Penetration Testing:
# 5 Questions Every Business Should Ask

CES Penetration Testing Service identifies and exploits vulnerabilities in a business network to understand the impact on confidentiality, integrity, and availability of information systems and provide recommendations to mitigate associated risks.

Challenge

Left and right, increasingly sophisticated cyberattacks are impacting companies' bottom lines, not to mention ruining their reputation. So as a business operating online in any way, do you...

› Test security controls, incident response processes, or network shielding?
› Comply with regulations such as PCI and SOX, or are you looking to ensure that your organization complies with security policies?
› Know every cyber risk your organization is exposed to?
› Understand the vulnerabilities and configuration gaps of your network infrastructure?
› Train employees how to identify the most up-to-date threats

Ransomware attacks rose 250% in 2021 alone, demonstrating just how defenseless teams' networks really were. So, with more problematic and deceptive threats developed daily, how can businesses ensure every far corner of their infrastructure is adequately safeguarded? Especially when your key areas of responsibility probably look like...

The Map of Cybersecurity Domains
Henry Jiang | Maarch 2021 | REV 3.0
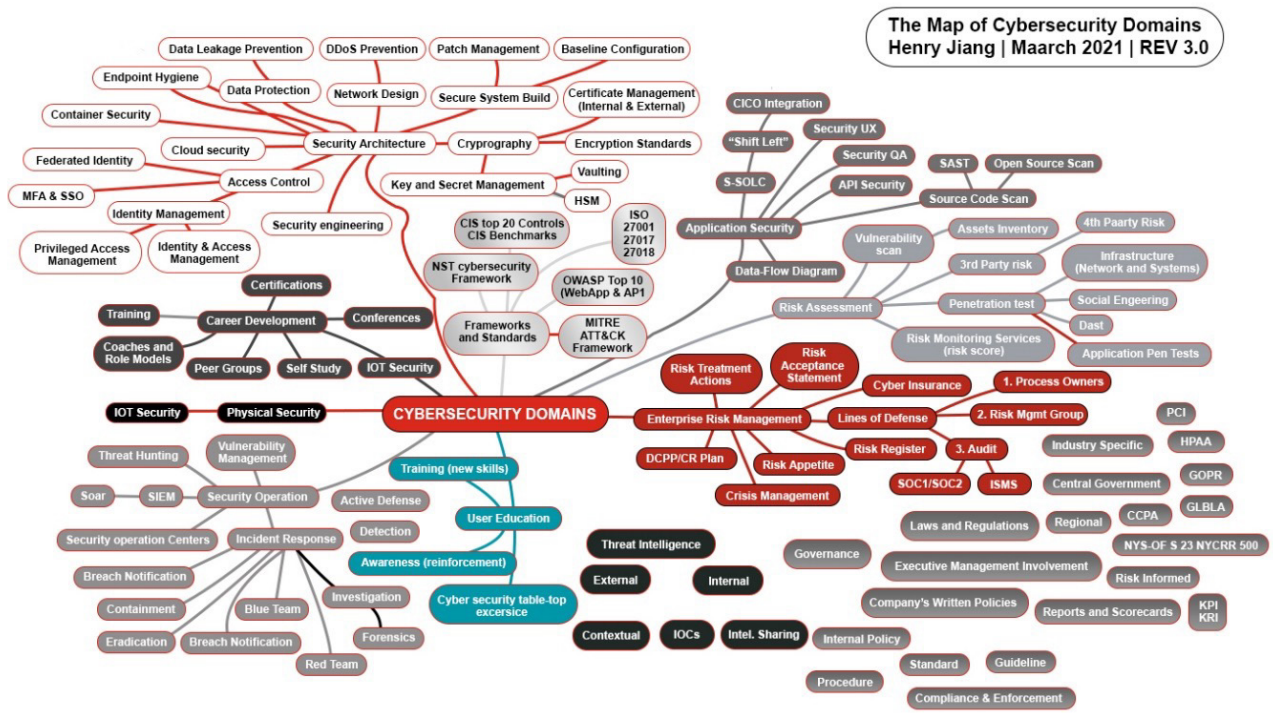
The Solution

With the average cost of a ransomware attack on a business being $133,000, minimize risks and protect employees, systems, and data using Penetration Testing from Claro Enterprise Solutions. Using our solution, teams can quickly identify and exploit vulnerabilities found on your system, understand the impact on confidentiality, integrity, and availability of the data systems, and provide suggestions to mitigate any potential risks. Practices that establish and provide a security strategy focused on risks aligning with your business objectives and real-time information concerning the status of the local corporate network for decision making.
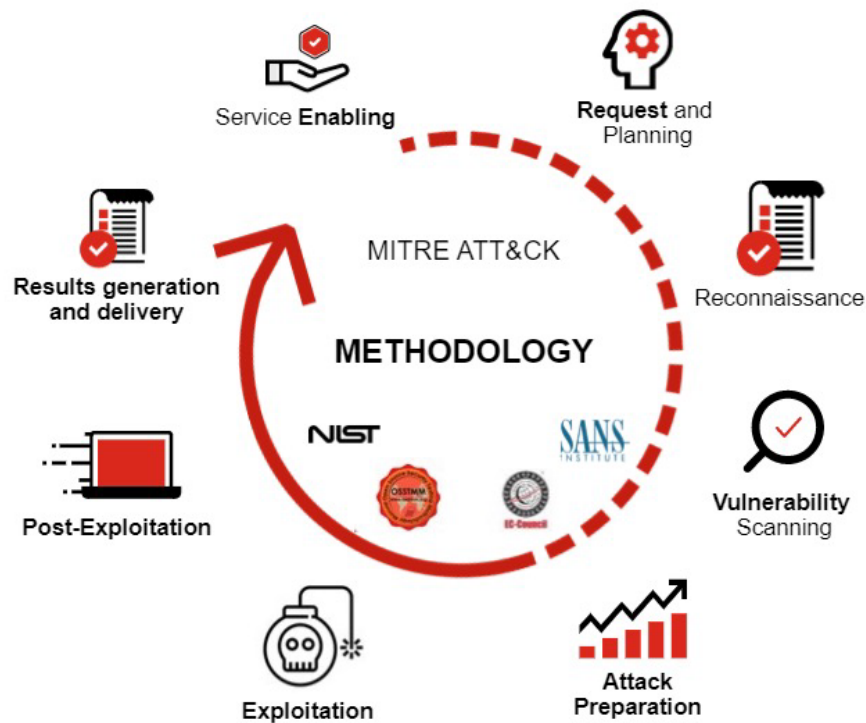
$99.6B by 2027

12.2% CAGR 2021-2027

Benefits

Claro Enterprise Solutions' team of over 600 highly trained cybersecurity analysts focuses on strengthening your information security environment by providing personalized, in-depth analyses of networks plus detailed suggestions for patching possible security gaps. Use our solution to...

> Discover personalized recommendations and methods for patching security gaps to prevent future incidents
> Establish a safe perimeter of the customer's network at all points of contact with the public internet
> Create a security strategy focused on risks and aligned with business objectives
> Have real information on the status of the local corporate network for decision-making
> Reduce economic losses and/or lessen damage to your reputation after a cyberattack
> Eliminate false positives and know which vulnerabilities are truly exploitable
> Validate compliance with security policies regarding people, processes, and technology within your organization
> Access specialized support from over 600 cybersecurity analysts with experience in global security threats
> Gain industry-specific methodologies based on international information security standards
> Utilize over 1,200 certifications, including CISA, CISM, CISSP, CCNA, ITIL, ISO27001, GCFA, CHFI, and more

Claro
Enterprise Solutions