Find and fix weaknesses before they are exploited

DXC Ethical Hacking and Vulnerability Management

Identify and manage vulnerabilities with testing assessments, simulations and mitigation strategies, vulnerability management or intelligence services.

Benefits

- Assess the resilience of your people and processes.
- Achieve the optimum return on investment from your vulnerability management solution.
- Identify mitigation strategies to improve defenses.

Key industries

- Healthcare and Life Sciences
- Travel and Transportation
- Banking and Capital Markets
- Manufacturing
- Public Sector
- Consumer Industries and Retail
- Energy
- Communications, Media and Entertainment

Control security risks

Security is regularly cited as the No. 1 board priority for enterprises and governments around the world.

Many organizations are learning the hard way that lacking the right security and risk strategy can result in lost revenue and, ultimately, market capital. Despite massive investment, security operations are failing to evolve as quickly as their adversaries. For most companies, it comes down to three core challenges:

- **Cyber threats** are becoming more sophisticated. Cyber crime is now one of the most lucrative "industries" on the black market. In fact, by 2022, the cost to global business may reach an astonishing $8 trillion.[1]
- **Regulatory pressures** are causing an increase in cost and complexity. The General Data Protection Regulation (GDPR) is a game changer that went into effect in Europe in May 2018. Organizations selling goods or services to European Union citizens must ensure that personally identifiable information is protected and that stringent processes are followed if data is lost.
- **The skills gap** keeps widening. Finding, hiring, training and retaining skilled employees are becoming ever more difficult. There just aren't enough cyber security professionals to meet demand and stay current on the latest tools, tactics and techniques employed by cyber criminals.

Ongoing security validation

Traditional penetration testing must be combined with simulation-based assessments to provide meaningful assurance.

At DXC Technology, we believe that to keep up with accelerated threat evolutions, traditional vulnerability identification methods must be complemented with robust and ongoing security validation.

Threat actors don't work just 1 month a year, and neither should our vulnerability detection architecture. We also have to:

- **Train like we fight:** White-hat penetration testers are often heavily restricted by scoping agreements. Black-hat hackers are not. If we hope to be ready for the adversary, we must evolve our penetration tests to simulate the actual attacks we are facing.
- **Embrace the evolution of cyber attack simulation:** We must address business questions such as, "Could threat group X steal designs for our latest product?" or, "Is it possible for organized crime group Y to identify our financial transfer process?" We can use threat intelligence to emulate the attackers that concern us most. This enables us to move past simple red teaming, to realistically mirror the real-world threats your enterprise faces.

[1] Juniper research, The Future of Cybercrime & Security: Enterprise Threats & Mitigation 2017-2022, April 2017

- **Optimize vulnerability management and remediation:** Attackers are quickly turning new vulnerabilities into weapons, so we must respond faster than in the past. The ability to provide evidence of a robust mitigation threat response is a key element of the GDPR.

DXC Ethical Hacking and Vulnerability Management services

DXC Ethical Hacking and Vulnerability Management services offer a comprehensive portfolio of services to ensure that your enterprise can identify, manage and mitigate vulnerabilities.

DXC's Penetration Testing offers a full suite of application and infrastructure testing. Our teams use manual and automated methodologies to provide thorough evaluations of your assets and to provide risk prioritization and mitigation recommendations. Penetration testing teams can also deliver customized social engineering assessments to determine the resilience of your people and processes.

Our approach to vulnerability management allows your enterprise to leverage DXC experts to implement a vulnerability management strategy. DXC's Managed Security Services provide support and guidance to enable you to get the optimum return on investment from your vulnerability management solution.

DXC's Cyber Attack Simulation delivers a real-world assessment to your business. Our advisors work with you to understand your primary business concerns. We then use our threat intelligence to understand the threat actor that is assessed to be the most likely attacker. We design a simulation that emulates the attacker's tools and tactics to provide a realistic representation of the threat. DXC advisors will execute the attack and provide detailed feedback and mitigation strategies to help you improve your defenses.

Expert resources and methodologies

DXC's advisory-led model gives your enterprise access to elite threat and vulnerability management professionals. Our approach allows your enterprise to exploit the vast knowledge of our strategists — who help align your overall defensive capabilities to your enterprise's business goals — as well as our deep technical specialists, who can advise to a granular level across the full spectrum of people, process and technology.

Threat and vulnerability experts are able to use DXC's proprietary threat intelligence, cultivated from our experience in operating 12 Security Operations Centers (SOCs) and our responses to scores of large-scale incidents each year.

Rely on DXC

Partnering with DXC has distinct advantages for enterprises competing in the global marketplace:

- DXC has more than 3,500 security professionals with deep specializations that include penetration testing, vulnerability management, SOC analytics, forensic investigation and threat intelligence.
- DXC's ethical hacking experts are accredited according to the highest government and industry standards, including the Council for Registered Ethical Security Testers (CREST) and Certified Ethical Hacker (CEH) qualifications.
- DXC advisors have a minimum of 5 to 10 years of experience at the highest security levels.
- DXC's proprietary threat intelligence allows us to deliver realistic simulation attacks to emulate the threat actor that concerns your organization most.
- DXC is vendor agnostic, which means we are not limited by any one technology but can work with best-in-class technology providers to deliver optimal security results.

Take the next step

Take the next step to see how DXC Ethical Hacking and Vulnerability Management services can help secure your business. Explore our extensive portfolio and leverage our advisors to identify how DXC can help you improve your security posture. For even more insight, request a whiteboard session with our expert advisory team to identify your organization's threat and vulnerability management pain points and requirements.

Learn more at

www.dxc.technology/security

MD_7504a-18. April 2019