CSPi
Technology Solutions

Security Assessments
Solution Overview

Real security intelligence that you can act on

Everyone talks about an intensifying threat landscape. And of course that is true. But today's security conversations need to go beyond scare tactics and hyperbole. They need to be focused, pragmatic, and emphasize actionable insights.

The focus on sophisticated threats has validity, but it is often misplaced for many organizations. They tend to be most vulnerable as a result of risks that intersect at the path of least resistance – email phishing, ineffective malware controls, compromised and weak passwords, and the like.

- ☐ **Gain actionable insights**
- ☐ **Improved threat detection**
- ☐ **Enhanced remediation**

At CSPi, our security assessments help clients gain visibility into what's hiding in plain sight, how a threat could permeate their environments, and how effectively they can sound their alarms. With actionable insights, organizations can more effectively identify the most obvious ways an attack could occur, their true capabilities to detect potential attacks, and how well they can remediate vulnerabilities.

Security assessment and deliverables

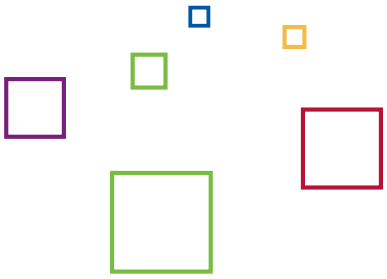
There are four key areas of focus to achieve actionable insight. Once we complete an assessment, we create a detailed report with findings and prioritized recommendations, debrief executives and the technical team, and provide six months of follow up support, guidance, and further analysis.

Understanding attack scenarios:

- Think like attackers to understand their motivations and valuable data they would target
- Uncover the easiest possible entry point
- Move beyond point-in-time visibility, delivering an ongoing process of understanding, testing, verifying, remediating, and defending

Identifying data at risk:

- Identify data valuable to an organization including credit card numbers, identities, and/or intellectual property
- Prioritize data to be protected
- Uncover possible regulatory requirements that need to be met



There are many vulnerability scanning tools available in the market, but most of them don't provide enough view into risk. It's important to understand and address attacker techniques, not just tool-based findings.

Quantifying the impact of a breach:

- Identify quantitative impacts of risks that may violate regulatory compliance requirements
- Identify qualitative impacts including reputation, brand, customer experience, trust, and likelihood to recommend

Recommendations to reduce risk:

- Develop a prioritized roadmap to address an organization's most pressing concerns
- Offer insight into what an organization is capable of (and should consider) doing to mitigate risk in the immediate, mid and long term

The value of a security assessment

Security assessments provide a functional security test, evaluating your security posture in action. You gain visibility and understanding into how your environment is responding to the most prevalent attack vectors. Many organizations rely on the cybersecurity success metric of, “did we get breached, yes or no,” which ultimately is ineffective. Doing a security assessment enables you to better understand what you should be measuring and what success looks like.

There are many vulnerability scanning tools available in the market, but most of them don’t provide enough view into risk. It’s important to understand and address attacker techniques, not just tool-based findings. A security assessment can help you gauge how technology and process are working together to protect information assets.

Much of security today puts a large onus on people as one of an organization’s biggest risk factors. However, security is still largely a technical challenge, which requires taking potential targets out of scope for an attacker. With the insight gleaned from a security assessment, organizations get an opportunity to rethink security approaches and strategies. For example, organizations can reevaluate whether passwords and security awareness training are effectively protecting the organization, or if stronger controls should be considered, like multi-factor authentication.

Why CSPi for security assessments

Integration expertise: As an integrator, CSPi is skilled across a broad spectrum of technologies, knows how these technologies should work together, and where things can break down. That expertise has been amassed from seeing technology environments firsthand. Our security professionals leverage that experience and powerful knowledge base as an integral part of the assessment process.

End-to-end consistency: Clients have access to a dedicated senior-level security professional for the entirety of the assessment process. Other assessment services rely on crowd-sourcing security testing activities. However, it can prove challenging to provide a clear picture of identified risks when correlating findings across five or 10 people.

Open, ongoing communication: Once the assessment and executive debriefing are complete, CSPi's senior-level security professional leads a monthly conference call to discuss progress. How much headway has the organization made with the proposed changes? What may be holding the organization back from making the changes? How can CSPi help? We also review indicators of compromise (i.e. email reputation scores highlighting the volume of spam and phishing emanating from the domain, compromised passwords, known vulnerable hosts, and exposure) and provide an update on any new known risk. If remediation has been done, there is often retesting that occurs.

See how CSPi's actionable security insights can work for you

Take advantage of a complimentary, 30-minute cybersecurity posture review, which identifies key areas of risk and what you can do to mitigate them. Click here to register now, or for more information contact us at 1-800-940-1111 or Technology_Solutions@cspi.com.

CSPi's security assessments provide actionable security intelligence based on threats that are unique to you and your organization. We can help you detect real threats, how and when they are happening, and how you can remediate as efficiently and cost-effectively as possible.