

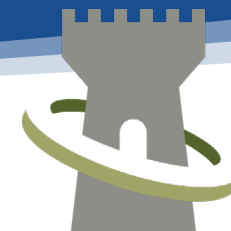
Integration of Network Segmentation within GRC Frameworks

Secure Halo

Richard Osborne – Director of Commercial Services

April 26, 2024

Your Mission Matters



SECURE HALO

SECURING THE ENTERPRISE

A Mission Critical Partners Company

Introduction

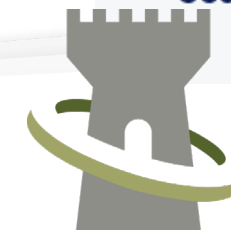
Approved Baseline Certifications					
IAT Level I		IAT Level II		IAT Level III	
A+ CE CCNA-Security Network+ CE SSCP		CCNA Security CySA+ GICSP GSEC Security+ CE SSCP		CASP+ CE CCNP Security CISA CISSP (or Associate) GCED GCIH	
IAM Level I		IAM Level II		IAM Level III	
CAP GSLC Security+ CE		CAP CASP+ CE CISM CISSP (or Associate) GSLC CCISO		CISM CISSP (or Associate) GSLC CCISO	
IASAE I		IASAE II		IASAE III	
CASP+ CE CISSP (or Associate) CSSLP		CASP+ CE CISSP (or Associate) CSSLP		CISSP-ISSAP CISSP-ISSEP	
CSSP Analyst		CSSP Infrastructure Support		CSSP Incident Responder	
CEH CFR CCNA Cyber Ops CySA+ GCIA GCIH GICSP SCYBER		CEH CySA+ GICSP SSCP CFR		CEH CFR CCNA Cyber Ops CySA+ GCFA GCIH SCYBER CHFI	
CASP Auditor		CASP Manager			
CEH CySA+ CISA GSNA CFR		CISM CISSP-ISSMP CCISO			



Director of Commercial Services



Certified Information
Security Manager.



SECURE HALO

SECURING THE ENTERPRISE

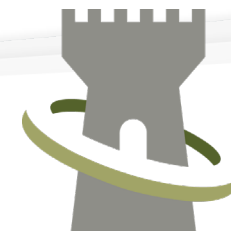
A Mission Critical Partners Company

Your Mission Matters

Discussion Overview

- Relevancy
- Breach History
- Pen-testing Easy Wins
- Lack of Segmentation in Compliance Models
- Credible References
- Interoperability Challenges
- How to Manage
- AI Improvements

Your Mission Matters



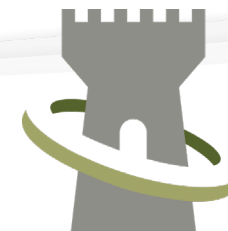
SECURE HALO

SECURING THE ENTERPRISE

A Mission Critical Partners Company

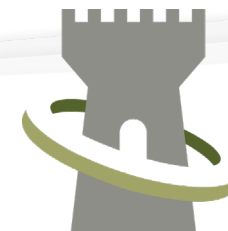
Relevancy

- **Governance:** Network segmentation aligns with governance by ensuring that network management practices adhere to organizational policies and standards. It helps enforce compliance with regulatory requirements and internal policies through controlled access and data flow between network segments.
- **Risk Management:** By segmenting networks, organizations can reduce their risk exposure by isolating critical systems and sensitive data. This makes it harder for malicious actors to access valuable resources and limits the damage in the event of a breach. It also helps in identifying, assessing, and managing risks specific to each segment.
- **Compliance:** Network segmentation supports compliance with various regulatory requirements that mandate the protection of sensitive information.



Breach History

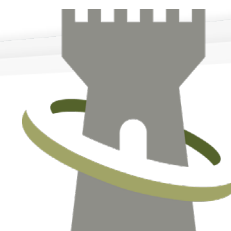
- In 2017 this credit reporting service suffered an exploitation of vulnerability of its Apache Struts servers. Due to the lack of segmentation, attackers managed to travel from unpatched server to unpatched server for 76 days.
- In 2013 this national retailer suffered a data breach from lack of segmentation between its POS systems and HVAC equipment.



Pen-testing Easy Wins

- Mission Critical Communication
- Critical Infrastructure
- Full Compromise of SD-WAN Architecture
- Easy Lateral Movement to Other Networks
- Unnecessary remote access from IOT devices
- VLAN neglect

Your Mission Matters



SECURE HALO

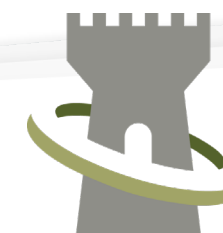
SECURING THE ENTERPRISE

A Mission Critical Partners Company

Networking Tool Display

No.	Time	Source	Destination	Protocol	Info
1	0	192.168.x.1	192.168.x.255	ARP	Who has 192.168.x.2? Tell 192.168.x.1
2	0.0001	192.168.x.2	192.168.x.1	ARP	192.168.x.2 is at xx:xx:xx:xx:xx:xx
3	0.001	192.168.x.2	192.168.x.3	DNS	Standard query 0x0000 A google.com
4	0.0015	192.168.x.3	192.168.x.2	DNS	Standard query response 0x0000 A google.com 216.x.x.x
5	0.002	192.168.x.2	216.x.x.x	TCP	12345 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460
6	0.0025	216.x.x.x	192.168.x.2	TCP	80 → 12345 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460
7	0.003	192.168.x.2	216.x.x.x	TCP	12345 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
8	0.0035	192.168.x.2	216.x.x.x	HTTP	GET / HTTP/1.1 Host: google.com
9	0.004	216.x.x.x	192.168.x.2	HTTP	HTTP/1.1 200 OK
10	0.0045	192.168.x.4	192.168.x.5	SMB	Negotiate Protocol Request
11	0.005	192.168.x.5	192.168.x.4	SMB	Negotiate Protocol Response
12	0.0055	10.x.x.x	Broadcast	TLSv1.2	Vmware who has 192.x.x.x

Your Mission Matters



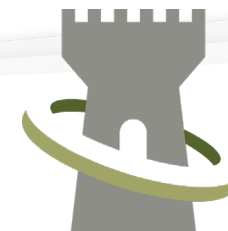
SECURE HALO

SECURING THE ENTERPRISE

A Mission Critical Partners Company

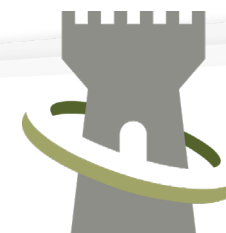
Compliance/Framework/Standards Models Requiring Segmentation

- **CIS (Center for Internet Security):** CIS benchmarks recommend network segmentation to enhance security.
- **FedRAMP/StateRAMP:** These standards for cloud services require network segmentation to isolate sensitive data and systems.
- **HIPAA (Health Insurance Portability and Accountability Act):** Requires safeguards to ensure the confidentiality, integrity, and availability of protected health information, which can involve network segmentation.
- **ISO 27001/2/17:** These standards include requirements for information security management systems, where segmentation can be used as a control to protect information.
- **IEC 62443:** Designed for industrial control systems, this standard includes recommendations for network segmentation to secure industrial networks.
- **NERC (North American Electric Reliability Corporation):** Enforces standards where critical network assets must be segregated from other networks.



Compliance/Framework/Standards Models Requiring Segmentation

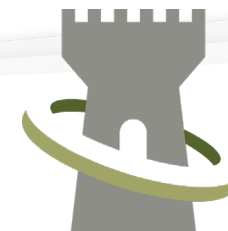
- **NIST 800-171:** Requires contractors to use segmentation to protect Controlled Unclassified Information (CUI).
- **NIST 800-53:** Provides a catalog of security controls for federal information systems, including network segmentation.
- **NIST CSF (Cybersecurity Framework):** While not prescriptive, it includes network segmentation as a recommended practice.
- **NIST Privacy Framework:** Similar to CSF, it can involve network segmentation to protect personal data.
- **PCI DSS (Payment Card Industry Data Security Standard):** Explicitly requires segmentation to protect cardholder data environments.
- **SOC2 (Service Organization Control 2):** This framework for managing data privacy includes network segmentation as a security measure in its Trust Services Criteria.



Compliance models that provide more information

- **PCI DSS (Separation of Credit Card Data)**
 - Payment Card Industry Data Security Standard
- **IEC 62443**
 - International Electrotechnical Commission
- **FFIEC Auditing Guide**
 - Federal Financial Institutions Examination Council
- **NERC CIP**
 - North American Electric Reliability Corporation – Critical Infrastructure Protection

Your Mission Matters



SECURE HALO

SECURING THE ENTERPRISE

A Mission Critical Partners Company

Conditional Access

- **Implementation**

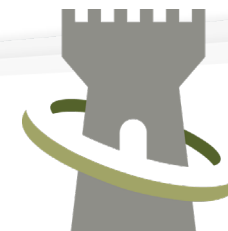
- Device Compliance
- Enrolled Devices
- Static IP

- **Benefits**

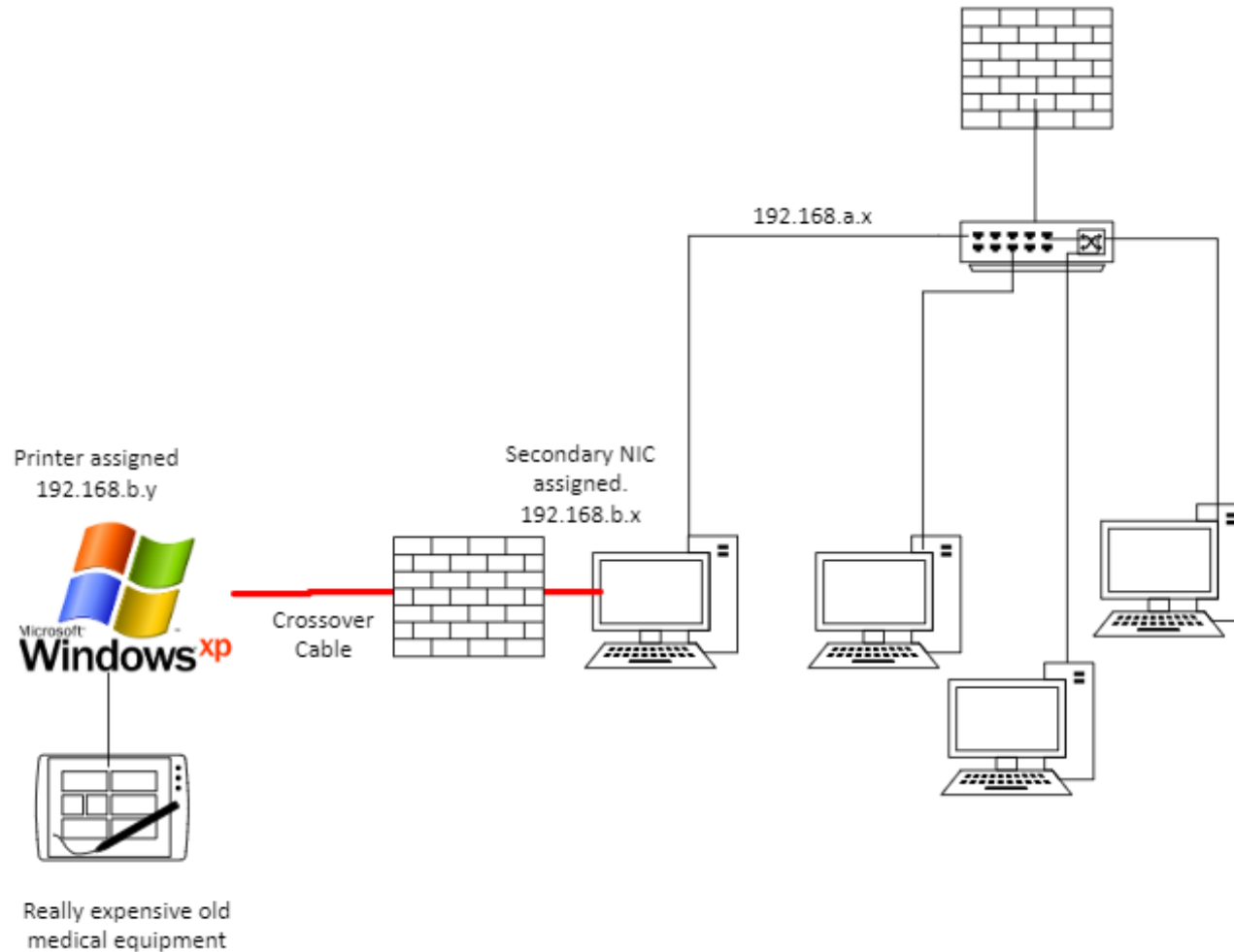
- Enhanced Security Posture
- Increased authentication factor
- Token Theft Mitigation
- Visibility and Control
- Reduced IT Overhead

- **Limitations**

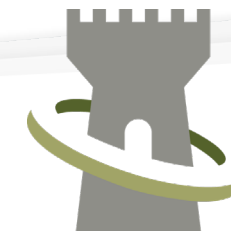
- Budgets
- Environment limitations
- Legacy Systems
- Simplified environments



Supporting EOL Equipment



Your Mission Matters



SECURE HALO

SECURING THE ENTERPRISE

A Mission Critical Partners Company

Interoperability Challenges

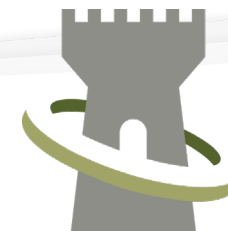
- **NGFW Capabilities**

- Application Awareness
- Integrated Intrusion Prevention (IPS)
- Advanced Threat Protection
- SSL Inspection
- Identity and Access Management
- Centralized Management

- **Features lost with mismatched hardware**

- Enhanced Network Visibility
- Segmentation and Micro-Segmentation
- Improved Traffic Steering
- Enhanced Threat Intelligence Sharing
- Automated Response Capabilities
- Consolidated Policy Management

Your Mission Matters



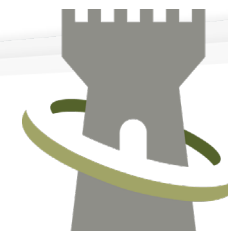
SECURE HALO

SECURING THE ENTERPRISE

A Mission Critical Partners Company

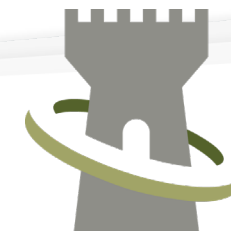
How to Manage

- Device Criticality and Interdependencies Assessment
 - (This means IT needs to talk to other departments)
- Define Security Zones
- Implementation of Access Control Lists (ACLs)
- Use of Firewalls and Segmentation Gateways
- Monitoring and Incident Response
- Validation and Testing
- Documenting Changes and Rationale
- User Access Management
- Compliance and Regulatory Considerations
- Training and Awareness
- Segmentation Performance Impact



AI

- Cisco DNA Center: Automates network management and integrates security policies using AI-driven insights for enhanced network visibility and control.
- Arista Networks - Cognitive Networking: Uses machine learning to automate network operations and optimize performance in real-time.
- VMware - VMware NSX: Provides a virtual networking and security software platform that utilizes AI to facilitate micro-segmentation and streamline data center operations.
- HPE - Aruba Networks: Offers AI-powered solutions for securing and optimizing network operations, focusing on user and device behavior analytics.
- Fortinet - FortiAI: Deploys deep learning AI to autonomously identify and classify threats in network traffic to enhance security postures.
- Palo Alto Networks - Cortex: AI-based continuous security platform that automates threat detection, investigation, and response across network, endpoint, and cloud environments.
- Nvidia - Nvidia AI Enterprise: An AI software suite designed to accelerate AI workloads on Nvidia-certified infrastructure, enhancing network operations and analytics.
- IBM - Watson AIOps: Uses AI to automate IT operations, helping to predict and prevent IT issues by analyzing data across various IT environments.
- Splunk - IT Service Intelligence: Employs AI and machine learning to monitor and analyze IT services and infrastructure, ensuring performance and security.
- Check Point Software - Check Point Infinity: A comprehensive security architecture powered by AI, designed to prevent sophisticated network and IT threats across all user environments.

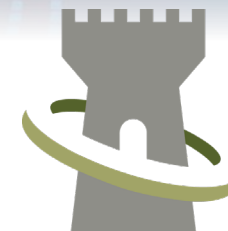


Richard Osborne
Director of Commercial Services
rosborne@securehalo.com

Direct: 202-893-9545

THANK YOU
Questions / Comments

Your Mission Matters



SECURE HALO

SECURING THE ENTERPRISE

A Mission Critical Partners Company