ASSESSMENT SUMMARY

ICS Assessment

NUMBER

February 26, 2018 DATE

Cyber Research Lab Assessment Report

NCCIC

ASSESSMENT SUMMARY

ICS Assessment

NUMBER

February 26, 2018 DATE

Cyber Research Lab Assessment Report

Table of Contents

Tables

NCCIC

Cyber Research Lab Assessment Report

1. Introduction

As a core part of its mission to reduce risk to the Nation's critical infrastructure (CI), Department of Homeland Security (DHS) National Cyber Assessments and Technical Services (NCATS) subject matter experts provide cybersecurity assessments to CI asset owners and operators to strengthen the cybersecurity posture of their industrial control systems (ICS). NCATS on behalf of the National Cybersecurity and Communications Integration Center (NCCIC) provides voluntary assessments based on standards, guidelines, and best practices. The assessment methodology provides a structured framework that asset owners and operators can leverage to evaluate and validate the cybersecurity of their ICS networks. The information gained from these reviews provides stakeholders with the understanding and context necessary to build effective defense-in-depth processes for enhancing their cybersecurity posture.

NCATS's Operational Assurance (OA) review includes evaluation of ICS design architecture, verification and validation of network traffic, and system log review and analysis. An evaluation of the design architecture includes a high-level preliminary evaluation of the site security posture, leveraging the Cyber Security Evaluation Tool (CSET®), followed by an in-depth review and evaluation of the ICS network design, configuration, and inter-connectivity to internal and external systems. This system analysis provides ICS asset owners with a comprehensive cybersecurity evaluation focusing on defensive strategies associated with their specific control systems network.

Network data traffic analysis provides asset owners with information to identify anomalous and potentially suspicious communications sourced from, or destined for, control systems assets. This service offering provides a sophisticated analysis of the asset owner's network traffic, which the asset owner collects from within their control system network environment. The OA assessment team analyzes the captured network traffic using a combination of open source and commercially available tools to develop a detailed representation of the communications, flows, and relationships between devices.

The system log analysis provides evaluation of system log data. Asset owners submit useful system or event logs, which provide a sampling of the central control system elements, such as an ICS server, a historian/database collector, or a remotely connected human-machine interface (HMI) system. OA provides SME consultation and a detailed final report including evaluation discoveries and recommendations to support the requesting facility's path to improved security and resiliency.

The NCATS OA team performed a Validated Architecture Design Review (VADR) of the Cyber Research Lab from January 17 to January 19, 2018. The OA assessment team worked directly with the information technology (IT), and management staff at Cyber Research Lab facilities to determine the overall cybersecurity posture of its system. The objective of this assessment was to identify vulnerabilities and weaknesses and recommend mitigations for Cyber Research Lab to consider. The OA assessment team provided a closeout briefing to Cyber Research Lab participants and executive personnel to highlight areas of strength and opportunities to enhance the organization's cybersecurity posture.

2. Systems Assessed

The Cyber Research Lab is a networked environment completely isolated from the campus network. The purpose of this lab environment is to allow researchers to accomplish their cybersecurity missions unhindered by typical cybersecurity controls such as those found in the business enterprise environment. With a mission that includes active network scanning, vulnerability scanning, and penetration testing, Cyber Research Lab teams rely heavily on the lab to conduct active engagements as well as test new tactics, techniques, and processes to continuously improve their service offerings.

The lab environment is made up of many enclaves that keep the working environment separated based on purpose. All of these enclaves are separated into different virtual local area networks (VLAN) terminated at a Fortinet firewall for access control and monitoring. The two enclaves described to be of most value to administrators were the management enclave and the data enclave. The management enclave is used to connect to the management interfaces of network equipment and other important infrastructure. The data enclave is used to store cyber data as well as scripts, configurations, and other network storage purposes. Both of these enclaves require two-factor authentication, which grants the required level of access based on the roles assigned to each user.

3. Observed Strengths

During the engagement, the OA assessment team identified various strengths regarding the existing architecture, policies, and procedures that Cyber Research Lab facilities currently have in place. Those strengths include the following:

3.1 Separation from Enterprise LAN

Separating the lab's work and environment from the enterprise network has not only lab's best interests in mind but also allows the lab teams to accomplish their work in a safe manner given the nature of their mission.

3.2 Good use of templates and images

The OA assessment team commends the sysadmin group in maintaining up-to-date and secure images to be deployed in the static environment. The choice to reimage the operational/dynamic environment equipment has proved effective in ensuring consistent delivery of services to the customers without the threat of potentially exposing the customers to harmful content.

3.3 Cybersecurity maturity despite limited staff

Although staff members seem to be heavily burdened with administrative responsibilities, the cybersecurity maturity of the organization is strong in both practices and culture.

4. Discoveries

Although the OA assessment team identified several strengths and good cybersecurity practices, they also identified a number of discoveries with potential consequences and risks.

4.4 Cybersecurity Evaluation

During the system architecture review, the OA assessment team used CSET to identify key areas of concern to assist in detailed focus areas. NCATS recommends asset owners use self-evaluation tools on a regular basis to understand their security posture and to identify areas for improvement. The OA assessment team has separately provided a detailed CSET analysis to the Cyber Research Lab.

Please consult the associated CSET file for details; the categories and areas of concern ranked from the CSET:

4.4.1 Account Management.

4.5 Discovery Table

Table 1 summarizes OA assessment team's discoveries during the cybersecurity assessment of the Cyber Research Lab's facilities. Specifically, the table categorizes potential weaknesses discovered during the assessment based on National Institute of Standards and Technology (NIST) Special Publication 800-53 security control categories; it explains the specific weakness found in the discovery; it describes the potential consequence or risk posed by the presence of the discovery; and it recommends mitigations[1] for the Cyber Research Lab to consider.

1 The recommendations in this report are informational and should be researched, tested, and approved prior to implementation. All DHS notifications and disclaimers should be read and understood prior to accepting and deploying the recommendations.

Table 1. Discovery Table

NIST SP 800-53 Security Control Category	Assessment Discovery	Consequence/Risk	Recommendations for Consideration
Audit and Accountability AU-6(4) Audit Review, Analysis, and Reporting | Central Review and Analysis	The lab has limited centralized logging in place.	Without analysis of logs, anomalous events and intrusions will go undetected and allow for misconfiguration issues and advanced intrusions. Review and analysis of logs stored locally is an ineffective, time-consuming process in understanding events affecting multiple components. In addition, many cyber attacks delete locally stored logs, creating a vacuum of forensic evidence. Malicious actions go unnoticed without log collection and analysis.	Implement a centralized log collection and analysis service (and/or a Security Information and Event Management tool). By collecting all logs and events in a centralized service, analysis can save time/resources, improve efficiency, and allow the discovery of anomalous activity at a system-wide level.
Configuration Management CM-7 Least Functionality	Unused IPv6 protocol.	Unnecessary services, ports, protocols, applications, and functions create vectors for malicious parties to gain access to the system. An attacker could attempt to use the unused IPv6 protocol to perpetrate further attacks on the system.	If IPv6 must remain enabled, configure it to meet organizational requirements. Alternatively, create a solution to actively alert system owners of IPv6 protocol misuse.

NIST SP 800-53 Security Control Category	Assessment Discovery	Consequence/Risk	Recommendations for Consideration
Contingency Planning CP-9(1) Information System Backup | Testing for Reliability / Integrity	A network attached storage (NAS) for configuration backups is located in the same server room as production equipment. The lab has no formalized process for testing the integrity of backups.	A localized event could corrupt both production systems and configuration backups, which would greatly increase system downtime. Without regularly testing backups, the lab may not be able to identify problems with the recovery process until a restoration is needed.	Consider moving the NAS to a different physical location to minimize the risk of a localized failure. Alternatively, create a second NAS in a different location as a replica. Test recovery processes and procedures and verify the integrity of data from backups.
Identification and Authentication IA-3 Device Identification and Authentication	Network ports and wireless access to the lab network are accessible from business office space. No network access controls are in place for these local lab network connections.	There is currently no mechanism to alert or block an unauthorized device, which could lead to network or system compromise.	Traditional network authentication methods, such as 802.1X or port based MAC controls, may be difficult to implement in the lab environment, as it is a dynamic environment with many different physical and virtual hosts and operating systems. Establish a method to perform real-time monitoring of MAC addresses used within the lab environment and use automation to validate these addresses against a list of approved physical and virtual MAC addresses and headers. Configure alerts to notify Cyber Research Lab administrators so they can properly investigate unknown MAC addresses.

NIST SP 800-53 Security Control Category	Assessment Discovery	Consequence/Risk	Recommendations for Consideration
Physical and Environmental Protection PE-3 Physical Access Control	Employees without a valid business need have physical access to the lab network and server equipment.	Unauthorized or accidental changes may occur when unauthorized individuals have physical access to equipment.	Add locks to the Cyber Research Lab network racks. Develop a procedure to allow physical equipment access only to those with a valid business need.
System and Communications Protection SC-7 Boundary Protection	Almost every lab network allows outbound Internet connectivity.	Internet connectivity significantly increases the risk of system compromise. This connectivity provides a communication channel for malware to enter a network environment and a mechanism to communicate back out to the Internet to allow for command and control scenarios.	Eliminate outbound Internet communication from protected networks such as the management and data enclaves. Identify solutions for getting needed data and updates into theses protected networks.
System and Information Integrity SI-4 Information System Monitoring	Log reviews are not occurring regularly.	Monitoring network traffic, logs, and the information system as a whole is essential to determine if a potential compromise is occurring or to determine when there is problem with the system.	Establish a process to monitor the information system. System administrators should be able to use monitoring to identify abnormal events, including unauthorized connections and indicators of attack. Consider using automation to reduce the amount of labor needed to perform these tasks. See AU-6(4).

NIST SP 800-53 Security Control Category	Assessment Discovery	Consequence/Risk	Recommendations for Consideration
System and Information Integrity SI-4 Information System Monitoring	There is no monitoring of software installation on static systems.	Unauthorized software changes can be an indicator of attack. Unmanaged software can expose a system to vulnerabilities that if left unpatched could lead to a system compromise.	Leverage existing tools to automate a review of software inventory to identify changes. Review identified software changes regularly to verify that software changes are following established controls and change management.

4.6 Network Traffic Analysis Detail

The OA assessment team provided communication verification for Cyber Research Lab using tools designed for network analysis. Communication verification is critical to validate real network traffic and communication paths. Prior to the review, Cyber Research Lab provided a network traffic packet capture (PCAP) of header data only from within the network infrastructure. The assessment team then analyzed and compared the information against the documented architecture design to identify any anomalous traffic communicating outside documented security zones and boundaries. This deep analysis provides Cyber Research Lab with a detailed perspective and baseline of traffic flows, protocol usage, and possible misconfigured devices or components that communicated on and traversed the network. The assessment team utilized an open-source network analysis framework to analyze the network traffic, which parses the PCAP data and provides specific files (reports), enumerating the communication flows of interest.

4.6.1 NCATS analyzed the network traffic, as follows:

- verify the accuracy of the ICS network diagram(s),
- identify any potential rogue devices and unauthorized or malicious data communications, and
- analyze data flows to ensure that boundary protection devices are working as designed.

Based on this analysis, the assessment team made the observations listed in Table 2.

Table 2. Network Analysis Observations and Recommendations

Item	Observation	Recommendation
1	IPv6 observed.	Disable, configure, or monitor (See CM-7).
2	Outbound Internet activity observed from protected networks.	Restrict outbound Internet access on protected networks (See SC-7).
3	DNS query from 192.168.10.107 to resolve madnet.ru, which is a known mobile advertising platform that has also been considered adware.	Monitor network traffic for indicators of compromise (See SI-4).
4	The Data Enclave's .99 address (NAS) is connecting to cloudfront, a CDN. Cloudfront has also been known for hosting adware.	Although this connection may be legitimate, we recommend further research. Additionally, we recommend restricting outbound access on protected systems such as the NAS (See SC-7).

4.7 Open Source Research

The OA assessment team conducted a search to identify any sensitive Cyber Research Lab information posted on the Internet. This search revealed nothing of significance, which shows that the Cyber Research Lab is following its established process to review information before public release. Any sensitive information found on the Cyber Research Lab's web site, in external email, or on social media sites, such as Facebook, LinkedIn, and Twitter, could be used for reconnaissance, social engineering (staff and vendor), and attack planning. An attacker could use such information to target staff members with spear-phishing emails that induce them to click on malicious Internet links or open bad attachments. The Cyber Research Lab should continue its vigilance in following policy to review information before publishing and guard against the inadvertent public release of sensitive information on the Internet.

5. Continuing Partnership

OA assessment team appreciates the opportunity to work with Cyber Research Lab and looks forward to a continued partnership. Table 3 contains a 180-Day Post-Assessment Report Feedback form. In approximately six months, a representative from the assessment team will contact Cyber Research Lab and arrange a conference call to discuss the discoveries noted in this report, the status of any mitigations you may have implemented or plan on implementing, and the path forward. The purpose of the 180-Day Post-Assessment Feedback form is to do the following:

- provide an opportunity to discuss the discoveries and recommendations to identify areas of value and improvement by your company based on the work presented in the report;
- evaluate the effectiveness of the efforts by OA assessment team SME supporting your organization;
- share recent alerts, advisories, and known vulnerabilities relative to your organization; and
- document improvements noted in cybersecurity posture resulting in the work performed with your organization by the OA assessment team (NCATS uses obfuscated information based upon groups of the assessments performed in reporting results outside of the organization).

National Cybersecurity and Communication Integration Center (NCCIC) also offers a number of free services and products to help secure control systems. These services include training, incident response, and malware analysis. Products include recommended practices, attack scenario descriptions, and white papers. For general questions or comments, please contact NCCIC at nccicustomerservice@hq.dhs.gov. For information on training or downloading white papers and other useful documents on ICS cybersecurity, visit our website at https://ics-cert.us-cert.gov. To report an incident or vulnerability, call 1-888-282-0870 or send an email to nccicustomerservice@hq.dhs.gov.

6. Acronyms

CI	critical infrastructure
CSET®	Cyber Security Evaluation Tool
DHS	Department of Homeland Security
DNS	domain name system
ICS	industrial control system
IT	information technology
NAS	network attached storage
NCATS	National Cyber Assessments and Technical Services
NCCIC	National Cybersecurity and Communications Integration Center
NIST	National Institute of Standards and Technology
OA	Operational Assurance
PCAP	packet capture
SME	subject matter expert
VADR	Validated Architecture Design Review
VLAN	virtual local area network

Table 3. 180-Day Post-Assessment Report Feedback Form

NIST SP 800-53 Security Control Category	Discovery	Recommendation	Mitigation Status	How Beneficial was the Recommendation?	Additional Information
Audit and Accountability **AU-6(4) Audit Review, Analysis, and Reporting | Central Review and Analysis**	The lab has limited centralized logging in place.	Implement a centralized log collection and analysis service (and/or a Security Information and Event Management tool). By collecting all logs and events in a centralized service, analysis can save time/resources, improve efficiency, and allow the discovery of anomalous activity at a system-wide level.	☐Currently Mitigated ☐In Process ☐Future plans to mitigate (0-6 months) ☐Future plans to mitigate (> 6 months) ☐No plans to mitigate	☐Very Beneficial ☐Somewhat Beneficial ☐Undetermined ☐Not Beneficial ☐Not practical to implement at this time	

NIST SP 800-53 Security Control Category	Discovery	Recommendation	Mitigation Status	How Beneficial was the Recommendation?	Additional Information
Configuration Management **CM-7 Least Functionality**	Unused IPv6 protocol.	If IPv6 must remain enabled, configure it to meet organizational requirements. Alternatively, create a solution to actively alert system owners of IPv6 protocol misuse.	☐Currently Mitigated ☐In Process ☐Future plans to mitigate (0-6 months) ☐Future plans to mitigate (> 6 months) ☐No plans to mitigate	☐Very Beneficial ☐Somewhat Beneficial ☐Undetermined ☐Not Beneficial ☐Not practical to implement at this time	

NIST SP 800-53 Security Control Category	Discovery	Recommendation	Mitigation Status	How Beneficial was the Recommendation?	Additional Information
Contingency Planning **CP-9(1) Information System Backup | Testing for Reliability / Integrity**	A network attached storage (NAS) for configuration backups is located in the same server room as production equipment. The lab has no formalized process for testing the integrity of backups.	Consider moving the NAS to a different physical location to minimize the risk of a localized failure. Alternatively, create a second NAS in a different location as a replica. Test recovery processes and procedures and verify the integrity of data from backups.	☐Currently Mitigated ☐In Process ☐Future plans to mitigate (0-6 months) ☐Future plans to mitigate (> 6 months) ☐No plans to mitigate	☐Very Beneficial ☐Somewhat Beneficial ☐Undetermined ☐Not Beneficial ☐Not practical to implement at this time	

NIST SP 800-53 Security Control Category	Discovery	Recommendation	Mitigation Status	How Beneficial was the Recommendation?	Additional Information
Identification and Authentication **IA-3 Device Identification and Authentication**	Network ports and wireless access to the lab network are accessible from business office space. No network access controls are in place for these local lab network connections.	Traditional network authentication methods, such as 802.1X or port based MAC controls, may be difficult to implement in the lab environment, as it is a dynamic environment with many different physical and virtual hosts and operating systems. Establish a method to perform real-time monitoring of MAC addresses used within the lab environment and use automation to validate these addresses against a list of approved physical and virtual MAC addresses and headers. Configure alerts to notify Cyber Research Lab administrators so they can properly investigate unknown MAC addresses.	☐Currently Mitigated ☐In Process ☐Future plans to mitigate (0-6 months) ☐Future plans to mitigate (> 6 months) ☐No plans to mitigate	☐Very Beneficial ☐Somewhat Beneficial ☐Undetermined ☐Not Beneficial ☐Not practical to implement at this time	

NIST SP 800-53 Security Control Category	Discovery	Recommendation	Mitigation Status	How Beneficial was the Recommendation?	Additional Information
Physical and Environmental Protection **PE-3 Physical Access Control**	Employees without a valid business need have physical access to the lab network and server equipment.	Add locks to the Cyber Research Lab network racks. Develop a procedure to allow physical equipment access only to those with a valid business need.	☐Currently Mitigated ☐In Process ☐Future plans to mitigate (0-6 months) ☐Future plans to mitigate (> 6 months) ☐No plans to mitigate	☐Very Beneficial ☐Somewhat Beneficial ☐Undetermined ☐Not Beneficial ☐Not practical to implement at this time	

NIST SP 800-53 Security Control Category	Discovery	Recommendation	Mitigation Status	How Beneficial was the Recommendation?	Additional Information
System and Communications Protection **SC-7 Boundary Protection**	Almost every lab network allows outbound Internet connectivity.	Eliminate outbound Internet communication from protected networks such as the management and data enclaves. Identify solutions for getting needed data and updates into theses protected networks.	☐Currently Mitigated ☐In Process ☐Future plans to mitigate (0-6 months) ☐Future plans to mitigate (> 6 months) ☐No plans to mitigate	☐Very Beneficial ☐Somewhat Beneficial ☐Undetermined ☐Not Beneficial ☐Not practical to implement at this time	

NIST SP 800-53 Security Control Category	Discovery	Recommendation	Mitigation Status	How Beneficial was the Recommendation?	Additional Information
System and Information Integrity **SI-4 Information System Monitoring**	Log reviews are not occurring regularly.	Establish a process to monitor the information system. System administrators should be able to use monitoring to identify abnormal events, including unauthorized connections and indicators of attack. Consider using automation to reduce the amount of labor needed to perform these tasks. See AU-6(4).	☐Currently Mitigated ☐In Process ☐Future plans to mitigate (0-6 months) ☐Future plans to mitigate (> 6 months) ☐No plans to mitigate	☐Very Beneficial ☐Somewhat Beneficial ☐Undetermined ☐Not Beneficial ☐Not practical to implement at this time	

NIST SP 800-53 Security Control Category	Discovery	Recommendation	Mitigation Status	How Beneficial was the Recommendation?	Additional Information
System and Information Integrity **SI-4 Information System Monitoring**	There is no monitoring of software installation on static systems.	Leverage existing tools to automate a review of software inventory to identify changes. Review identified software changes regularly to verify that software changes are following established controls and change management.	☐Currently Mitigated ☐In Process ☐Future plans to mitigate (0-6 months) ☐Future plans to mitigate (> 6 months) ☐No plans to mitigate	☐Very Beneficial ☐Somewhat Beneficial ☐Undetermined ☐Not Beneficial ☐Not practical to implement at this time	