.

5 Security Controls Validation

We'll test the effectiveness of the organization's security controls, including tools, procedures, and policies. Our team will safely execute the same tactics, techniques, and procedures (TTPs) that attackers use to perform the audit and educate the team.

6 Monitoring & Incident Response

We'll use managed detection and response, endpoint detection and response, and security log files to improve our visibility of the company's network. Our experts will proactively hunt, adjudicate, and eradicate threats before they become a problem.

7 Post-Acquisition Security

We'll help develop and test the organization's cybersecurity strategy, operations, and educational programs. Our consultants will advise the client on incident response, business continuity, disaster recovery, security policy, compliance, privacy, governance, training, and disclosures.

"I found the PacketWatch personnel to operate at the highest level of professionalism, technical expertise, and efficiency."

Call 1-800-864-4667 or visit www.packetwatch.com to discuss your M&A Cyber Due Diligence Strategy.

6263 N Scottsdale Rd, Suite 255, Scottsdale AZ 85250