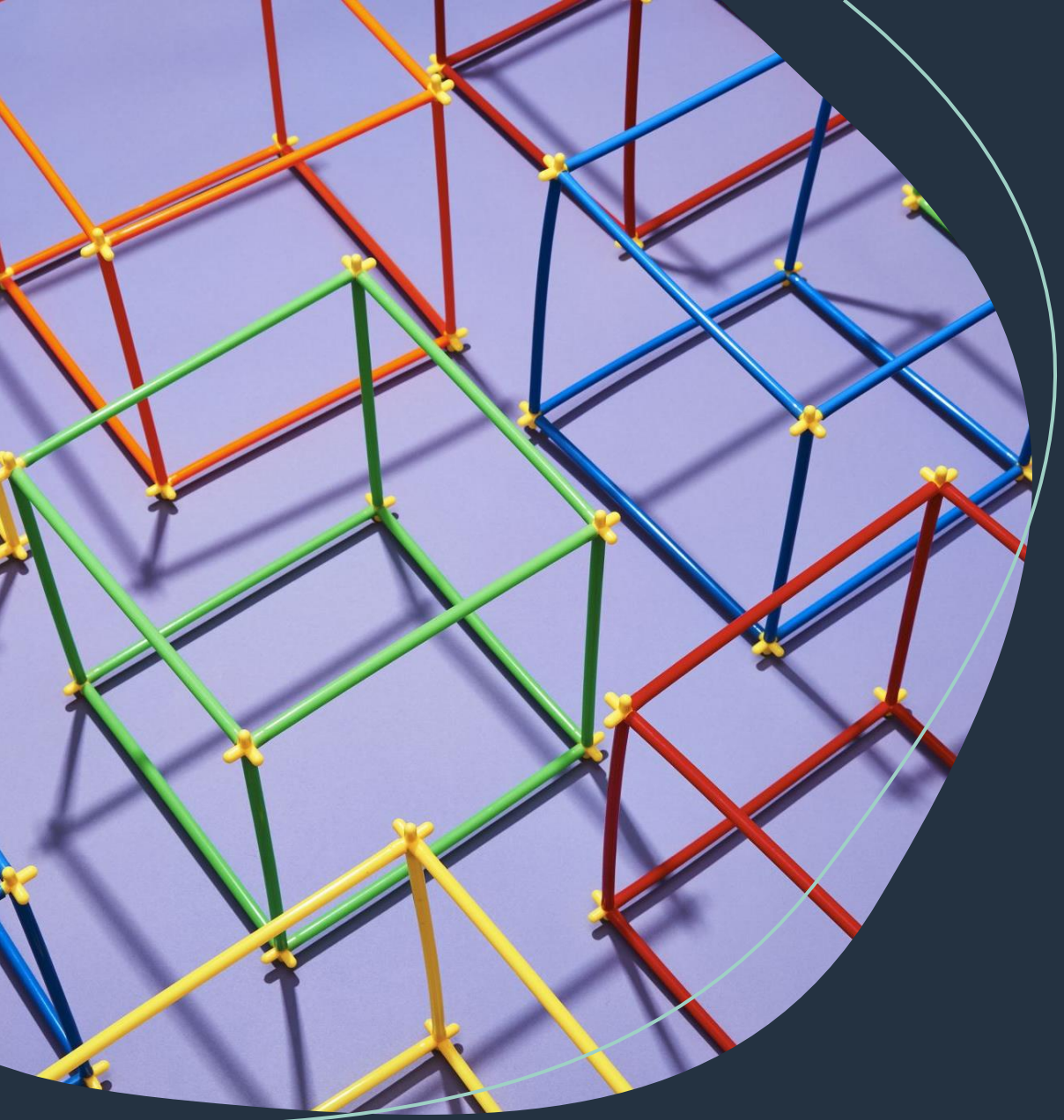
Skeletons in the Closet: Securing Legacy Systems

COISSA Infosec Summit 2024

Michael Miller



Agenda

- Introduction
- What Are Legacy Systems?
- How Did We Get Here?
- Security Challenges
- Other Challenges
- Security Solutions
- Summary

$> whoami

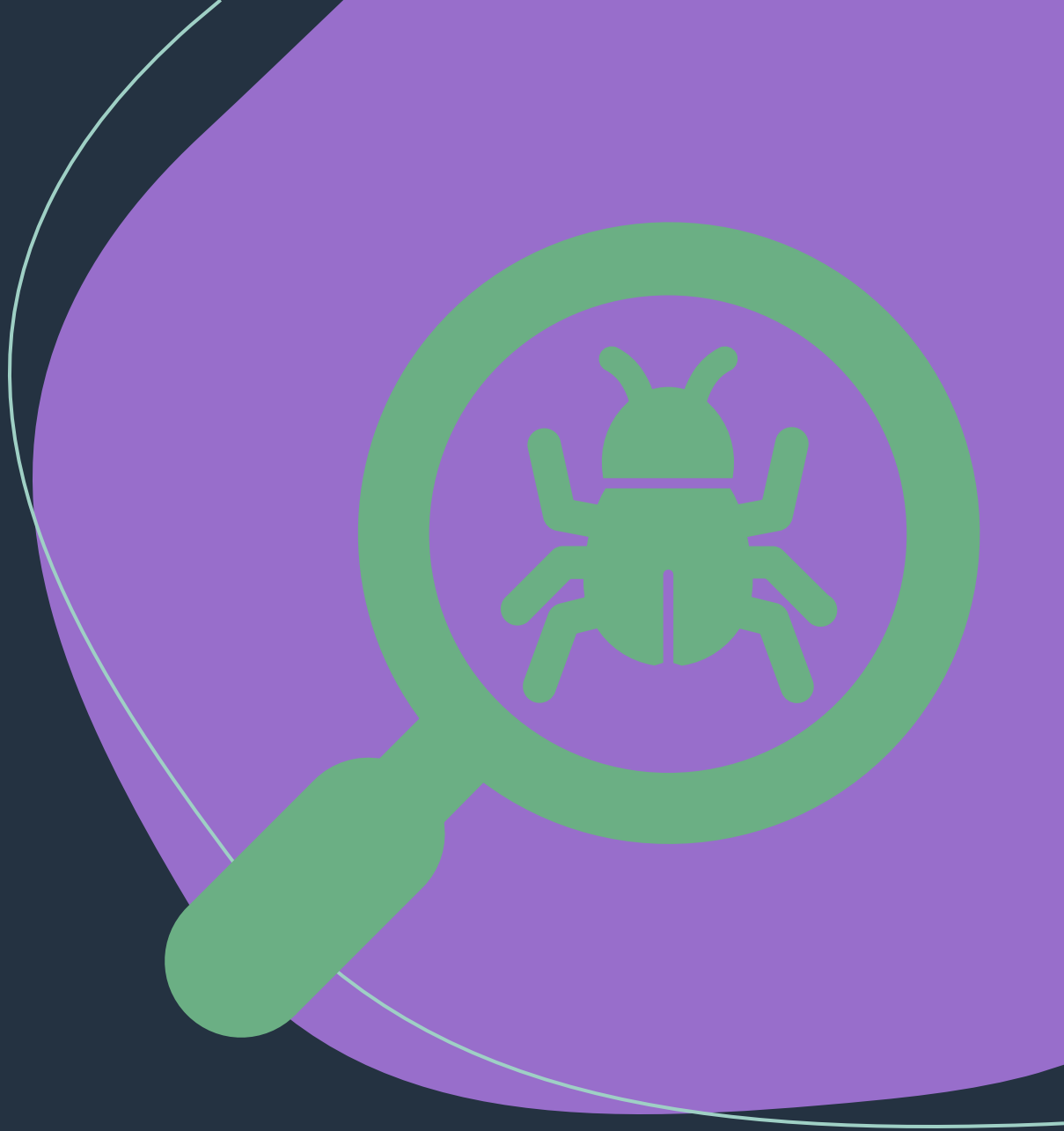
- Manager, Cybersecurity Platform Engineering @ Cardinal Health
- IT/Cybersecurity for 12+ years in a variety of industries
- Worked with companies ranging in size from <$1M ARR to >$200B ARR
- BS Cybersecurity & Information Assurance from WGU
  AAB Network Administration & Computer Programming from NSCC
- CISSP, CCSP, SSCP, GISP, CEH, ECES, CySA+, and many more
- Participate in InfraGard, ISSA, (ISC)2, SANS Advisory Board, NSCC IT Advisory Board, CAMO at NSCC, Adjunct Teacher at NSCC
- I enjoy spending time with my wife and kids, traveling, cooking, public speaking, and tinkering with my home lab

$> who

- Cybersecurity professionals?
- Students?
- Managers/leadership?

What Are Legacy Systems

- End of Life (EoL) Operating Systems
- End of Life (EoL) Applications/Software
- End of Life (EoL) Hardware/Platforms
- Essentially anything that is…
  - No longer supported by the vendor or supplier
  - Cannot be easily replaced
  - Creates risk in the environment



How Did We Get Here

- Ineffective lifecycle management practices
- Insufficient funding to replace
- Fear of change or potential business impact
- Vendor lock in (and lock out)
- Asset depreciation

Security Challenges

- Vulnerabilities
- Insecure Protocols
  - TLS 1.1
  - SMB v1
- Password simplicity
- Compliance with regulations

Other Challenges

- Hardware Support
- Vendor Support
- Incompatibility with other systems

Security Solutions

Upgrade

- That’s it!
- That’s the end of my TED Talk!
- Thanks for Coming!

Seriously though…

Upgrading is the ideal option, just not often the easiest or most viable solution

Upgrade

- Upgrade hardware
- Upgrade operating systems
- Upgrade software

Upgrade

Advantages

- Most effective approach
- Completely eliminates the legacy system

Challenges

- Expensive
- Potential business impact
- Staff resistance to change
- May require entire system/process changes

System Hardening

- Disable/remove unnecessary services
- Enable host-based firewalls and take an “allow only” approach
- Disable and remove unnecessary accounts
- Application allowlisting (AppLocker)

System Hardening

Advantages

- Reduces attack surface of the systems
- Can eliminate risk for vulnerable services if they are disabled

Challenges

- Requires administrative access
- Requires knowledge of required services
- Potential business impact
- Time consuming

Network Segmentation

- Segment systems onto their own VLANs
- Apply filtering rules and access controls to limit the traffic to and from the “Legacy VLANs”
- Consider separate hardware for separation of control
  - Firewalls, routers, or switches

Network Segmentation

Advantages

- Separates systems into controllable groups
- Controls access to and from legacy systems

Challenges

- Communication between systems
- Complexity of management
- Time consuming
- Potential business impact

Internet Isolation

- Block all traffic from the Internet
- Block all traffic TO the Internet

Internet Isolation

Advantages

- Prevents direct access in from the Internet or out to the Internet
- Requires an existing foothold elsewhere to exploit

Challenges

- Sometimes these assets are on the perimeter
- Sometimes they need to access the Internet

Domain Segmentation

- Separate legacy systems onto their own domain
- Allows for modern systems to function on a newer domain level
- Allows for trusts to be implemented to further implement access controls

Domain Segmentation

Advantages

- Separates authentication of assets and systems
- Allows for different functional domain levels

Challenges

- Authentication complications between environments
- Challenging and time consuming
- Probable business impact

Increase Monitoring & Detection Capabilities

Increased Network Monitoring

- NIDS/NIPS
  - Snort
  - Suricata
  - Security Onion
- Zeek Network Security Monitoring
- Premium network detection tools
- Send logs to SIEM

Increased Windows Monitoring

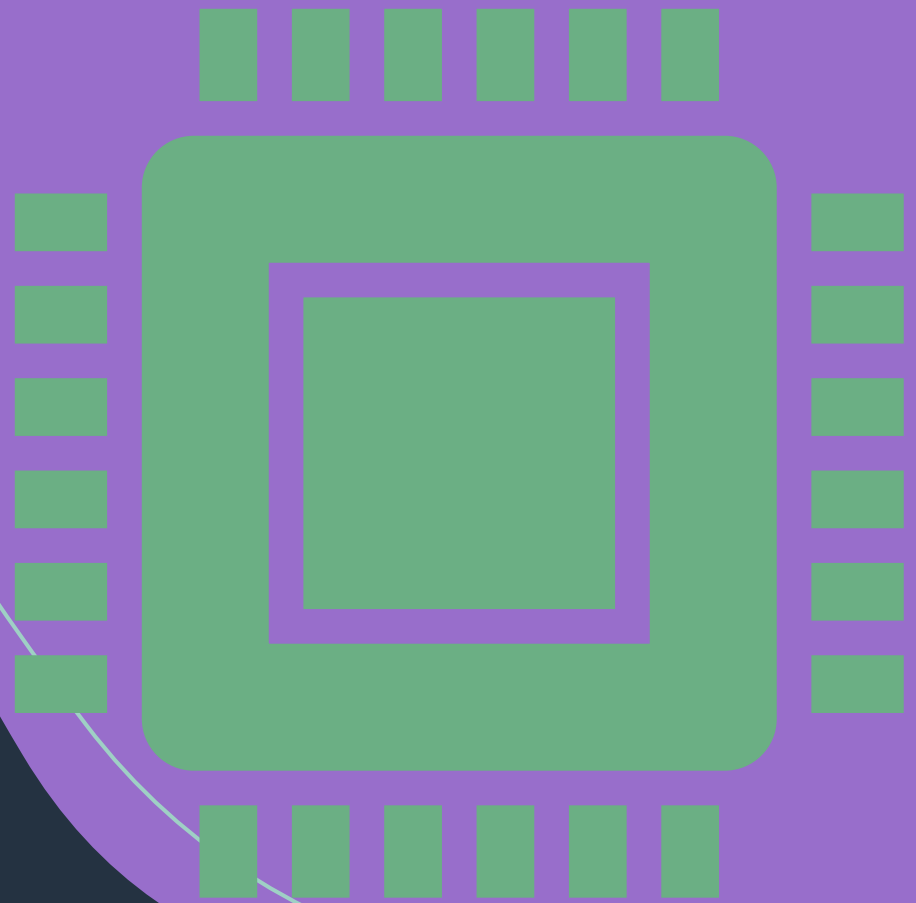
- Sysmon (Windows 7/Server 2008 +)
- OSSEC/Wazuh (XP/2003 +)
- Velociraptor (Windows 7/Server 2008 +)
- Send logs to SIEM

Increased Linux Monitoring

- OSSEC/Wazuh
- Velociraptor (Need to build from source)
- Send logs to SIEM

Summary

- Legacy systems are pervasive in a lot of environments
- These systems present a wide range of risks
- While upgrading is the most effective solution it is usually not the most viable
- System hardening is effective at controlling and reducing attack surface
- Network segmentation and Internet isolation are effective mitigating controls from the network
- Increased network and endpoint monitoring will increase your chances of detecting events



Q & A

- Thank You!