MINIMIZING RISK THROUGH STRENGTHENING YOUR SECURITY POSTURE

TOP OFFERINGS

24X7 MANAGED SECURITY (SOC) / INCIDENT RESPONSE

Security operations powered by MDR/XDR. Including Security Awareness, ongoing testing, and incident response.

RANSOMWARE READINESS ASSESSMENT (RRA)℠

Discover how Nth Generation can safely emulate real ransomware attacks no one else has tested in a replica of your server.

VIRTUAL CHIEF INFORMANTION SECURITY OFFICER (VCISO)

Strengthen your security posture by leveraging Nth Generation's Virtual CISO services – a security brain trust comprised of a tenured Nth CISO team. Our vCISO will collaborate with your team to maximum security with minimal cost and resource allocations.

CYBER INSURANCE READINESS ASSESSMENT (CIRA)

Nth Generation helps organizations achieve superior policies by leveraging the same framework and tools the insurance underwriters are utilizing. We can empower you to shore up the primary security controls necessary to mitigate ransomware and security incidents.

PENETRATION TESTING, RED & PURPLE TEAMING

A comprehensive vulnerability assessment followed by penetration testing, allows organizations to see how vulnerable they are to attacks and steps to improve the security posture. Collaboration between attackers and those managing security counter measures provides a more granular view into the security posture of the organization.

BUSINESS CONTINUITY PLANNING (BCP) & DISASTER RECOVERY

Let our experts guide your strategic method through our business impact assessments to create your business continuity and disaster recovery plan. Nth will help you recognize the threats and risks facing your organization through a series of interviews, and create a solid plan designed to meet your organization's service level objectives.

ASSESSMENTS

ADVANCED PEN TESTING

COMMVAULT ANALYSIS

CYBER INSURANCE READINESS ASSESSMENT

EMAIL SECURITY ASSESSMENT

COMPLIMENTARY CIS CONTROLS ASSESSMENT (FORMERLY "TOP 20")

An Nth Security expert collaborates on every security control that the CIS CSC "Top 20" recommends. A Gantt chart and heat map will be created to help guide your organization's alignment with this valuable framework and best practice.

HYBRID CLOUD ASSESSMENT

DATA RISK ASSESSMENT

PRIVILEGED ACCOUNT MANAGEMENT RISK ASSESSMENT

Privileged accounts including shared, administrative, default and hardcoded passwords are critical attack points found throughout an organization's IT infrastructure. Privileged accounts are exploited in virtually every advanced cyber-attack. Before an organization can begin to manage the risk these accounts present, it is imperative to identify them. Nth Generation will identify these privileged account weaknesses throughout the in-scope environment.

EDR/XDR OVERVIEW / DEMONSTRATION

AI POWERED NETWORK BEHAVIOR ASSESSMENT

CYBER THREAT ASSESSMENT

NETWORK WIRELESS ASSESSMENT

VDI INFRASTRUCTURE ASSESSMENT

REMOTE WORK SECURITY ENDPOINT ASSESSMENT

We're here to help keep your business secure.
For more information call:
800.548.1883

STRATEGIC SERVICES

BUSINESS CONTINUITY PLANNING (BCP) & DISASTER RECOVERY (SEE PG1)

VIRTUAL CHIEF INFORMATION SECURITY OFFICER: (SEE PG 1)

SECURITY FRAMEWORK GAP ASSESSMENT:

Assess security posture based on industry frameworks and provide respective remediation recommendations. Frameworks include: ISO, NIST, CIS CSC, COBIT and ACET.

DOCUMENTATION REVIEW:

Conduct a comprehensive review of policies, procedures, and topology used throughout the environment.

REGULATORY GAP OR READINESS ASSESSMENT:

Document the existing posture and prudently draft remediation plans based on regulations, such as: HIPAA; PCI-DSS; CCPA; NYCRR 500; FFIEC; NCUA; and SOX.

RISK ASSESSMENT:

Document and prioritize the risks affecting the organization. By focusing on the primary risks, organizations can prudently leverage resources.

SECURITY AWARENESS TRAINING:

Conduct end-user awareness training to educate staff on precautionary actions in order to secure the corporations, as well as themselves, from information security threats.

CONTROLS VALIDATION:

A comprehensive assessment of the company's documented controls and validation to ensure the controls are functioning as intended.

SECURITY TESTING

INCIDENT RESPONSE:

Enhance preparedness for future incidents. Nth will assist in developing and/or testing of your incident response plan, enabling the organization to be ready when an incident strikes.

PHISHING:

Email-based attacks are the primary attack vector used to gain a foothold in organizations. Leverage our phishing services to test to see how susceptible the user population is to phishing attacks.

PHYSICAL SECURITY ASSESSMENT:

Have an assessment conducted to determine the quality of your physical security controls between the perimeter and the data center and/or executives.

PENETRATION TESTING AND/OR RED & PURPLE TEAMING (SEE PG1):

Utilizing a blended attack of technical, physical, and social methods, the organization is assessed on their risk of attack vectors.

SOCIAL ENGINEERING (INTERNAL/EXTERNAL):
Remotely, organizations can be tested on their susceptibility to social attacks including telephone and/or email use. On-site engagements can test physical security operations regarding tailgating, ineffective badging, and weak visitor processes.

VULNERABILITY ASSESSMENT:

A comprehensive review of the systems and applications that may contain vulnerabilities exposing an organization. Recommendations for prioritization and remediation are provided.

MANAGED VULNERABILITY AND END POINT PROTECTION SERVICES (STRATEGIC):

Ensure your organization is staying up-to-date with vulnerabilities potentially affecting the organization and mitigate endpoint security concerns with our managed services.

WIFI ASSESSMENT:

Wireless networks extend an organization's network to attack from outside of the physical walls. We will assess the susceptibility to rogue access point injection, guest network isolation, that the countermeasures are functioning properly and the use of appropriate wireless security standards.

TO REQUEST AN ASSESSMENT EMAIL:
assessments@nth.com