Leverage Cyber Security Validation to Optimize Security Investment

Cyber security spending has increased by 70 percent in the last four years, according to Moody's 2023 cyber survey. Businesses spend millions of dollars to protect critical digital assets from attack. Proactive organizations conduct cyber security validation to ensure that their cyber security investment pays off.

Cyber security validation involves testing and evaluating the effectiveness of an organization's cyber security strategy. Through simulated cyberattacks, security testing, and continuous monitoring, cyber security validation helps companies identify and prioritize their security gaps. This allows them to improve their security posture and demonstrate regulatory compliance.

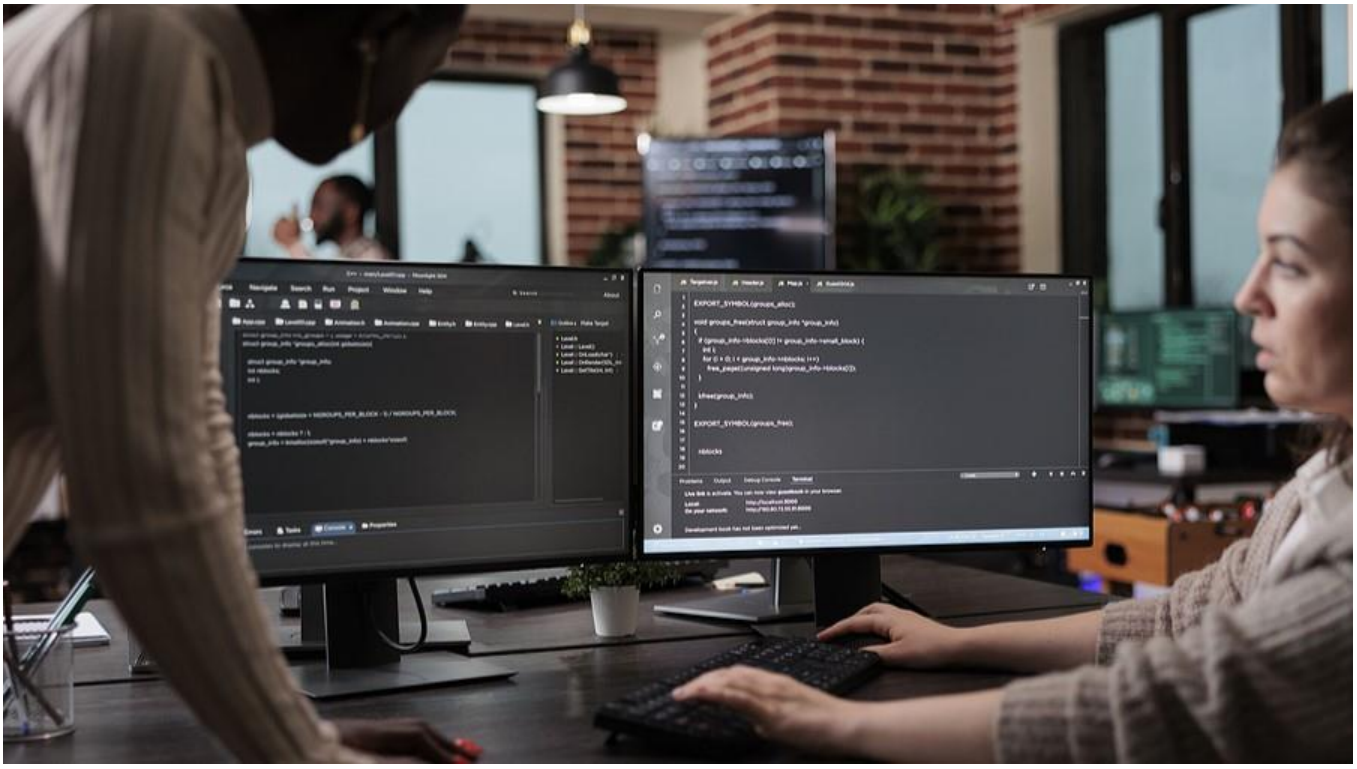
By evaluating existing controls and procedures against security best practices, and by testing security measures in realistic scenarios, organizations map out next steps. They also gain the data necessary to effectively prioritize security investments, aligning security strategies with business objectives and risk appetite.

Cyber security validation can include various types of assessments, each with its own benefits and limitations. Three common types of assessments include breach and attack simulations (BAS), red teaming, and penetration testing.

Breach and Attack Simulation (BAS)

BAS involves continuously testing the security posture of an organization by simulating realistic cyberattacks using automated tools. This process helps to identify vulnerabilities, gaps, and misconfigurations in the company's security controls and processes. It also provides actionable recommendations and remediation guidance to improve the security posture.

Performed continuously or periodically, BAS covers the entire attack surface of an organization. Consequently, it proves useful in identifying common vulnerabilities and maintaining a baseline security posture. Because it is highly automated, this type of assessment requires minimal interaction with the company's security team.



For example, a BAS might simulate a malware infection or data exfiltration. The resulting report will detail the success rate of defense against attacks. Once the security team makes adjustments to controls and procedures, another BAS will provide quantitative measurement of the benefit the changes have made.

Penetration Testing

Penetration testing involves ethical hackers conducting authorized attacks on specific systems, networks, or applications using the same tools an adversary might use. Performed occasionally, it involves moderate interaction with the security team. And it proves particularly useful in validating the security of specific systems and finding complex vulnerabilities.

While more time-consuming and expensive than a BAS, penetration testing involves greater scope, depth, and accuracy. Many organizations will use BAS to monitor their security posture on a regular basis. They will then use penetration testing periodically to perform a deeper analysis, identifying and fixing as many vulnerabilities as possible.

Red Teaming and Purple Teaming

Red teaming involves a team of ethical hackers mimicking the tactics and procedures of real-world adversaries. While BAS and penetration testing aim to identify as many vulnerabilities as possible, red teaming targets a specific objective. For instance, a red team might be given a specific task such as disrupting a particular service or compromising a specific account.

Similar to red teaming, purple teaming combines the offensive (red team) and defensive (blue team) side of cyber security. In this collaborative approach, the two teams work together to identify and remediate vulnerabilities. The red team launches simulated attacks against the target, while the blue team monitors and responds to the incidents.

Both red teaming and purple teaming provide valuable feedback on the effectiveness and resilience of security defenses and incident response. While incredibly valuable, red teaming requires careful planning and communication. It should only be performed by qualified professionals who have the necessary skills and experience.

eMazzanti Offers Comprehensive Cyber Security Validation Services

The cyber security professionals at eMazzanti deliver a variety of cyber security validation services to help organizations mature their security strategies. From ongoing monitoring to penetration testing and red teaming, our consultants have conducted thousands of tests.

The eMazzanti team brings intimate knowledge of exploits and attackers and proven methodology. By simulating real-world attacks on people, systems, and processes, they uncover security vulnerabilities and flaws that may introduce compliance risks. Armed with that information, they will help your organization develop a comprehensive remediation plan.