SAGA

A NOVENTIQ Company

GETTING CYBER SECURE WITH PENETRATION TESTING SERVICE

Security
Operation
Service

SECURITY ASSESSMENT SERVICES
PENETRATION TESTING

PAIN POINTS

New types of cyber-attacks evolved into sophisticated, innovative, becoming cheap to conduc

Statutory, contractual requirements, lack of controlover operations by virtue of outsourcing /cloud

Realistic insight on effectiveness of security measures to better understand current exposure, threats & risks, stage of technology updates

Forward-looking strategic planning assumptions when allocating resourcesand selecting products and prioritizing services and initiatives

Exponential growth of data, devices, processing power, algorithms, and networked systems,bringing new risks and vulnerabilities

Protecting access to sensitive information and keeping business processes uninterruptible

Strong cybersecurity strategy with a clear, detailed plan that standardizes security across an organization.

Governmental laws, applicable regulatory & compliance to be strictly followed due to high priced fines and penalties for consumer data breaches

Cybersecurity shifts from a technology -focused to a business-focused discipline. Communicating and influencing key stakeholders across the organization are key attributes in ensuring the success of a defensible security program

SAGA
A NOVENTIQ Company

Security Operation Service

Penetration testing service, (also called pen testing or ethical hacking), provides a systematic process of "real life" test of an exposure to known security vulnerabilities. It determines the extent to which it is susceptible to external / internal attacks.

SOLUTION

Efficient and tangible assessment of the security of information assets, communications, and control infrastructure.

Focuses on network, application, and system vulnerabilities an unauthorized user could exploit from inside and outside of the organization with varying levels of access and information.

Attack scenarios include the ability to view, steal, corrupt, modify, deny access to, or destroy corporate information assets as an "Outsider" with no knowledge of client's operations and as an "Insider" (employee, consultant, or business partner).

Qualified automated and manual penetration tests, proven techniques, methodologies, and tools to detect undesirable risk conditions.

Non-disruptive manner in most cases to the organization, providing valuable insights on its security posture.

Penetration testing service delivered per specific need meeting contractual, regulatory, or corporate governance requirements.

Detailed report on the current security state with steps for remediation for all issues found

Performed by certified pen testers (OSCP and CEH certificates)

SAGA
A NOVENTIQ Company

Security Operation Service

To protect yourself, you should regularly conduct security testing to:

VALUE

- Ensure your existing security controls are effective
- Identify security flaws so that you can resolve them or implement appropriate controlsive
- Gain insight on inadequate or improper configurations
- Be aware on known and unknown hardware or software flaws
- Test new software and systems for bugs; (example: identifies broken access control, with incorrect or incomplete authentication mechanisms, as the leading API exposure)
- Identify operational weaknesses in processes or technical countermeasures
- Support your organization's compliance with security and other relevant privacy laws or regulations (e.g., PCI DSS,HIPAA, GDPR)
- Assure customers and other stakeholders that their data is being protected avoiding the hefty costs and penalties of a data breach
- Identify apps and systems that are impossible to secure or modernize (End-of-Support / End-of Life)
- Could improve an organization's revenues by highlighting redundant services, inefficient processes, and so on
- In merges & acquisitions security testing can help in due diligence stage to gain more information and better insights on cyber risks

SAGA
A NOVENTIQ Company

Security Operation Service

saga.rs