

38th Engineering Squadron

Plan, engineer, implement, assess, and restore

AF cyber capabilities throughout the cyberspace domain



38 ES / ENCS

Cyber Readiness Assessment Team





Overview



- **Services**
 - **Assessment**
 - **CCRI Areas**
 - **Report and Remediation**
- **Request for assistance**
- **Contact**
- **Deliverable Samples**



Assessment



- **In-house developed automated tools**
- **Command Cyber Readiness Inspection (CCRI) areas**
 - Internal network (switch, router and other infrastructure devices)
 - ACAS, ESS, DNS (not managed by 561/83/26 NOS)
- **Review applicable STIGs, TASKORD, and/or OPORD with local Subject Matter Experts**
- **NIPR assessment (remotely)**
- **SIPR or other network assessment (on site customer funded)**



CCRI Areas



- **Internal Network**
 - Layer 2/Layer 3 Switches/Routers
- **Vulnerability Scan**
 - Assured Compliance Assessment Solution (ACAS)
- **Endpoint Security**
 - HBSS (Host-Based Security System)/ Endpoint Security Solutions (ESS)
 - Microsoft Defender for Endpoint (MDE)
- **Domain Name System (DNS)**



Report and Remediation



- **Course of Action/Mitigation Plan**
- **Remediation assistance upon request (on site customer funded)**



Request for Assistance



- **Request 38 ES support through Air Force Information Network (AFIN) Mission Assurance Center (AMAC)**
 - **Service Request Management (SRM)**
 - <https://eitsm2.us.af.mil/>
 - **Infrastructure: Enterprise Network Assistance**
- **Workload prioritized by AMAC**



Contact



- **38 ES POCs**
 - Courtesy POCs listed below on request submitted to AMAC
- **Phu Tran (Section Chief)**
 - Email: phu.tran.1@us.af.mil
 - Phone: 405-734-8533
- **Will McDonald (Tech Lead)**
 - Email: will.mcdonald@us.af.mil
 - Phone: 405-734-8653
- **38 C2 Cell (Assist RFS Process)**
 - Email: 38es.ewoc.engineeringworkload@us.af.mil



ACAS - Results

Assessment Area	Network Vulnerability Scan				
Concern Indicator	High Risk				
	Total Open	Remain Open	Host Scanned	AVG	Weighted
Critical and High	1665	1665	484	3.44	34.40
Medium	1432	1432	484	2.96	11.83
Low	59	59	484	0.12	0.12

Finding Result	High Risk		3.09
Indicator Override	-		

Scan Name	Good Hosts	Bad Hosts	Critical	High	Medium	Low	Total Scanned	WVI	Access Rate
Total PMO	154	61	43	290	391	41	215	2.14	71.63%
Total Non-PMO	330	30	605	727	1041	18	360	3.54	91.67%
TOTAL (PMO + Non-PMO)	484	91	648	1017	1432	59	575	3.09	84.17%



ESS - Results



Assessment Area	Endpoint Security				
Concern Indicator	Moderate Risk				
	Total Open	Possible	Remain Open	Percentage	Weighted %
Category I	2	57	2	3.51%	35.09%
Category II	17	570	17	2.98%	11.93%
Category III	3	27	3	11.11%	11.11%

Finding Result	Moderate Risk	3.88%
Indicator Override	-	

SUMMARY	RATING
2.1.1 ePO MAINTENANCE BASELINE RELEASE	COMPLIANT
2.1.2-7 ePO Components	COMPLIANT
2.2.2 MCAFEE AGENT DEPLOY. MANDATED USCC MR	NOT COMPLIANT
2.2.3-6 POINT PRODUCT DEPLOY. -MANDATED USCC MR	PARTIAL
2.3 CLIENT MODULE CONFIGURATION	PARTIAL
2.4 ROGUE SYSTEM DETECTION	NOT COMPLIANT
2.5 ROLLUP REPORTING	COMPLIANT
2.6 WHITELISTING	NOT COMPLIANT
2.7 TRAINING	NOT COMPLIANT
OVERALL RATING	NOT COMPLIANT



DNS - Results



Assessment Area	Domain Name System				
Concern Indicator	Moderate Risk				
	<i>Total Open</i>	<i>Possible</i>	<i>Remain Open</i>	<i>Percentage</i>	<i>Weighted %</i>
Category I	12	105	12	11.43%	114.29%
Category II	98	1392	98	7.04%	28.16%
Category III	3	62	3	4.84%	4.84%
Finding Result	Moderate Risk				9.82%
Indicator Override	-				



Internal Network - Results



Assessment Area	Internal Network				
Concern Indicator	High Risk				
	Total Open	Possible	Remain Open	Percentage	Weighted %
Category I	27	107	27	25.23%	252.34%
Category II	45	630	45	7.14%	28.57%
Category III	0	72	0	0.00%	0.00%
Finding Result	High Risk				18.73%
Indicator Override	-				



Sample Findings Report



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	Assessment Report	Rule ▾													
2	Device Name ▾	101163	101165	101167	101169	101171	101173	101175	101177	101179	101181	101183	101185	101187	101189
3	131.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✗
4	131.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗
5	131.	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✗	✓	✗
6	131.	✗	✗	✓	✗	✓	✓	✗	✓	✓	✓	✗	✗	✗	✗
7	131.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✗
8	131.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✗
9	131.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✗
10	131.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✗
11	131.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✗
12	131.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✗
13	131.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✗
14	131.	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✗	✓	✗
15	131.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✗
16	131.	✓	✓	✓	✗	✓	✓	✓	✗	✓	✓	✓	✓	✗	✗
17	131.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗
18	131.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✗
19	131.	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✗	✓	✗
20	131.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✗
21	131.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗
22	131.	✓	✗	✓	✗	✓	✓	✗	✓	✓	✓	✓	✓	✓	✗
23	131.	✓	✗	✓	✗	✓	✓	✗	✓	✓	✓	✓	✓	✓	✗
24	131.	✗	✓	✓	✗	✓	✓	✓	✗	✓	✓	✗	✓	✗	✓
25	131.	✓	✗	✓	✗	✓	✓	✗	✓	✓	✓	✓	✗	✗	✗



Sample Findings Report



	A	B	C	D	E	F	G
1	DeviceName	Rule	Function	Exception	Status	StatusCo	Severi
1544	131	101177	Test-V-101177	FailureException: Command 'spanning-tree' does not have root guard configured on the following swi	Fail		2 low
2422	131	101185	Test-V-101185	FailureException: Command 'ip dhcp snooping vlan' not configured	Fail		2 medium
2424	131	101185	Test-V-101185	FailureException: Command 'ip dhcp snooping vlan' not configured	Fail		2 medium
2862	131	101189	Test-V-101189	FailureException: Command 'ip arp inspection vlan' not configured	Fail		2 medium
2864	131	101189	Test-V-101189	FailureException: Command 'ip arp inspection vlan' not configured	Fail		2 medium
3742	131	101201	Test-V-101201	FailureException: Either 'udld enable' or 'udld aggressive' needs to be enabled globally, or 'udld port' n	Fail		2 medium
3744	131	101201	Test-V-101201	FailureException: Either 'udld enable' or 'udld aggressive' needs to be enabled globally, or 'udld port' n	Fail		2 medium
5722	131	220518	Test-V-220518	FailureException: All 'line vty' configs must be set to organizationally-defined 'session-limit' number if	Fail		2 medium
5724	131	220518	Test-V-220518	FailureException: All 'line vty' configs must be set to organizationally-defined 'session-limit' number if	Fail		2 medium
6822	131	220523	Test-V-220523	InconclusiveException: Base must manually review line vty ACL 'ACL_REMOTE' to determine if IP addr	Inconclusive		3 medium
6824	131	220523	Test-V-220523	InconclusiveException: Base must manually review line vty ACL 'ACL_REMOTE' to determine if IP addr	Inconclusive		3 medium
8142	131	220529	Test-V-220529	FailureException: Multiple findings:: The following ACLs contain deny statements without 'log-input' p	Fail		2 medium
8144	131	220529	Test-V-220529	FailureException: Multiple findings:: The following ACLs contain deny statements without 'log-input' p	Fail		2 medium
9462	131	220535	Test-V-220535	FailureException: Command 'username Shawnc' does not contain 'common-criteria-policy' for passw	Fail		2 medium
9464	131	220535	Test-V-220535	FailureException: Command 'username Shawnc' does not contain 'common-criteria-policy' for passw	Fail		2 medium
14302	131	220557	Test-V-220557	FailureException: No CoPP configuration found. Ensure CoPP class-map exists with valid matching poli	Fail		2 medium
14304	131	220557	Test-V-220557	FailureException: No CoPP configuration found. Ensure CoPP class-map exists with valid matching poli	Fail		2 medium
16062	131	220566	Test-V-220566	InconclusiveException: Base must verify configurations are backed up when changes occur	Inconclusive		3 medium
16064	131	220566	Test-V-220566	InconclusiveException: Base must verify configurations are backed up when changes occur	Inconclusive		3 medium
16722	131	220569	Test-V-220569	InconclusiveException: Model WS-C3750X-24P IOS 15.2(2)E3 is on APL REMOVAL list	Inconclusive		3 high
16724	131	220569	Test-V-220569	InconclusiveException: Model WS-C3750X-48P IOS 15.2(4)E6 is on APL REMOVAL list	Inconclusive		3 high



38 ES Honey Badgers



Questions?

