**RISK MITIGATION PLAN**

*for*

**Mission Partner Name**

*in support of*

**OPERATION NAME**

# (U) EXECUTIVE SUMMARY

|  |
| --- |
| *This section should contain a brief summary of the operation, some refresher info about what a IR Team provides (e.g. “…identify critical missions and associated supporting cyberspace assets”, “perform Cyber Key Terrain (C-KT) analysis”, “risk assessment and recommendations”) and an extremely brief summary of CVA/Hunt style findings.* |

On order IR Team will in accordance with <ORGANIZATION> ensure and improve the readiness of the receiving unit by securing the Cyber key terrain and critical assets for the supported command. This plan is not intended to suplant the current security plan of the supporting unit but enhance the security posture and validate the results of both the current state and the post implementation security compliance.

IR Team will use best practices in the conduct of the assessment. All material results and findings will be recorded and the risk mitigation plan will be completed in compliance with all applicable laws and legal authorities.

# (U) MISSION ANALYSIS

|  |
| --- |
| *This section should contain a mission decomposition and support model (e.g. Dagger) and refined versions of the PDAL and network map. It is intended to highlight the assets that local defenders should focus on, and the various control/enforcement points available to them.* |

## (U) Cyber Dependency Model

----DIAGRAM HERE----

## (U) Prioritized Defended Asset List (PDAL)

(U) In order to preserve the core mission capability that was identified during mission analysis, the following systems and infrastructure devices are the most critical assets to protect. Any efforts to harden defenses, improve monitoring, or restore services in the event of any kind of incident should be directed at these assets first.

|  |  |  |  |
| --- | --- | --- | --- |
| ID | Server/System | Hostname | IP Address |
| A | Domain Controller 1 | DC001 | 192.168.21.83 |
| B | Domain Controller 2 | DC002 | 192.168.21.84 |
| C |  |  |  |
| D |  |  |  |
| E |  |  |  |
| F |  |  |  |
| G |  |  |  |
| H |  |  |  |
| I |  |  |  |
| J |  |  |  |
| K |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| ID | Network Infrastructure | Hostname | IP Address |
| L | Core Router | CORE-RTR | 192.168.6.1 |
| M |  |  |  |
| N |  |  |  |
| O |  |  |  |
| P |  |  |  |
| Q |  |  |  |

## (U) Cyber Key Terrain

----DIAGRAM HERE----

# (U) RISK ASSESSMENT

|  |
| --- |
| *This section should contain an assessment of the overall risk picture for the supported network. It should reflect technical/architectural considerations as well as an intelligence assessment of likely adversary goals. The overall risk assessment is focused on the Prioritized Defended Asset List (PDAL), and informed by the severity of any technical vulnerabilities or personnel limitations, as well as adversary capability and intent.*  *The intent is to communicate the most important risks, and point out specific short and long term mitigations that should be prioritized by local cyberspace defenders. The recommendations should focus on a handful of key priorities that local resources can act on in order to make the biggest dent in their overall risk. It should NOT be an enormous list of Nessus findings!*  *Local defenders may already know about all the things they \*could\* do to harden their network. After mapping the mission and applying an intel-focused assessment though, the value of the IR TEAM may be in helping to suggest what they \*should\* do first given limited time, money, etc.* |

## (U) Risks Identified

(U) Given the current network architecture, system configuration, and intelligence awareness of adversary capability and intent, there are several areas of concern that pose significant risk to the network operational mission.

|  |  |
| --- | --- |
| 1 | Local cyber defenders have no clear asset tracking, incident response plan, or forensic tools |
| 2 | Network traffic is not restricted, even from external networks |
| 3 | Several well-known and easily exploited vulnerabilities exist for all systems |
| 4 | Internal hosts are not standardized or hardened against malicious activity |

These areas of significant risk are discussed in more detail below.

### (U) Risk Mitigation – Network

|  |  |
| --- | --- |
| 1 | Network traffic is not restricted, even from external networks |

(U) Initial network discovery confirmed that network infrastructure devices were not configured to restrict any kind of traffic, even from the external internet. This could permit a remote adversary to easily discover and compromise any internal asset.

(U) Additionally, network infrastructure devices were not configured to DISA STIG policy and are extremely vulnerable to compromise. Default passwords and lack of multi-factor administrator authentication permit anyone with network access to control all settings on internal routers and firewalls, as well as any network traffic moving across them.

(U) RECOMMENDATIONS

1. NETWORK – Restrict Traffic
   1. Several detailed documents have been provided to local network defenders to describe recommended network segmentation and hardening.
   2. Summary of Recommendations: Block all inbound network traffic at the base boundary firewall (DEF-EDGE-FW) unless explicitly permitted, then isolate internal subnets to restrict freedom of movement for any adversary that compromises a single endpoint (e.g. via spear-phishing).
2. NETWORK – Apply DISA STIGs
   1. Change default passwords ASAP, and then apply DISA STIGs guidance available at <http://iase.disa.mil/stigs/Pages/index.aspx> in order to harden all infrastructure devices.

### (U) Risk Mitigation – Host

|  |  |
| --- | --- |
| 1 | Several well-known and easily exploited vulnerabilities exist for all systems |
| 2 | Internal hosts are not standardized or hardened against malicious activity |

(U) Hosts are susceptible to malicious exploits and activity when systems are not actively protected and maintained. The network workstations and servers were often observed to be four years or more behind in patches. Since the network has limited monitoring and prevention capabilities elsewhere in the domain this allows attackers to easily exploit well known vulnerabilities that currently exist on most systems.

(U) In addition to standard patch cycles there are currently no protections against malware that can be sent via email, external media, or network shares. This vulnerability allows state and non- state threat actors to easily establish a foothold in the network and expand from one system.

(U) RECOMMENDATIONS

1. HOST – Install patches
   1. Install the latest updates on servers listed on the PDAL first and then continue on to user workstations. We have identified that many servers listed on the PDAL have not been patched for four years and leave many well-known vulnerabilities open for exploitation.
2. HOST – Install Host Based Security System (HBSS)
   1. Antivirus – Activate the anti-virus module to detect malicious programs and scripts that may have bypassed other security measures.
   2. Firewall – Enable the firewall to prevent unauthorized connections on the network between computers that have not been authorized.
   3. Asset Baseline Monitor – Prevent the end users from installing unauthorized software on devices. Unauthorized software can be used to appear legitimate on the workstation and circumvent other protections put in place.
   4. Device Control Module – HBSS should monitor and prevent the use of external media devices on workstations. Preventing access to unauthorized storage can limit the ability of a user accidently or purposefully exfiltrating data outside of the domain.
   5. More details for HBSS can be found at: <https://disa.deps.mil/ext/cop/mae/CyberDefense/HBSS/SitePages/home.aspx>
3. HOST – Apply DISA STIGs
   1. Workstation hardening procedures are provided in the form of STIGs from DISA. These documents help local technicians apply a standard profile for patches and configuration to all systems.
4. HOST – Install Enhanced Mitigation Experience Toolkit (EMET)
   1. EMET makes exploitation of software difficult by applying security mitigation techniques to any software it should protect. EMET should be installed to protect internet facing applications against direct exploits like buffer overflow that may not be detected by anti-virus.
5. HOST – Baseline
   1. To identify what software does not belong on a system, a list of approved software and configurations need to exist to compare against. Apply a baseline to all hosts to identify files and software that do not belong.

### (U) Risk Mitigation – Monitoring

|  |  |
| --- | --- |
| 1 | Unable to respond to past security incidents because no historical data is stored |

(U) The vast majority of successful network compromises are not detected in real-time, but rather several weeks or even months after the fact. Without centrally archived logging information it is often infeasible to determine the scope of a breach, understand actions taken by an adversary, or even adequately restore network security. Unfortunately, the network does not have any form of host or infrastructure log archival in place.

(U) RECOMMENDATIONS

1. MONITORING – Enable Windows Event Forwarding (WEF)
   1. WEF is used to forward an audit log of various system and security related information to one or more Windows Event Collectors (WEC) in the environment. That log information can be used to identify sources of compromise, and aid defenders in response actions.
   2. <https://msdn.microsoft.com/en-us/library/windows/desktop/bb427443(v=vs.85).aspx>
2. MONITORING – Enable Syslog Forwarding
   1. Network infrastructure devices such as routers and firewalls are capable of emitting audit information in a “Syslog Message Format” that can be stored centrally and later consumed by a wide variety of security monitoring tools. This will help local defenders maintain the security of their networks.
   2. <http://www.cisco.com/c/en/us/products/collateral/services/high-availability/white_paper_c11-557812.html>
3. MONITORING – Enable NetFlow
   1. NetFlow enabled on correct devices allow the local defenders to view source and destination IP addresses and ports. This will be used to make sure the network is properly set up. This also ensures that nothing suspicious is communicating to or from the network (i.e beaconing endpoints).

### (U) Risk Mitigation – Process

|  |  |
| --- | --- |
| 1 | Local cyber defenders have no clear asset tracking, incident response plan, or forensic tools |

(U) The network has a complex network relationship with Riffa Air Base and DISA, and DEF cyber assets have no established asset or ownership tracking system. This greatly complicates efforts to determine who is responsible for the administration of a particular system, and who should respond to a potential incident. This also greatly increases reaction time for local defenders as various parties attempt to obtain necessary credentials and network access to compromised systems, giving network adversaries more time to achieve their ultimate goals.

Local defenders lack documentation and tools to assist them in responding to an incident appropriately, which may result in lost forensic evidence or incomplete mitigation in the event of a security breach.

(U) RECOMMENDATIONS

1. PATCH MANAGEMENT
   1. Install the latest updates on servers listed on the PDAL first and then continue on to user workstations. A vulnerability scan of the mission owner’s systems can be found in the Nessus Scan Report.
2. PROCESS – Establish Asset Tracking System
   1. After the initial IR TEAM survey was complete, local defenders were provided with a listing of all IPs, host names, and related Active Directory data. This information should be used to establish an asset tracking process, and ensure that appropriate responders have system credentials and network access when it is needed.
3. PROCESS – Establish Incident Response Plan
   1. Local defenders should have a Standard Operation Procedure for categorizing potential cyber incidents and responding accordingly. This will assist investigations and containment efforts.
4. PROCESS – Establish Baseline Toolkit
   1. Local defenders should have a standard baseline network and forensic toolkit that everyone is trained on.

# (U) ADVERSARY ACTIVITY

## Summary

**Intelligence Summary**

Pre-mission intelligence indicated two cyber threats: local hacktivist groups and State sponsored actors. The following past report on the adversary activity for situational awareness provided by the ASIA:

Vulnerability scanning against the external webserver was conducted from a hacktivist related server and executable files were discovered that called back to additional hacktivist servers. Evidence of compromise was found throughout the network which indicated widespread infection of the hollaback botnet/malware. The local defender’s response included blocking connections to the external hacktivist servers, killing malicious processes, removing malicious executables, and creating indicators of compromise’s (IOCs) for distributed defense actions. A possible rogue system was detected on the network. The local defenders removed the host from the network for further analysis.

Indications of a DDoS attack against the network’s webserver were seen, but did not affect the mission or PDAL assets.

# (U) LESSONS LEARNED

* Exercise Issues
* IR TEAM Coordination
* IR TEAM Work Performed
* Deconfliction

# APPENDIX A – PRIORITIZED RISK MITIGATIONS

The table below is a prioritized list of improvements that will have the greatest impact to risk reduction. Details for each item can be found in section 3.1 above.

|  |  |
| --- | --- |
| 1 | MONITORING – Enable Windows Event Forwarding (WEF) |
| 2 | MONITORING – Enable Syslog Forwarding |
| 3 | PATCH MANAGEMENT – Establish a patch management plan. |
| 4 | PROCESS – Establish Asset Tracking System |
| 5 | PROCESS – Establish Incident Response plan |
| 6 | NETWORK – Restrict Traffic |
| 7 | NETWORK – Apply DISA STIGs |
| 8 | HOST – Install patches |
| 9 | HOST – Install Host Based Security System (HBSS) |
| 10 | HOST – Apply DISA STIGs |
| 11 | HOST – Install Enhanced Mitigation Experience Toolkit (EMET) |
| 12 | HOST – Baseline |
|  |  |
|  |  |
|  |  |
|  |  |

# APPENDIX B – ADDITIONAL RECOMMENDED ACTIONS

NETWORK MAPS

* Implement a process to ensure network maps stay up-to-date

SENSORS

* Implement NACs on switches and routers
* Implement appropriate ingress and egress filtering at subnet boundaries to allow only specifically permitted traffic
* Ensure that firewall rules are implemented on the Firewalls to deny traffic that could exploit potential vulnerabilities in network as explained in the CVE's.
* Tune Sensors/IDS
* Enable Netflow on boundary devices
* Enable SPAN Ports on switches facing closest to network gateways
* Ensure Network Sensor grid is laid down over critical-assets, C-KT, and enclaves required to protect.

NETWORK AND HOST LOGS

* Ensure appropriate logging is enabled on all devices
* Ensure logs and sensor/IDS data are stored off-node in a central repository
* Ensure logs and sensor/IDS data are reviewed daily and someone is specifically assigned responsibility for this requirement

PATCHING AND CHANGE MANAGEMENT

* Ensure a recurring patching system (to include appropriate testing) is implemented and automated to the extent possible
* Validate admin accounts meet password complexity for C-KT and all network devices.
* Close ports on servers that are not being utilized, and monitor the ports that are being utilized
* Ensure all host computers are patched and updated

SIGNATURES/IOC’S

* Routinely scan nodes for vulnerabilities, report to Sys-Owner/DAA, and mitigate according to node priority/impact
* Check ACLs on routers and switches and patch against known vulnerabilities.  Write detection rules for snort/bro
* Establish over-watch with NSA utilizing SharkSheer sensor grid.
* Push agents to all end-points of C-KT, critical assets, IO, and CMD Staff enclaves.
* Create IOCs based off of CVEs and push to end-points and perform sweeps.
* Ensure all Operating Systems and applications affected with CVE's are patched.
* Ensure Port Security is enabled / enforced.
* Verify all firmware versions on legacy devices.

# APPENDIX B – CRITICALITY REPORTS

Criticality Report: Domain Controllers

Capabilities Affected:

* ***Sensors and Radar***
* ***Launch Capabilities***
* ***Maintenance***
* ***Standards & Evaluations***

Related Systems:

* ***PDAL A– Domain Controller 1***
* ***PDAL B– Domain Controller 2***

Both Domain Controllers for the network have multiple vulnerabilities categorized by the security industry as Critical and are high risk due to their essential functions on your network.

Both Domain Controllers host a service for Domain Name Resolution that is susceptible to the following types of vulnerabilities:

* Arbitrary Code Execution – A remote attacker could execute any command he wanted without authorization
* Denial of Service – A remote attacker could cause your DNS server to become unresponsive, denying legitimate traffic from accessing any network services you provide.

|  |  |
| --- | --- |
| **Short Term** | **Long Term** |
| Both Domain Controllers have vulnerabilities tracking all the way back to 2011, which indicates they have not received regular updates since then. Patching both servers according to [Microsoft Knowledge Base Article 832475](http://support.microsoft.com/kb/832475) will mitigate these vulnerabilities. | Upgrade both servers to at least Windows Server 2008 R2 Service Pack 2. Continue with regular patches to keep the systems secure. |

Vulnerability summary (Across critical systems above)

|  |  |
| --- | --- |
| Critical Vulnerabilities | 34 |
| High Risk Vulnerabilities | 1422 |
| Medium Risk Vulnerabilities | 78 |
| Findings that can be fixed with patching | 1534 |

\*Detailed results are available and have been provided to local NCC.

Criticality Report: Data Repositories

Capabilities Affected:

* ***Sensors and Radar***
* ***Launch Capabilities***
* ***Maintenance***
* ***Standards & Evaluations***

Related Systems:

* ***PDAL C– DEF-MEDSQL001***
* ***PDAL E– DEF-OPS002***
* ***PDAL G– DEF-SQL002***

Critical database systems are susceptible to publicly available exploits dating back all the way to 2007. It is common that critical systems such as these are not updated over long periods of time, due to business needs that require them to have near 100% up-time. Due to the sensitive nature of the data and its impact to your mission and member’s privacy, comprehensive patching of all database servers should become priority.

|  |  |
| --- | --- |
| **Short Term** | **Long Term** |
| Segregate critical databases to **only** talk to their corresponding user interfaces. This is already being accomplished with your local NCC/NOSC personnel. | Plan for a scheduled outage of database assets (one at a time) to apply patches for vulnerabilities classified as **critical**. Prior to patches, NCC should use identical images of database servers to validate functionality |

Vulnerability summary (Across critical systems above)

|  |  |
| --- | --- |
| Critical Vulnerabilities | 46 |
| High Risk Vulnerabilities | 2670 |
| Medium Risk Vulnerabilities | 114 |
| Findings that can be fixed with patching | 2830 |

\*Detailed results are available and have been provided to local NCC.

Criticality Report: User Interface Devices

Capabilities Affected:

* ***Air and Missile Defense***
* ***Maintenance***
* ***Standards & Evaluations***

Related Systems:

* ***PDAL F– DEF-MSDI002***
* ***PDAL H– DEF-MX001***
* ***PDAL I– DEF-PWR001***

Front end servers for critical database systems are vulnerable to unauthorized view or modification of configuration and administrative information. The location where website files are hosted is easily accessible and modifiable by regular domain users. Given threat intelligence regarding possible spear phishing attacks to your network, it is highly likely that a normal domain user account could be compromised and used to modify this critical data without any escalation of privileges.

|  |  |
| --- | --- |
| **Short Term** | **Long Term** |
| Disable sharing of inetpub folder on all hosts above over SMB. Find alternate methods for web developers to modify website files/configuration. | Modify network file share permissions for critical information to be accessible only to users with the need to know (typically administrative users). |

Vulnerability Summary (Across critical systems above)

|  |  |
| --- | --- |
| Critical Vulnerabilities | 64 |
| High Risk Vulnerabilities | 2111 |
| Medium Risk Vulnerabilities | 124 |
| Vulnerabilities that can be fixed with patching | 2348 |