CHECK POINT | CHECK POINT PROFESSIONAL SERVICES Consult • Design • Deploy • Operate • Optimize | CHECK POINT Cyber Resilience Team

Cybersecurity Resilience (Penetration) Test

Protect Your Critical Assets from Cyber Threats

In an era plagued by daily cyber-attacks, safeguarding your company's assets is paramount.

With over three decades of cybersecurity experience, Check Point brings together a powerhouse of security teams. This group consists of a global Incident Response Team, 300+ cyber security researchers, dedicated threat hunting and analysis groups, and the Cybersecurity Resilience Team (CRT).

Introducing the Cybersecurity Resilience Team (CRT): a specialized group of offensive security professionals that evaluate your business's defensive capabilities against the latest malicious techniques. We provide recommendations to enhance your infrastructure's resilience.

Partner with Check Point's CRT to fortify your defenses and protect your organization from evolving cyber threats.

Check Point's CRT Expert will:

- Work side-by-side with your response team to detect, react, and mitigate your security vulnerabilities
- Help you experience, assess, and remediate a simulated cyber-attack in a controlled/live environment
- Identify and protect your most critical assets and vulnerabilities at every level of your asset's hierarchy
- Reduce your response time to potential security events and service interruptions

Why Check Point?

- Worldwide cybersecurity leader for over 30 years.
- Safely protecting over 100,000 organizations of all sizes.
- Industry leading penetration testers with vast experience in offensive and defensive security related activities.
- Collaboration with Check Point's preeminent Research and IRT teams.

Types of CRT Offered by Check Point

Application Security

- **Web Application Security**

  Our Web Application Security assessment focuses on evaluating the security of your web-based applications. We thoroughly examine the key components of your web applications, such as the front-end interfaces and back-end systems. This assessment helps identify vulnerabilities and weaknesses in the web application's design, implementation, and configuration, ensuring a robust and secure online presence following OWASP top 10 methodology.

- **Mobile Application Security**

  With the increasing popularity of mobile applications, securing them against potential threats is crucial. Our Mobile Application Security assessment thoroughly examines the security aspects of your mobile apps, including their architecture, data storage mechanisms, communication channels, and integration with server environments. By identifying vulnerabilities specific to mobile platforms, we help ensure the protection of user data and sensitive information following OWASP MSTG methodology.

- **Desktop Application Security**

  Desktop applications play a significant role in various industries and their security is of utmost importance. Our Desktop Application Security assessment focuses on evaluating the security posture of your desktop applications. We analyze the key components, deployment strategies, and communication mechanisms of your desktop applications to identify potential vulnerabilities and protect against security breaches. This assessment helps ensure that your desktop applications are robust and resilient against attacks.

Infrastructure Security

- **External Pentest**

  Our External Infrastructure Penetration Testing service focuses on evaluating the security of your external-facing systems and infrastructure. By simulating real-world attacks from an external perspective, we identify vulnerabilities and weaknesses in your network perimeter, public-facing services, and associated components. This assessment helps you understand potential entry points for external threats and provides recommendations to strengthen your external infrastructure security.

- **Internal Pentest**

  With our Internal Infrastructure Penetration Testing service, we assess the security of your internal systems and infrastructure, including your Active Directory (AD) and Azure environments. By conducting targeted evaluations from an internal perspective, we identify vulnerabilities and weaknesses that could be exploited by insider threats or compromised accounts. This assessment assists you in strengthening your internal security measures, ensuring the integrity and confidentiality of your infrastructure.

- **Cloud Security Assessment**

  Our Cloud Security Assessment focuses on evaluating the security of your cloud infrastructure, specifically targeting leading cloud service providers such as AWS, GCP, Azure and others. We assess the configuration, access controls, data storage mechanisms, and communication channels within your cloud environment. By identifying potential vulnerabilities and misconfigurations, we help you enhance the security posture of your cloud deployments, protecting your critical assets and data.

- **Voice over IP (VoIP) Penetration Testing**

  Our VoIP Penetration Testing service assesses the security of your VoIP infrastructure and systems. We evaluate the architecture, configuration, and communication channels of your VoIP environment, including its integration with your network infrastructure. By identifying vulnerabilities specific to VoIP technologies, we help you mitigate potential risks, safeguard the confidentiality of your voice communications, and ensure the overall integrity of your VoIP infrastructure.

- **Wi-Fi**

  Our Wi-Fi Security Assessment focuses on evaluating the security of your wireless network infrastructure. We examine the deployment, configuration, encryption protocols, access controls, and authentication mechanisms of your Wi-Fi network. By identifying vulnerabilities and weaknesses, we help you strengthen the security of your wireless infrastructure, ensuring that unauthorized access or data breaches are mitigated.

- **Vulnerability Assessment**

  During the vulnerability assessment, we will utilize Nessus, NMAP, and other common tools to conduct an automated scan. These tools will help us identify and analyze potential vulnerabilities in the network infrastructure, systems, and applications. The results obtained from the scan will be used to generate comprehensive reports and recommendations for enhancing the overall security posture.

Social Engineering

- **Phishing Campaigns**

  Our Phishing Campaigns service focuses on assessing the vulnerability of your organization to phishing attacks. We simulate and execute targeted phishing campaigns to evaluate the effectiveness of your security measures and the response of your employees. By emulating real-world phishing techniques, such as deceptive emails, malicious links, or spoofed websites, we gauge the susceptibility of your staff to phishing attempts. This assessment helps identify potential weaknesses in your organization's defense against phishing, allowing you to implement targeted solutions and enhance your overall security posture.

- **Awareness training**

  Our Awareness Training service is designed to educate your employees about the risks associated with phishing attacks and other cybersecurity threats. We provide comprehensive training programs that cover topics such as recognizing phishing emails, identifying suspicious websites, and adopting secure online practices. By assessing your organization's specific needs and web applications' key components, we tailor the training to address your unique challenges.

The 3 Ways to Perform a Pentest

Black Box Test

Penetrating the system with limited access and information, simulating an attack as a site user or a collaborator of the company.

Grey Box Test

Penetrating the system from the outside with a limited amount of information on the organization and its information system. Simulation of an attack as a site user or a collaborator of the company.

White Box Test

The penetration tester has all the information about the system, including the source code. He works and collaborates with the organization technical team in order to detect as many vulnerabilities as possible.

Deliverables

- A detailed report outlining the findings of the penetration test, including identified vulnerabilities and recommendations for remediation.
- An executive summary of the report that provides an overview of the findings and recommendations in a format suitable for executive review.
- A debrief session with the customer to discuss the findings and recommendations and answer any questions the customer may have.

Contact Details

CRT@checkpoint.com