UNCLASSIFIED

38TH ENGINEERING SQUADRON



Hardening, Standardization, Optimization (HSO)

HONEY BADGERS NEVER QUIT!

UNCLASSIFIED

Hardening, Standardization & Optimization (HSO) – Overview

Partner with base communication squadrons to identify challenges affecting base network performance, analyze CORA technology areas and provide remediations where possible

Identifies vulnerabilities that exist and provides remediation steps to improve posture

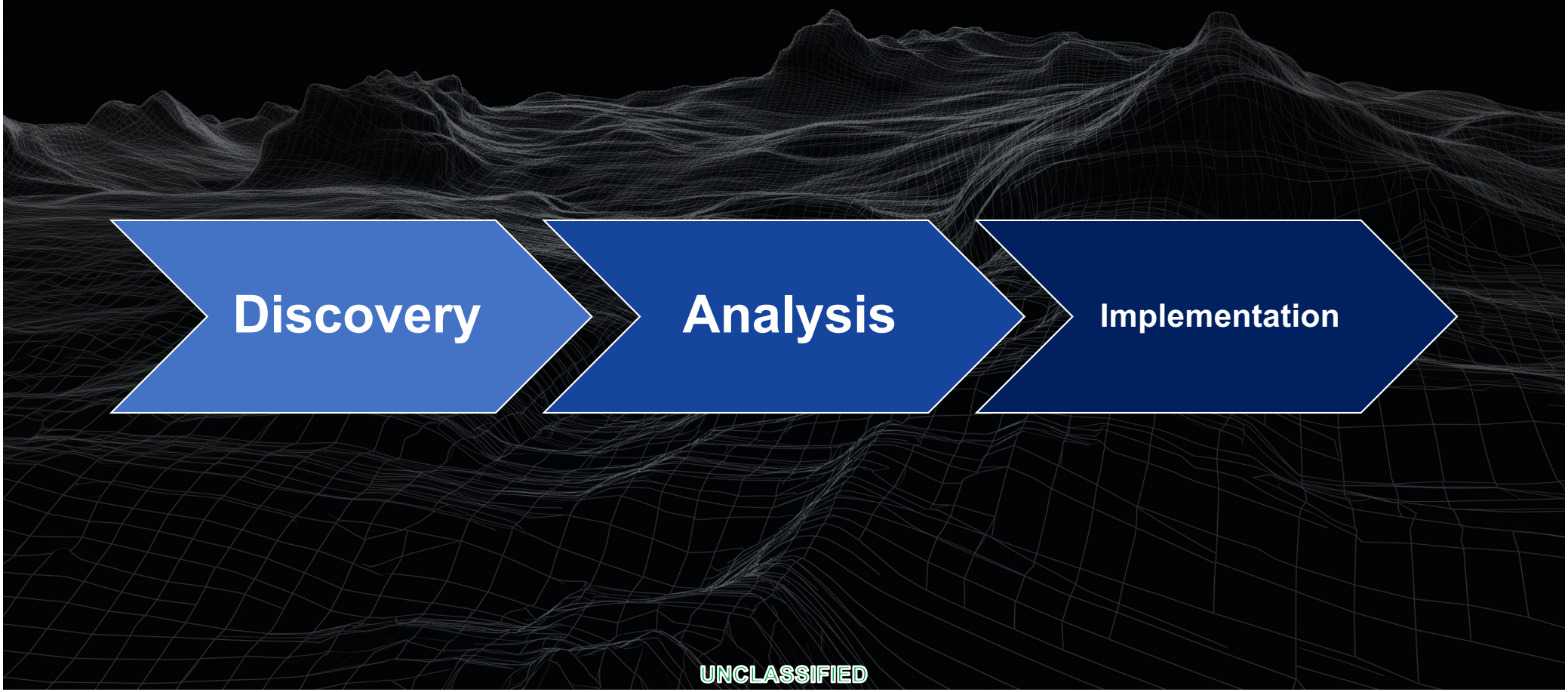
Delivers definable network performance

Creates standard configuration which enables troubleshooting

Improves network robustness and availability

Delivers valuable data to mission partners

Three phases of HSO



HSO Discovery

Partner with base communication squadrons to identify challenges affecting base network performance

Establish a “jump-box” on the NIPR internal network management VLAN and perform remote discovery (Solarwinds)

SIPR/JWICs discovery must be completed onsite and requires a customer funded TDY

Leverage custom-developed scripts to run more than 100 show commands per device on internal network infrastructure

Once the configuration files are captured, another custom script is run to parse/clean the data for human consumption & analysis

All the files and configuration data is uploaded to an internal Teams page

Partner with Vulnerability Analysis section to check configuration compliance with DISA STIGs

HSO Analysis: Areas of Concern

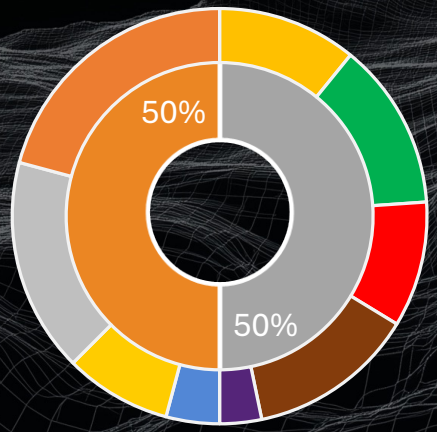
- Hardware Models (Identify EoL/EoS Equipment)
- Software Version
- Half Duplex / HAIPE Ports
- Spanning Tree (Root)
- NTP Status
- VLAN Naming
- Unauthorized or unknown 802.1x sessions
- POE Usage & Percentages
- Bandwidth Utilization History
- Ports in VLAN 1
- CDP/LLDP/MLDP
- Devices that refuse SSH connections
- ISE
- IP Scheme

UNCLASSIFIED

Scoring Methodology

Orders / Directives/ Policies (ODP)

- **Weight 5**: Cyber Defense Monitoring, Detect, Response; Cross Domain Solution (CDS)
- **Weight 4**: Network Vulnerability Scans; Endpoint Security
- **Weight 2**: Cybersecurity and resiliency; Insider Threat (SIPR only)
- **Weight 1**: Supply Chain Risk Management (SCRM



Cyber Maintenance

- **Weight 5**: Boundary; Cross Domain Solution (CDS) *Combined
- **Weight 4**: Network Vulnerability Scans; Endpoint Security; Internal Network
- **Weight 3**: Domain Name System (DNS); Traditional Security; Mobility
- **Weight 2**: Internal Web Server; Releasable Networks (REL); Video/Voice Over IP (VVOIP); Internal Database; Exchange; Virtual Infrastructure
- **Weight 1**: Windows Operating System; Unix Operating System; Other

Overrides

- Boundary vulnerabilities tied to Key Indicators of Risk (KIORs) result in a severity override of two levels
  - Example: Moderate Risk → High Risk → Very High Risk
- Internal vulnerabilities linked to Key Indicators of Risk (KIORs) result in a severity override of one level
  - Example: Moderate Risk → High Risk
- Measure indicators linked to Key Indicators of Risk (KIORs) will result in Critical Override that makes the measure receive a “zero” score
- If a mitigation is allowed by the Security Technical Implementation Guide (STIG) or JFHQ-DODIN adjudication process, the override is negated

UNCLASSIFIED

Key Indicators of Risk

Control Access

- Deny by Default Posture
- 802.1x / C2C
- Encryption
- Permissions Management

Detect Anomalies

- Monitor Network Traffic
- Endpoint Security
- CSSP
- Privileged Shell Management
- Network Vulnerability Scan
- Log Review / Monitoring

Minimum Defensive Posture

- Highly Exploitable Vulnerabilities (J2 / ACAS)
- Account Management
- End of Life / End of Support

Mission Assurance

- MRT-C / MADSS
- COOP / Disaster Recovery

Key Indicators of Risk tie directly to CORA scoring through severity and critical overrides impacting CORA scoring and reinforcing the significance of JFHQ-DODIN priorities

HSO Implementation

Once the analysis is completed an After-Action Report (AAR) is generated and communicated to the customer

The customer may request assistance developing a detailed implementation plan and onsite engineering assistance to enact the plan

Depending on the size and complexity of the network a team of 4-6 personnel travel onsite for up to 4 week to implement the plan, TDY is customer funded

Who Does This Support?

Base Communication Squadrons and base mission systems
- RFS (Service NOW)

Other 38 ES Flights/sections (ENO, ENP, ENII)

16 AF, 688 CW, or MAJCOMs

Performance Monitoring Teams

Counterfeit equipment taskforce

IPv6 and Zero Trust implementation

TASKORDs:

Jumpbox

Duplex

Operation Epic Fury

BadgerWare / HoneySuite

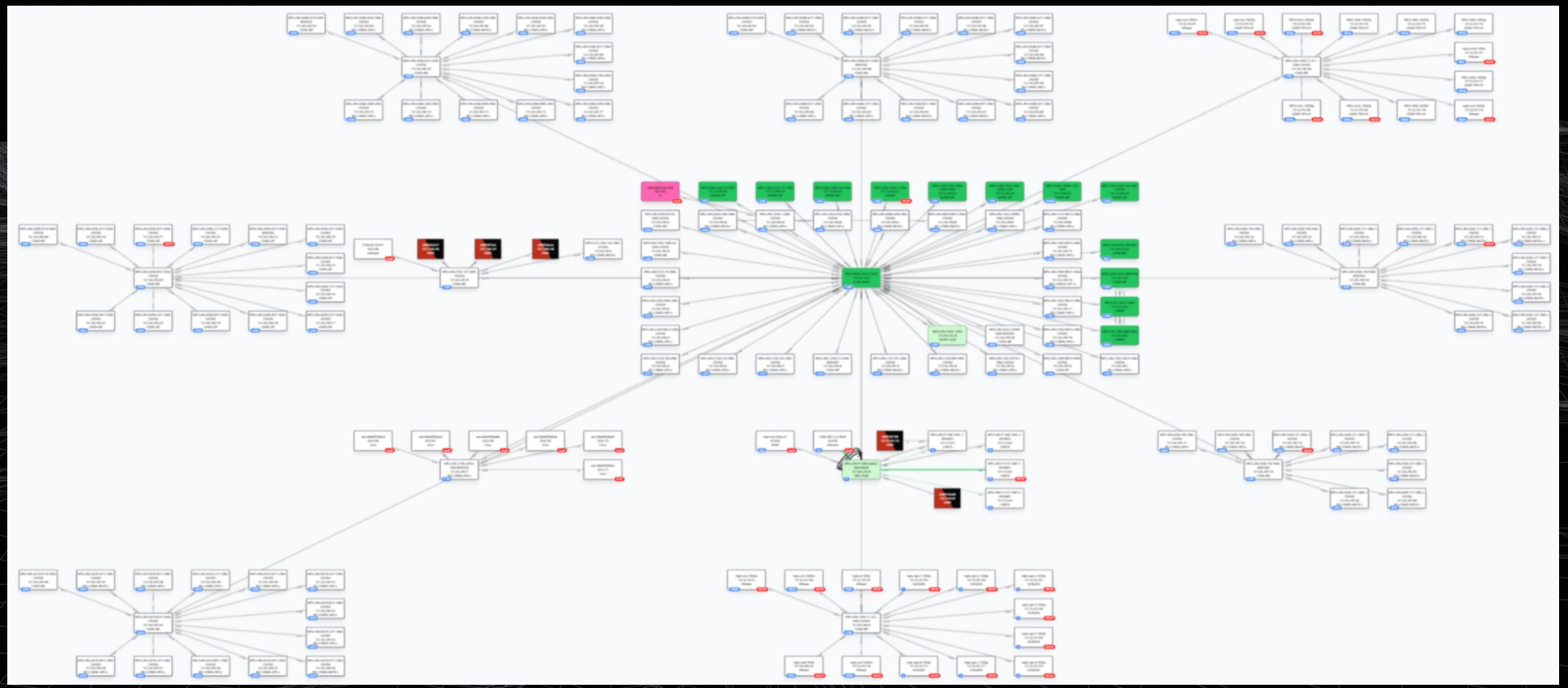
The 38 ES tool automates the discovery, mapping, and technical evaluation across network and virtualized enterprise infrastructure layers.

- **Topology Mapping:** Generates high-fidelity, interactive logical network topology.
- **Compliance Audits:** Conducts DISA STIG evaluations for network infrastructure, VMware Hypervisors, Hosts, Machines and Management Software.
- **Configuration Audits:** Executes BAN-FS compliance evaluations to standardize and optimize enterprise network infrastructure configurations
- **Safe Remediation:** Produces non-disruptive, tailored configuration scripts to enforce baseline integrity.
- **Dashboarding:** Synthesizes assessment artifacts into the interactive Cyber Readiness Dashboard.

Deliverables

- HoneySuite
- Detailed After Action Report
- Captures (text file), Findings (spreadsheet)
- Network Drawings
- End of Support Device List
- Vulnerability Assessment Report and Score Card (before and after)

Example Deliverables: Network Diagram (HoneySuite)



UNCLASSIFIED

Top STIG Violations

(Accounts for 8.265 of 12.9%)

1	V-237779	5.9246%
2	V-220556	0.7221%
3	V-220649	0.7134%
4	V-253911	0.4524%
5	V-253914	0.4524%

Overall Weighted Score



Worst Devices By KIOR

(Accounts for 113 of Potential KIORs)

1	MPLS-CDN-L1052-108A-ZONE4-4600	23
2	MPLS-CDN-H16000-T124-4300	23
3	MPLS-CDN-L1052-108A-ZONE3-4300	23
4	MPLS-CDN-L1052-108A-ZONE1-4600	22
5	MPLS-CDN-L1030-106-4300-CN1050	22

CAT I (High)

Failed/Open: **1185** of Performed: **7663**

Pass	81.9%
Fail	15.5%
Inconclusive	2.6%

CAT II (Medium)

Failed/Open: **3342** of Performed: **38247**

Pass	84.6%
Fail	8.7%
Inconclusive	6.6%

CAT III (Low)

Failed/Open: **195** of Performed: **4398**

Pass	93.2%
Fail	4.4%
Inconclusive	2.4%

UNCLASSIFIED

Automated Deliverables

Cyber Maintenance Overall Grade

Technology Area	Weight	Impact	Concern Indicator	SO
E Boundary Security	5	-12.5%	Very High Risk	3
S Internal Network	4	-10%	Very High Risk	3
E DNS	3	-7.5%	Very High Risk	3
E Endpoint Security	4	-6%	High Risk	0
S Vulnerability Scan	4	-2%	Moderate Risk	0

Final Risk Rating

56%

High Risk

Vulnerability Scan

1.72 VPH

14026	45355	33840	13652
Crit/High	Medium	Low	Hosts

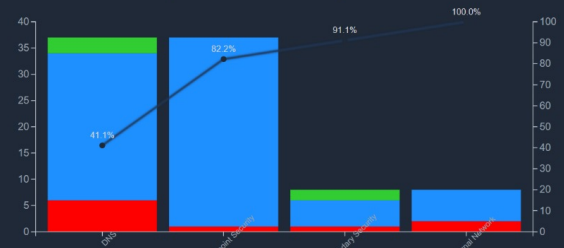
Potential KIORs By Area



ODP Overall Grade

ODP Area	Weight	Impact	Concern Indicator
Network Vulnerability Scan	4	-6%	0.88
		Critical Overrides:	0

Cyber Maintenance Finding Counts



Cyber Maintenance Finding Results

Technology Area	Score	Finding Result	KIOR Categories
Boundary Security	10.83%	High Risk	Encryption, Account Management, Log Review / Monitoring
DNS	12.74%	High Risk	Account Management, Encryption, COOP / Disaster Recovery, Permissions Management, Log Review / Monitoring
Endpoint Security	11.38%	High Risk	
Internal Network	13.52%	High Risk	Account Management, Encryption, 802.1x / C2C, Log Review / Monitoring, Permissions Management
Vulnerability Scan	1.72	Moderate Risk	

Questions

