Introduction to Protecting Your Network & Meeting Cybersecurity Insurance Requirements

Top Cybersecurity Must-Haves

- Endpoint Security & Antimalware Solutions
- Multi-Factor Authentication
- User Awareness Training
- Effective Backup & Recovery
- Web Filtering
- Secure Video Conferencing
- Incident Response Plan & Dedicated Response Team

Cyber Insurance Preparation

Keeping the attackers and their malware out of the network

- Multi-Factor Authentication (MFA) –Required for access (1) to the network generally, (2) to privileged accounts, (3) to web or cloud-based email, (4) by vendors, and (5) to online backups.
- Patch Management/Patching Cadence (speed especially important with respect to high-severity vulnerabilities)
- Employee Training – phishing training/testing (periodic phishing training with low failure rates)
- Remote Desktop Protocol (RDP) – e.g., remote access controls (VPN, network-level authentication, MFA), firewall configuration
- Presence/management of End-of-Life (EOL) software
- Email/web filtering and response systems – Sender Policy Framework (SPF), DKIM (Domain Keys Identified Mail), DMARC (Domain-based Message Authentication, Reporting and Conformance)
- Microsoft Office 365 – e.g., Data Loss Prevention, Advanced Threat Protection add-on

Cyber Insurance Preparation Continued

Preparing for, responding to, and mitigating an attack

- Backup Practices – use of encryption; maintenance of backups online, offline, onsite and offsite; testing of restoration from backups
- Incident Response/Ransomware Plans – Document your plan with a playbook for a ransomware event; Exercise the plan with realistic table-top exercises; Identify and include your response vendor(s).
- Disaster Recovery/Business Continuity Plans – Recovery Time Objectives (RTO)

Detecting network intrusions and suspicious behavior

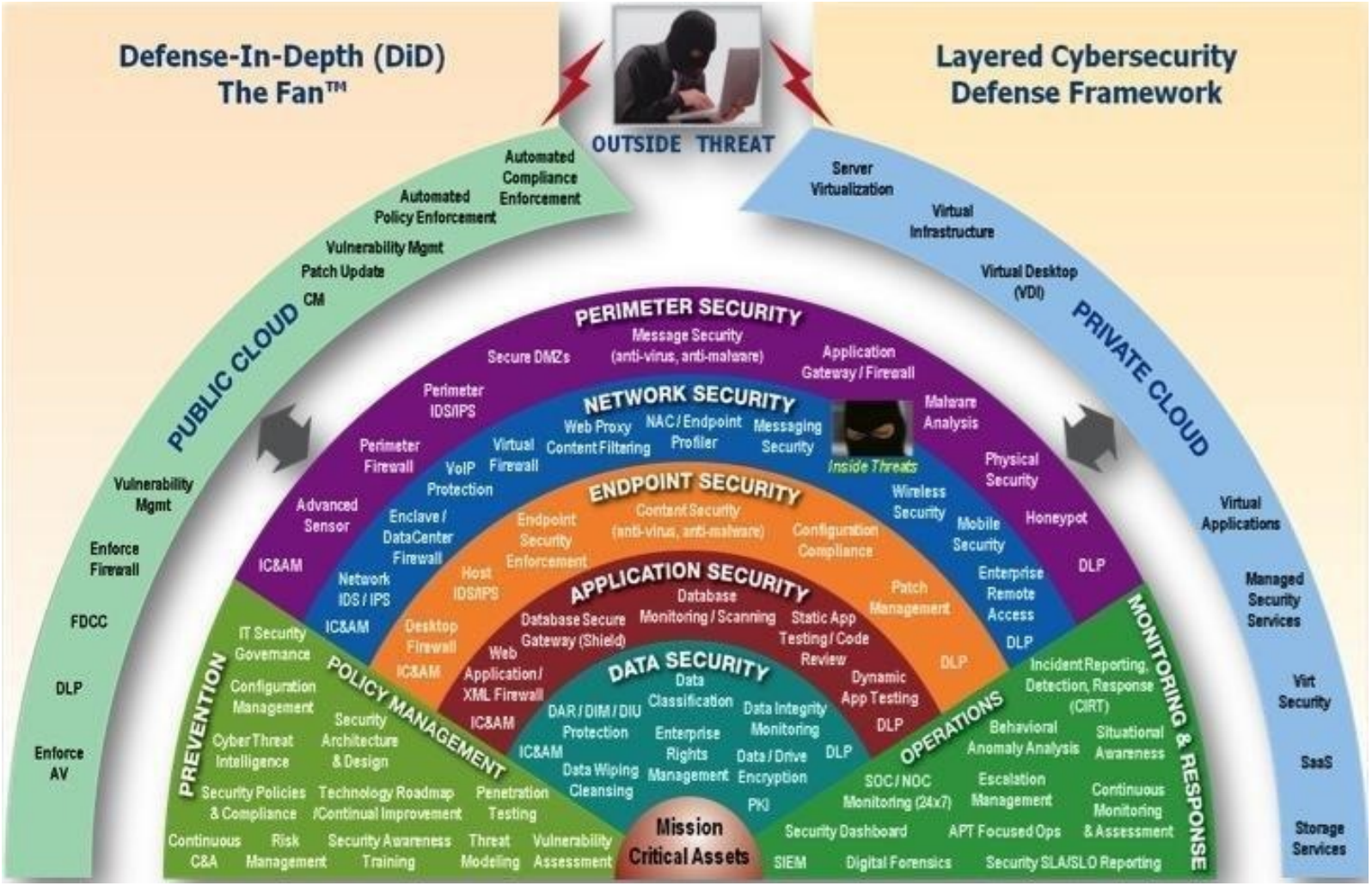
- Endpoint Protection Products (EPP) and Endpoint Detection and Response (EDR) Products
- Vulnerability scans
- Other Endpoint Protection Solutions – such as signature and behavioral-based antivirus products
- Intrusion Detection Systems and Intrusion Prevention Systems
- Security Incident Event Management (SIEM)

Cyber Insurance Preparation Continued

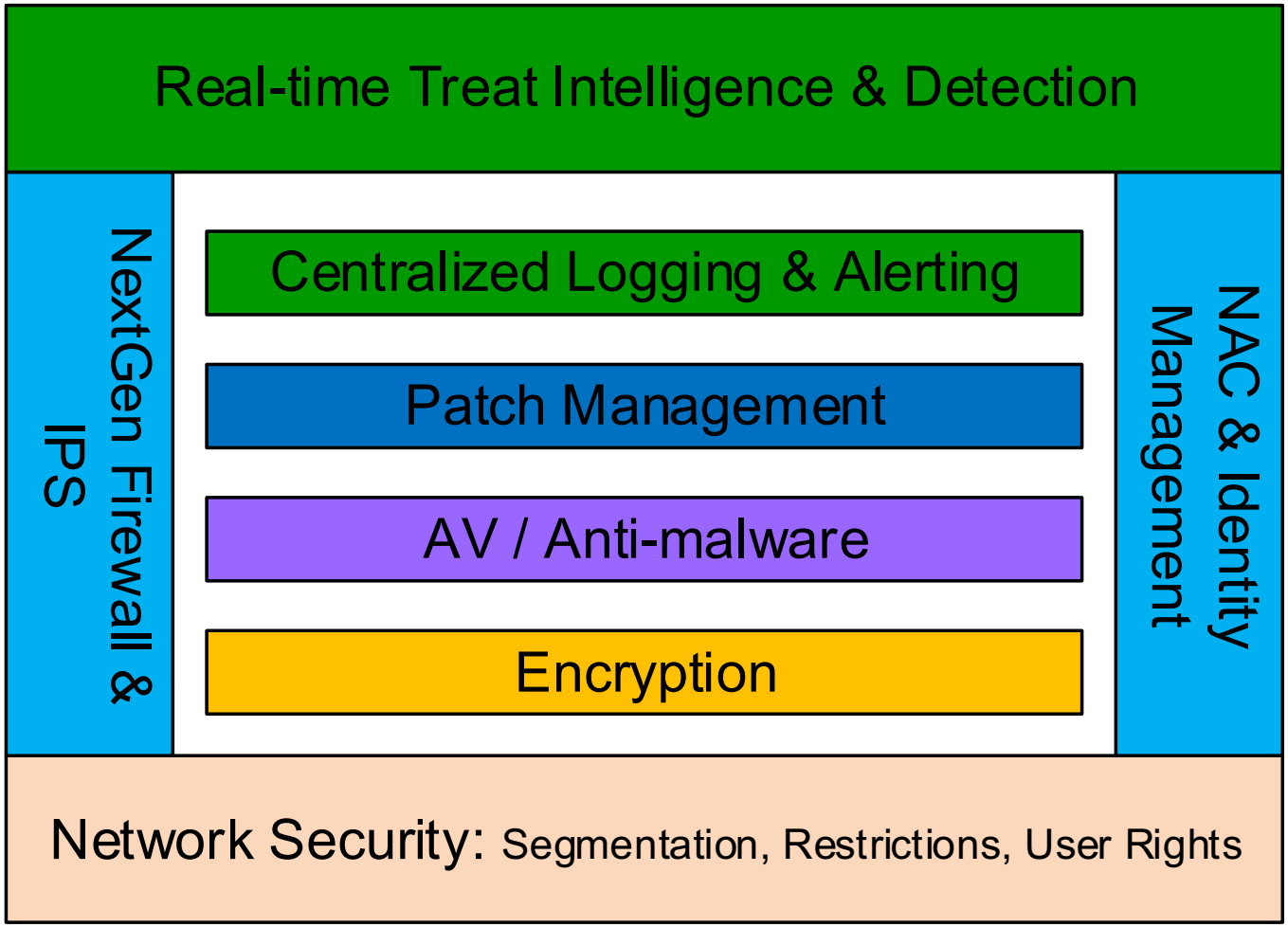
Protecting user and privileged accounts/limiting the attackers' lateral movement

- Identity Access Management (IAM)/Privileged Account Management (PAM)
- Network Segmentation/Segregation
- Configuration Management Practices – hardened baseline configurations
- Service Account Management

Cybersecurity: A Multi-Layered Approach



Multi-Layered Approach (Scaled Down)



Thank You

For more information, or to schedule a meeting with one of our cybersecurity experts, please contact:

Michael Randazza
646-595-6645
mrandazza@promenet.com

Promenet, Inc… A Proud Corporate Sponsor of PAIS

Promenet

AICPA SOC