Managed Vulnerability and End Point Protection Services:

DON'T JUST INFORM, TRANSFORM

Challenges

- There is a shortage of qualified Cybersecurity Engineers
- Full time, dedicated Cybersecurity Engineers can be costly
- Cybersecurity is not your core competency
- Is your company purchasing or implementing appropriate solutions?
- Were you aware the CIS Critical Security Controls suggests doing weekly vulnerability scanning?
- The California Consumer Privacy Act (CCPA) is coming January 2020!

Solutions

- Nth has a suite of Security Services that provide cutting-edge security products managed by seasoned Cybersecurity professionals who possess an average of 21 years of experience in the field.
- Determine your security vulnerabilities
- Strengthen your security posture and compliance profile
- Leverage advanced AI to actively protect against devastating attacks

Offerings

- Managed Endpoint Protection
- Managed Vulnerability Assessments: Both Internal and External

Offerings

MANAGED ENDPOINT PROTECTION

- Subscription based remote endpoint protection (EPP) management services.
- Endpoints are any machines/computing devices that communicate over a network to access corporate resources.
- Typical EPP products combine antivirus/antimalware, script control, computer memory protection, and device policy enforcement.
- A computer virus is a rogue program designed to damage a computer, exploit vulnerabilities, and/or send out protected information from someone's computer system.
- Malware is a broader term for computer programs that can harm a computer's data or services. Viruses are a type of malware.
- Antivirus and antimalware are defensive cybersecurity applications designed to stop viruses and other malware before they can do any damage.

Reporting

EXECUTIVE OVERVIEW:

Designed for leadership, these reports will review the services at a high, business-impact level, along with recommendations for an improved security posture, as appropriate.

- Summarizes malware detections (ransomware, viruses, worms, and possible other malware).

TECHNICAL DETAIL:

Tailored for engineer or IT-centric employees. This will contain deep, technical drilldowns, along with recommendations for ongoing technical advice.

- List detailed malware detections and actions performed by Nth to resolve.

MANAGED VULNERABILITY ASSESSMENTS:
BOTH INTERNAL AND EXTERNAL

Internal

- Internal facing services such as web apps, email servers and FTP servers.
- Internal only network-attached resources such as servers, network elements, security appliances, desktops/laptops, mobile devices hooked up to the internal network and copiers/printers/projectors and campus physical security connected to the network.
- Private attack service: what every hacker on the Internet can attack if they make it inside the “security perimeter”; what Insider Threats and Advanced Persistent Threats can attack; and what non evil employees, contractors, or temps can accidentally damage.
- Determine a company’s overall exposure to inside attacks especially characterizing efficacy of Defense in Depth, lateral segmentation, or other network defensive architecture attack mitigation (or lack thereof).

External

- Internet facing services such as web apps, email servers and FTP servers.
- Public attack service: what most hackers on the Internet can pummel.
- Determine a company’s overall internet-facing vulnerabilities to global attacks.
- Nth performs the assessments across the Internet the same way a hacker would.

Reporting

EXECUTIVE OVERVIEW:

Designed for leadership, these reports will review the services at a high, business-impact level, along with recommendations for an improved security posture, as appropriate.

- Summarizes the vulnerabilities discovered including overall numbers of vulnerabilities by machines and graphs showing vulnerability counts by Impact Level.

TECHNICAL DETAIL:

Tailored for engineer or IT-centric employees. This will contain deep, technical drilldowns; along with recommendations for ongoing technical advice.

- Demonstrate Trends:
  - Closing of vulnerabilities (aka “security holes”) over time.
  - Opening of new “holes” over time.
  - Can be correlated with infrastructure configuration changes, tech refresh, policy changes, etc. so as to identify risky behavior and modify planning/execution and identify opportunities to inject security requirements into infrastructure change control and more.

NTH PROGRESSIVE RED TEAM SECURITY SERVICES: