Let's Agree

"For the agency to protect its full environment it needs to understand its full environment," - CDM program manager at CISA

Cyber attacks are no longer random acts but are targeted based on reconnaissance that determine weaknesses.

- Direct attacks
- Through third party providers

In order to improve cybersecurity, all organizations need

Vulnerability Assessment
Penetration Testing
Threat Intelligence

CyVision
Prioritized Protection

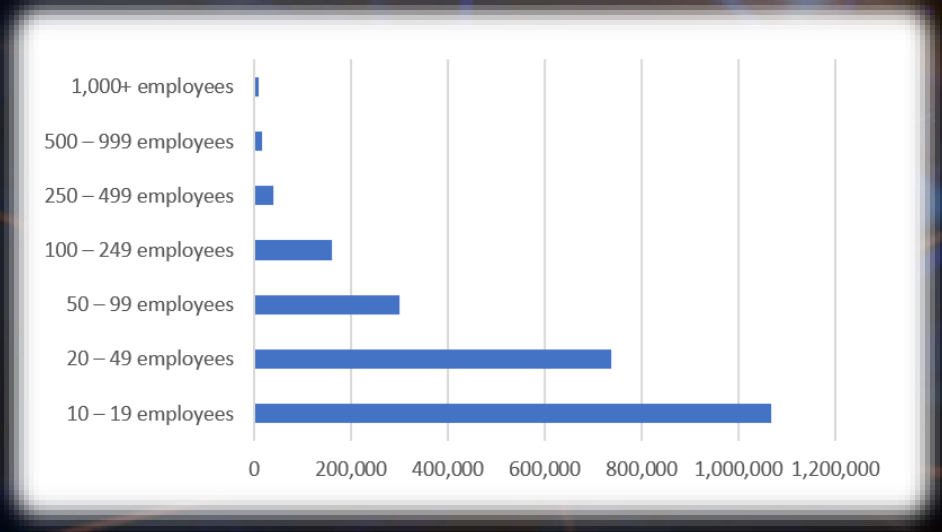
Opportunity

Reality

- 1,000's of environments that are not consistent
- Needs are expanding
- Minimal staffing focused on operations, not security
- Resources and budgets are constrained

Goal

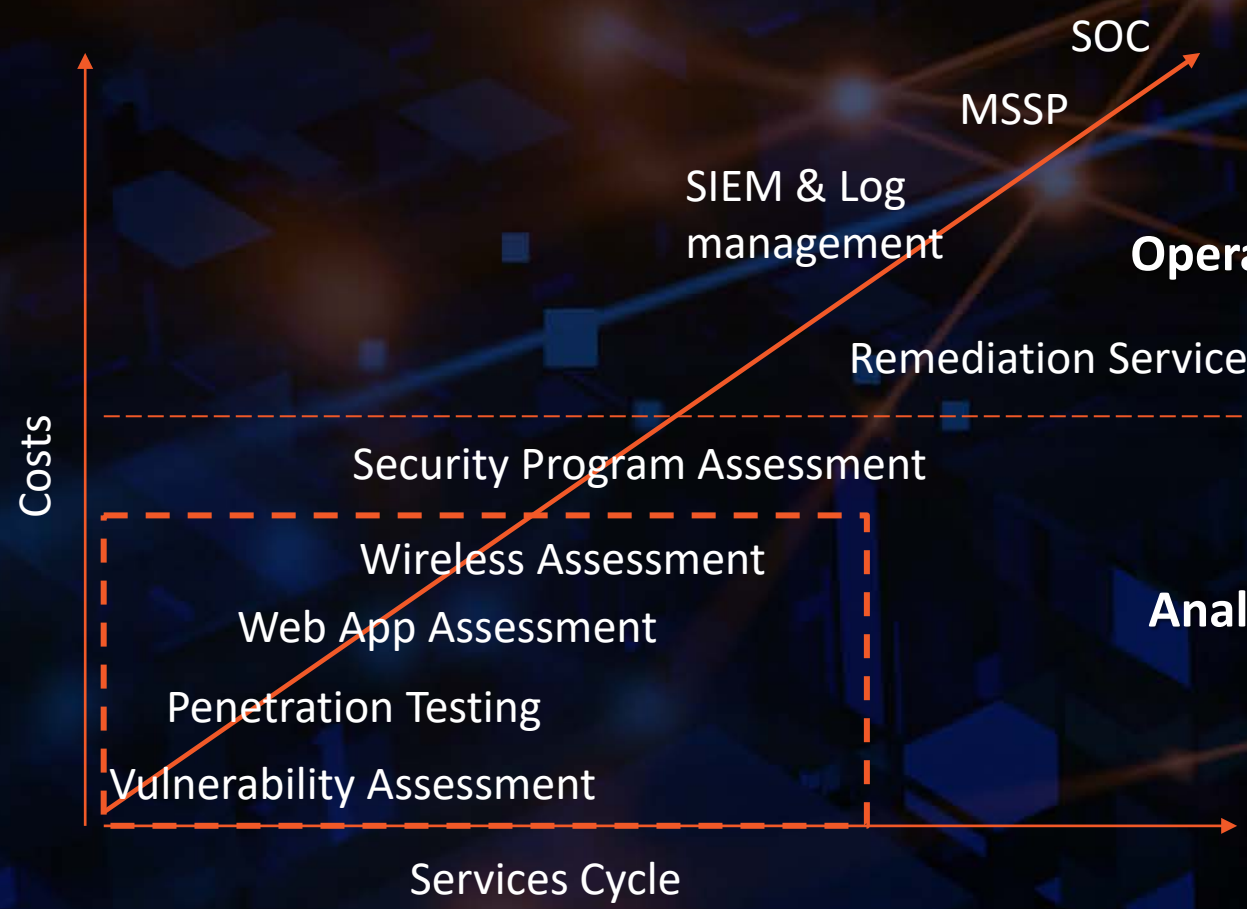
- Consistent results
- Actionable results in a timely manner
- Prioritized reporting based on consequence



Providing value to those "below the cyber poverty line"

CyVision
Prioritized Protection

Where we fit

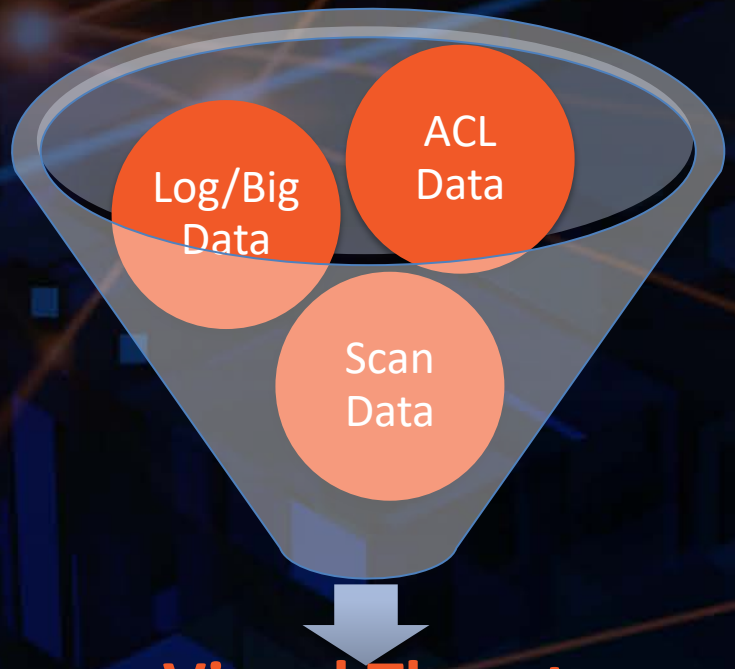


High Tech offerings

Low Tech offerings

CyVision
Prioritized Protection

We analyze the three (3) types of cyber security data common to all networks



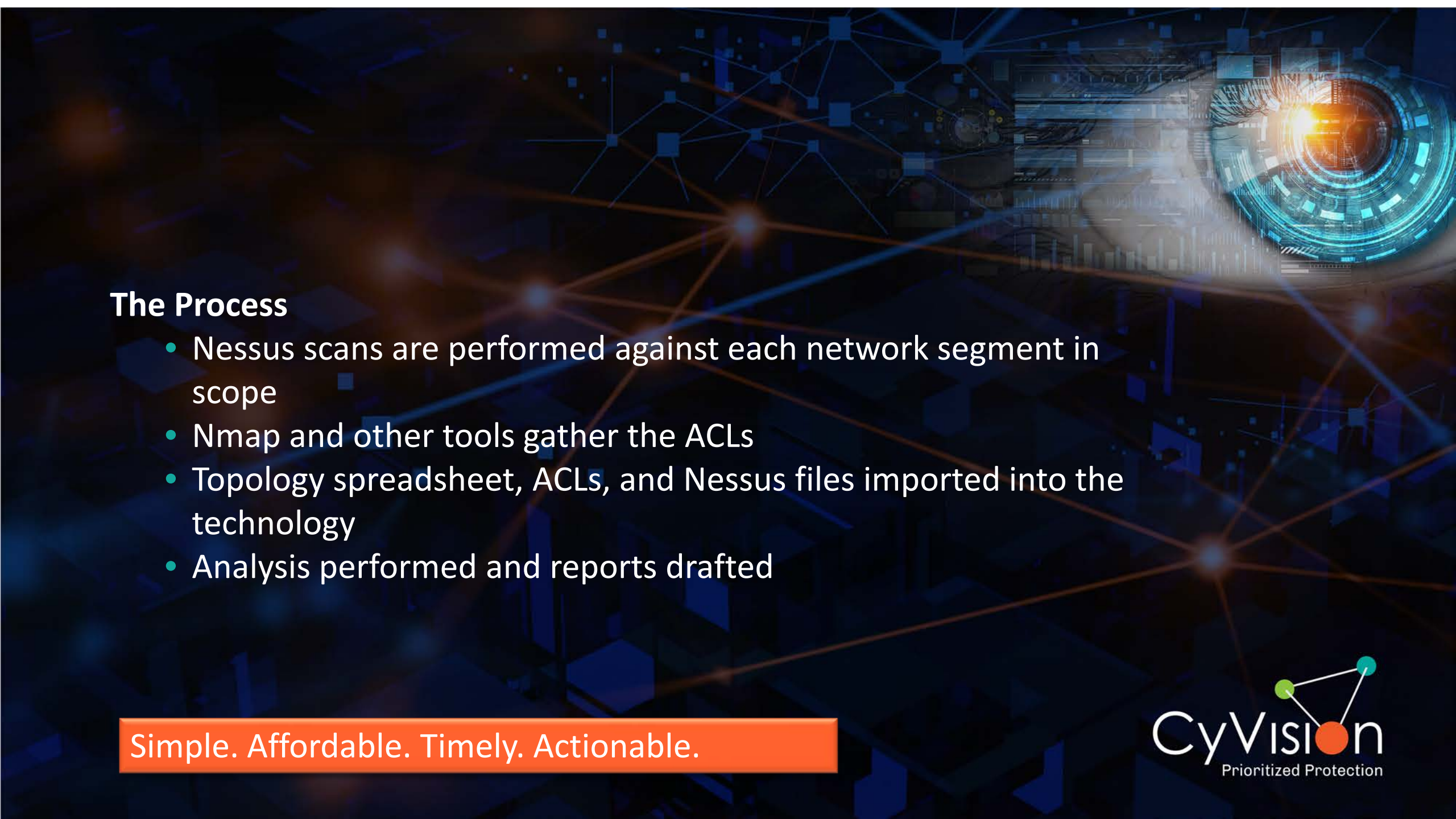
We generate a combined view of vulnerabilities
SMEs make the decisions

Visual Threat Picture

Scan data is information about the endpoint configurations.

Access Control Lists (ACL) is about how the endpoint connect/communicate.

CyVision
Prioritized Protection



The Process

- Nessus scans are performed against each network segment in scope
- Nmap and other tools gather the ACLs
- Topology spreadsheet, ACLs, and Nessus files imported into the technology
- Analysis performed and reports drafted

Simple. Affordable. Timely. Actionable.

CyVision
Prioritized Protection

The Timeline

- Day One – Three
  - Data Gathering
- Day Four – Five
  - Analysis and Report Generation

Summary of Benefits:

- More accurate reports
- Fewer false positives
- Situational Awareness
- Proactive cyber management
- NIST Risk Equation

Actionable results lead to Improve Overall Security

CyVision
Prioritized Protection

VPN Connectivity

- Use organization's VPN solution
- Use small form-factor appliance

Fieldwork

- ACL Collection
  - No access restrictions between VLANs – Faux ACL
  - Obtain ACLs
  - Perform nmap scans within each VLAN to create a simulated ACL
- Vulnerability Scan
  - If necessary, whitelist assessment device IP address (all ports)

Analysis & Reporting

- Six vulnerability rankings
  - Super Critical – Findings with CVSS score of 9.0 to 10.0 with known exploits
  - Critical – Findings with CVSS score of 7.0 to 8.9 with known exploits
  - Severe – Findings with CVSS score of 9.0 to 10.0 with no known exploits
  - High – Findings with CVSS score of 7.0 to 8.9 with no known exploits

Expanded vulnerability rankings for greater insight

CyVision
Prioritized Protection

The Audiences

- CEO/CIO/CISO/The Board
- Remediation & Network Managers
- Remediation & Compliance
- Solution Architects

Additional targeted reports as needed

CyVision
Prioritized Protection

Assessments provide:

- More accurate and comprehensive reporting
- Lower cost basis
- Faster overall delivery of actionable reports

A foundation to work together

CyVision
Prioritized Protection

For More Information Regarding Faith-Based Institutional Cybersecurity Assessments

Contact

- Steven Crummey – steve@cyvisiontechnologies.com
- Jay Conway – jconway@cyvisiontechnologies.com
- Chris Springfield – springfieldc@cphsecuritygroup.com

A foundation to work together

CyVision
Prioritized Protection