State of North Dakota
Security Assessment Report

[2023 Legislative Brief]

[SANITIZED VERSION]

SECUREYETI

DOCUMENT REVISION HISTORY

VERSION	DATE	CHANGE DESCRIPTION
1.0	09/28/2022	Initial Draft
1.1	12/05/2022	NDUS Comments & Remarks
1.2	12/21/2023	ITD Comments & Remarks
1.3	02/14/2023	State Auditor Comments & Remarks
1.4	02/24/2023	Final Draft

SUBMITTED TO:

James Kary
Systems Auditor
Office of the State Auditor

(701) 328-2580
jkary@nd.gov

PREPARED BY:

Casey Bourbonnais
Lead Technical Tester
Secure Yeti

(918) 986-7060
casey.bourbonnais@secureyeti.com

TABLE OF CONTENTS

1. INTRODUCTION

Under the guidance and direction of the State Auditor's office, Secure Yeti conducted a network security assessment of key network resources and infrastructure utilized by North Dakota's State Agencies and the twelve state-funded entities that constitute the North Dakota University System (NDUS).

The objective of this assessment was to evaluate the overall security posture of the network by subjecting network systems and resources to methods and techniques commonly used by threat actors. This process allows for the proactive remediation of identified weaknesses and vulnerabilities before they can be exploited by an attacker.

From 12/07/2021 through 09/30/2022, Secure Yeti performed a vulnerability assessment and penetration test against the internal and external networks of thirteen separate state-funded entities. Additional on-site wireless (WiFi) and physical tests were also conducted at five of the thirteen locations. All involved entities were also subjected to a custom-built phishing campaign.

It is important to note that this report represents a "snapshot" of each environment at the point-in-time it was assessed. The security posture observed during testing may have improved, deteriorated, or remained the same since this assessment was completed.

Secure Yeti understands the importance that the State of North Dakota has placed on cybersecurity. We sincerely appreciate the opportunity to have worked with the State Auditor's office during this engagement. Should you have any questions regarding these findings, or the content of this report, please feel free to contact us.

2. KEY PARTICIPANTS

OFFICE OF THE STATE AUDITOR

Josh Gallion State Auditor	jcgallion@nd.gov (701) 328-4780
James Kary Systems Auditor	jkary@nd.gov (701) 328-2580

INFORMATION TECHNOLOGY DEPARTMENT (ITD)

Jessica Newby Governance, Risk & Compliance Team Lead	jnewby@nd.gov (701) 328-4395

NORTH DAKOTA UNIVERSITY SYSTEM (NDUS)

Darin King Vice Chancellor IT / CIO	darin.r.king@ndus.edu (701) 792-6262
Brad Miller Director of Information Security	brad.miller@ndus.edu (701) 792-6282
Bryan Ford Senior Security Engineer	bryan.ford@ndus.edu (701) 792-6222
Michael Roue Security Apprentice	michael.roue@ndus.edu (701) 792-6306

SECURE YETI

Brett Lessley Project Manager	brett.lessley@secureyeti.com (918) 986-7060 x1005
Casey Bourbonnais Lead Technical Tester	casey.bourbonnais@secureyeti.com (918) 986-7060 x1010

3. SUMMARY OF SCOPE

The scope of this assessment included network resources at thirteen state-funded entities:

(ITD)	Information Technology Department
(CTS)	Core Technology Services
(BSC)	Bismarck State College
(DCB)	Dakota College at Bottineau
(DSU)	Dickinson State University
(LRSC)	Lake Region State College
(MaSU)	Mayville State University
(MiSU)	Minot State University
(NDSCS)	North Dakota State College of Science
(NDSU)	North Dakota State University
(UND)	University of North Dakota
(VCSU)	Valley City State University
(WSC)	Williston State College

Specific IP ranges and subnets were defined in advance for each location before the assessment began.

Resources were evaluated using three separate angles of attack:

- External User with no access to network resources provided. This approach evaluates risk from the perspective of a malicious hacker.
- Internal User with no access to network resources provided. This approach evaluates risk from the perspective of a visitor.
- Internal User with network access given to a typical employee. This approach evaluates risk from the perspective of a malicious insider or disgruntled employee.

External testing was conducted from various AWS and Google Cloud resources. ITD and NDUS whitelisted Secure Yeti's external IP addresses to ensure that connectivity was maintained throughout the assessment.

Internal Testing was performed using remote testing units supplied by Secure Yeti. These units were deployed to the same network subnets that hosted standard employee workstations at each location.

TOTAL IP ADDRESSES: 410,390

EXTERNAL ADDRESSES:
165,398

INTERNAL ADDRESSES:
240,896

EXCLUSIONS:
4,096

CIDR BLOCK	BLOCK SIZE (IN IP's)	BLOCKS	TOTAL
/16	65,536	3	196,608
/18	16,384	4	65,536
/19	8,192	2	16,384
/20	4,096	10	40,960
/21	2,048	4	8,192
/22	1,024	19	19,456
/23	512	46	23,552
/24	256	155	39,680
/28	16	1	16
/32	1	6	6

SUMMARY OF THE IP SPACE AND UNIQUE CIDR BLOCKS TESTED. DOES NOT INCLUDE IPV6 BLOCKS.

4. EXCLUSIONS

The following exclusions were agreed upon at the beginning of the assessment:

- Network segments critical to supporting Public Safety infrastructure and the 911 system were out of scope and not tested.
- Network segments supporting K-12 Video infrastructure were out of scope and not tested.
- Denial of Service (DoS) attacks were not included in the testing methodology and were not intentionally initiated or attempted.
- All storage arrays and underlying infrastructure were considered out of scope for intrusive testing. This included all fibre-channel and iSCSI arrays, controllers, and switches.

5. METHODOLOGY

Vulnerability Assessment: Used automated tools to systematically review/scan network resources for known security weaknesses and misconfigurations.

ITD	CTS	BSC	DCB	DSU	LRCS	MaSU	MiSU	NDSCS	NDSU	UND	VCSU	WSC
X**	X	X	X	X	X	X	X	X	X	X	X	X

Penetration Testing: Attempted to exploit discovered weaknesses and vulnerabilities to gain unauthorized access to network resources.

ITD	CTS	BSC	DCB	DSU	LRCS	MaSU	MiSU	NDSCS	NDSU	UND	VCSU	WSC
X**	X	X	X	X	X	X	X	X	X	X	X	X

Phishing Campaign: Sent fake emails attempting to trick employees into divulging credentials or clicking bogus links.

ITD	CTS	BSC	DCB	DSU	LRCS	MaSU	MiSU	NDSCS	NDSU	UND	VCSU	WSC
X	X	X	X	X	X	X	X	X	X	X	X	X

Wireless Network Assessment: Used specialized scanners to detect misconfigurations in the wireless network setup, verified strength of wireless encryption, identified, and located rogue access points.

ITD	CTS	BSC	DCB	DSU	LRCS	MaSU	MiSU	NDSCS	NDSU	UND	VCSU	WSC
X	-	-	X	-	X	-	X	-	-	-	-	X

Physical Assessment: Identified opportunities to compromise physical safeguards responsible for the protection of network resources including alarm sensors, cameras, door locks, exposed network ports, and unattended workstations to gain unauthorized access to secure areas.

ITD	CTS	BSC	DCB	DSU	LRCS	MaSU	MiSU	NDSCS	NDSU	UND	VCSU	WSC
X	-	-	X	-	X	-	X	-	-	-	-	X

***Denotes that the assessment team was not able to thoroughly scan or test individual offices of the statewide ITD network as done in the prior assessment. After the last assessment, ITD moved to a zero-trust framework that increased overall security, but severely limited lateral movement on the internal network. Although ITD offered the assessment team additional permissions, granting those would have defeated the purpose of the zero-trust model. Reported findings are based on limited permissions provided.*

Legend:	*(ITD)*	*Information Technology Department*	*(MiSU)*	*Minot State University*
	(CTS)	*Core Technology Services*	*(NDSCS)*	*North Dakota State College of Science*
	(BSC)	*Bismarck State College*	*(NDSU)*	*North Dakota State University*
	(DCB)	*Dakota College at Bottineau*	*(UND)*	*University of North Dakota*
	(DSU)	*Dickinson State University*	*(VCSU)*	*Valley City State University*
	(LRSC)	*Lake Region State College*	*(WSC)*	*Williston State College*
	(MaSU)	*Mayville State University*		

6. RISK RATING SYSTEM

Critical *(16-POINTS)*	Critical severity rankings require immediate action through mitigating controls, direct remediation, or a combination thereof. Exploitation of discovered critical severity vulnerabilities not only results in privileged access to the target system/application or sensitive data, but also allows access to other hosts or data stores within the environment.
High *(8-POINTS)*	High severity rankings require immediate evaluation and subsequent resolution. Exploitation of high severity vulnerabilities discovered in the environment can directly lead to an attacker gaining privileged access (e.g., administrator, root, SA, etc.) to the system/application or sensitive data.
Medium *(4-POINTS)*	Medium severity rankings require review and resolution within a short period. From a technical perspective, vulnerabilities that warrant a medium severity ranking can lead directly to an attacker gaining non-privileged access (e.g., standard user) to the system/application or sensitive data or cause a denial-of-service (DoS) condition on the host, service, or application.
Low *(2-POINTS)*	Low severity rankings require review and resolution once the remediation efforts for critical, high, and medium severity issues are complete. From a technical perspective, vulnerabilities that warrant a low severity ranking may leak information to unauthorized or anonymous users used to launch a more targeted attack against the environment.
Info *(1-POINT)*	Informational rankings present no direct threat to the confidentiality, integrity or availability of the data or systems supporting the environment. These issues pose an inherently low threat to the organization and any proposed resolution should be considered as an addition to the information security procedures already in place.

7. CONTROL FAMILIES / RISK CATEGORIES

CONTROL FAMILY		DESCRIPTION
Access Control	(AC)	The AC Control Family consists of security requirements detailing asset-specific access and reporting capabilities like account management, system privileges, and remote access logging to determine when users have access to the system and their level of access.
Audit & Accountability	(AU)	The AU control family consists of security controls related to an organization's audit capabilities. This includes audit policies and procedures, audit logging, audit report generation, and protection of audit information.
Awareness & Training	(AT)	The control sets in the AT Control Family are specific to security training and procedures, including security training records.
Configuration Management	(CM)	CM controls are specific to an organization's configuration management policies. This includes a baseline configuration to operate as the basis for future builds or changes to information systems. Additionally, this includes information system component inventories and a security impact analysis control.
Contingency Planning	(CP)	The CP control family includes controls specific to an organization's contingency plan if a cybersecurity event should occur. This includes controls like contingency plan testing, updating, training, and backups, and system reconstitution.
Identification & Authentication	(IA)	IA controls are specific to the identification and authentication policies in an organization. This includes the identification and authentication of organizational and non-organizational users and how the management of those systems.
Incident Response	(IR)	IR controls are specific to an organization's incident response policies and procedures. This includes incident response training, testing, monitoring, reporting, and response plan.
Maintenance	(MA)	The MA controls in NIST 800-53 revision five detail requirements for maintaining organizational systems and the tools used.
Media Protection	(MP)	The MP family includes controls that are specific to access, marking, storage, transport policies, sanitization, and defined organizational media use.
Personnel Security	(PS)	PS controls relate to how an organization protects its personnel through position risk, personnel screening, termination, transfers, sanctions, and access agreements.
Physical & Environmental Protection	(PE)	The PE control family is implemented to protect systems, buildings, and related supporting infrastructure against physical threats. These controls include physical access authorizations, monitoring, visitor records, emergency shutoff, power, lighting, fire protection, and water damage protection.

CONTROL FAMILY		DESCRIPTION
Planning	(PL)	PL controls in NIST 800-53 are specific to an organization's security planning policies and must address the purpose, scope, roles, responsibilities, management commitment, coordination among entities, and organizational compliance.
Program Management	(PM)	The PM control family is specific to who manages your cybersecurity program and how it operates. This includes, but is not limited to, a critical infrastructure plan, information security program plan, plan of action milestones and processes, risk management strategy, and enterprise architecture.
Risk Assessment	(RA)	The RA control family relates to an organization's risk assessment policies and vulnerability scanning capabilities.
Security Assessment & Authorization	(CA)	The CA control family includes controls that supplement the execution of security assessments, authorizations, continuous monitoring, plan of actions and milestones, and system interconnections.
System & Communications Protection	(SC)	The SC control family is responsible for systems and communications protection procedures. This includes boundary protection, protection of information at rest, collaborative computing devices, cryptographic protection, denial of service protection, and many others.
System & Information Integrity	(SI)	The SI control family covers controls that protect system and information integrity. These include flaw remediation, malicious code protection, information system monitoring, security alerts, software and firmware integrity, and spam protection.
System and Services Acquisition	(SA)	The SA control family relates to controls that protect allocated resources and an organization's system development life cycle. This includes information system documentation controls, development configuration management controls, and developer security testing and evaluation controls.

8. EXECUTIVE SUMMARY

8.1. RISK ASSIGNMENT

Testing discovered a total of 130 unique findings across the 13 entities assessed. After a thorough analysis, these findings have been rated at the following risk levels:

CRITICAL	HIGH	MEDIUM	LOW	INFO
1	36	54	39	0
TOTAL: 130				

In determining risk, our team analyzed two key factors for each finding:

1) IMPACT: defined as "the magnitude of harm that can be expected." When calculating impact, the following possibilities are considered:

   - degradation of mission capabilities
   - damage / loss of organizational assets or data (& sensitivity of that data)
   - financial loss
   - reputational loss
   - loss of life or physical harm

2) LIKELIHOOD: defined as "the probability of an event occurring." When calculating likelihood, we consider:

   - the likelihood of the event occurring or being initiated
   - the likelihood of the event being successful
   - factors that mitigate risk (i.e. – small user-base, located on an isolated network, rarely used)
   - factors that magnify risk (i.e. – publicly accessible, weak password policies, misconfigurations)

				IMPACT		
		Info	Low	Medium	High	Critical
LIKELIHOOD	Critical	Info	Low	Medium	High	Critical
	High	Info	Low	Medium	High	Critical
	Medium	Info	Low	Medium	Medium	High
	Low	Info	Low	Low	Low	Medium
	Info	Info	Info	Info	Low	Low

[OVERALL RISK]

OVERALL RISK DETERMINATION CHART – BASED ON IMPACT-LIKELIHOOD ANALYSIS.

8.2. CONTROL FAMILY CATEGORIZATION

In addition to the assessment of risk, findings are sorted into NIST control families. If the observed deficiency for a particular finding applies to multiple families, a secondary classification is assigned.

The table below shows the breakdown of findings based on control families:

CONTROL FAMILIES:	PRIMARY	SECONDARY	TOTAL
Access Control	26	16	42
Audit & Accountability	0	0	0
Awareness & Training	13	0	13
Configuration Management	1	52	53
Contingency Planning	0	0	0
Identification & Authentication	21	0	21
Incident Response	1	0	1
Maintenance	0	0	0
Media Protection	0	0	0
Personnel Security	0	0	0
Physical & Environmental Protection	0	5	5
Planning	0	0	0
Program Management	0	0	0
Risk Assessment	0	0	0
Security Assessment & Authorization	0	0	0
System & Communications Protection	47	1	48
System & Information Integrity	21	10	31
System & Services Acquisition	0	0	0
TOTAL:	130	84	214

8.3. HEAT MAP (LOCATION/RISK)

The heat map below displays the number of findings discovered at each location, grouped by their associated level of risk.

By cross-referencing or weighting this data, we can see which areas are most problematic:

LOCATION / RISK LEVEL:	CRITICAL (x16)	HIGH (x8)	MODERATE (x4)	LOW (x2)	VERY LOW (x1)	TOTAL POINTS
Information Technology Department:	0	6	2	4	0	64
Williston State College:	0	3	6	3	0	54
Minot State University:	0	3	6	2	0	52
Lake Region State College:	0	2	6	4	0	48
Core Technology Services:	1	2	2	4	0	48
Dickinson State University:	0	3	5	2	0	48
Dakota College at Bottineau:	0	2	5	6	0	48
Valley City State College:	0	4	2	3	0	46
University of North Dakota:	0	2	6	2	0	44
North Dakota State College of Science:	0	3	3	3	0	42
North Dakota State University:	0	2	4	3	0	38
Mayville State University:	0	2	4	1	0	34
Bismarck State College:	0	2	3	2	0	32
TOTAL POINTS:	16	288	216	78	0	598

DISTRIBUTION OF FINDINGS PER LOCATION, GROUPED BY LEVEL OF RISK.

8.4. HEAT MAP (CONTROL FAMILY/RISK)

The heat map below displays the number of primary and secondary NIST control families assigned to each finding, grouped by their associated level of risk.

By cross-referencing or weighting this data, we can see which areas are most problematic:

CONTROL FAMILY / RISK LEVEL:	CRITICAL (16 PTS)	HIGH (8 PTS)	MEDIUM (4 PTS)	LOW (2 PTS)	INFO (1 PNT)	TOTAL POINTS
System & Communications Protection:	0	24	12	12	0	264
Access Control:	0	11	21	10	0	192
Configuration Management:	0	7	17	29	0	182
System & Information Integrity:	0	10	10	11	0	142
Identification & Authentication:	0	6	4	11	0	86
Awareness & Training:	0	0	13	0	0	52
Physical & Environmental Protection:	0	1	4	0	0	24
Incident Response:	1	0	0	0	0	16
Media Protection:	0	0	0	0	0	0
Contingency Planning:	0	0	0	0	0	0
Audit & Accountability:	0	0	0	0	0	0
Maintenance:	0	0	0	0	0	0
Personnel Security:	0	0	0	0	0	0
Planning:	0	0	0	0	0	0
Program Management:	0	0	0	0	0	0
Risk Assessment:	0	0	0	0	0	0
Security Assessment & Authorization:	0	0	0	0	0	0
System & Services Acquisition:	0	0	0	0	0	0
TOTAL POINTS:	16	472	324	146	0	958

DISTRIBUTION OF FINDINGS BASED ON PRIMARY AND SECONDARY NIST CONTROL FAMILY ASSIGNMENTS, GROUPED BY RISK.

8.5. HEAT MAP (CONTROL FAMILY/LOCATION)

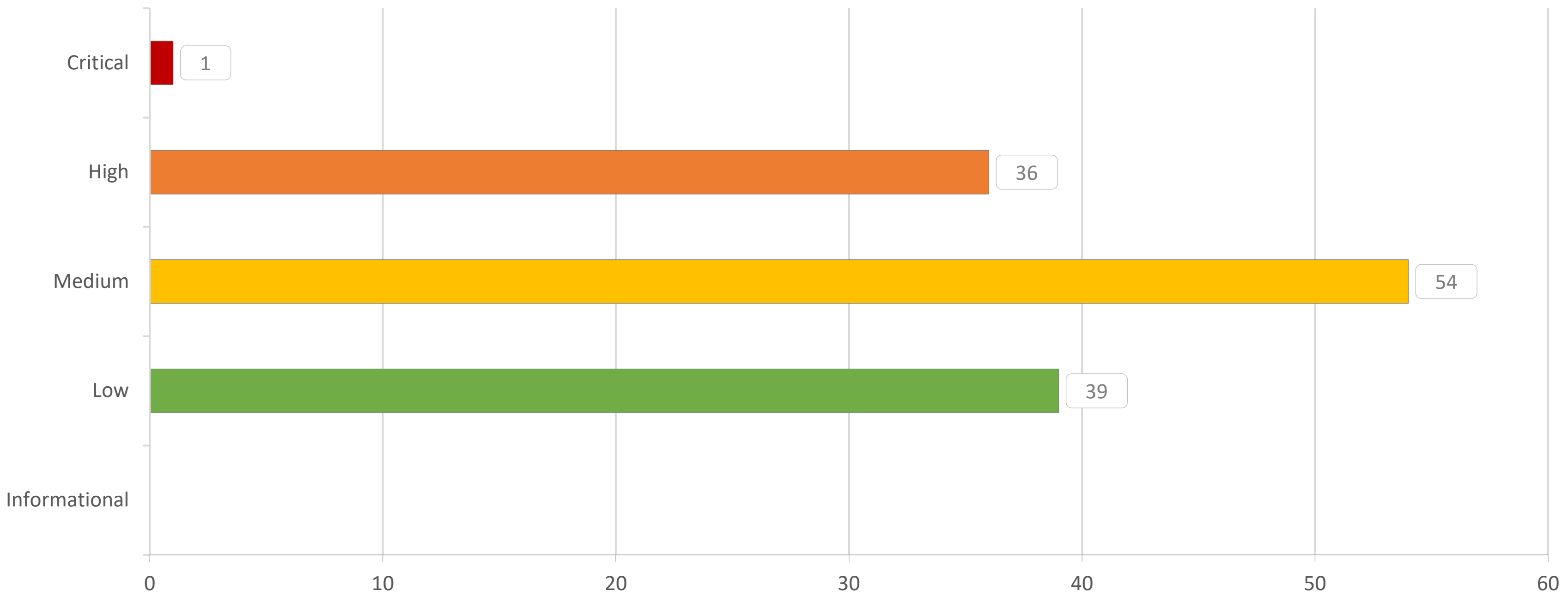
The heat map below displays the number of primary and secondary NIST control families assigned to each finding, grouped by location.

By cross-referencing or weighting this data, we can see which areas are most problematic:

RISK FAMILY / LOCATION:	ITD	CTS	BSC	DCB	DSU	LRSC	MaSU	MiSU	NDSCS	NDSU	UND	VCSU	WSC	TOTAL
Configuration Management:	7	3	3	8	3	5	2	4	4	3	3	4	4	53
System & Communications Protection:	5	3	3	5	4	4	2	5	2	3	3	4	5	48
Access Control:	5	3	0	6	3	5	0	5	3	0	4	3	5	42
System & Information Integrity:	0	2	4	1	3	2	3	1	3	5	3	2	2	31
Identification & Authentication:	3	0	0	1	2	2	2	2	2	1	2	2	2	21
Awareness & Training:	1	1	1	1	1	1	1	1	1	1	1	1	1	13
Physical & Environmental Protection:	1	0	0	1	0	1	0	1	0	0	0	0	1	5
Incident Response:	0	1	0	0	0	0	0	0	0	0	0	0	0	1
Media Protection:	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Contingency Planning:	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Audit & Accountability:	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Maintenance:	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Personnel Security:	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Planning:	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Program Management:	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Risk Assessment:	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Security Assessment & Authorization:	0	0	0	0	0	0	0	0	0	0	0	0	0	0
System & Services Acquisition:	0	0	0	0	0	0	0	0	0	0	0	0	0	0
TOTAL:	22	13	11	23	16	20	10	19	15	13	16	16	20	214

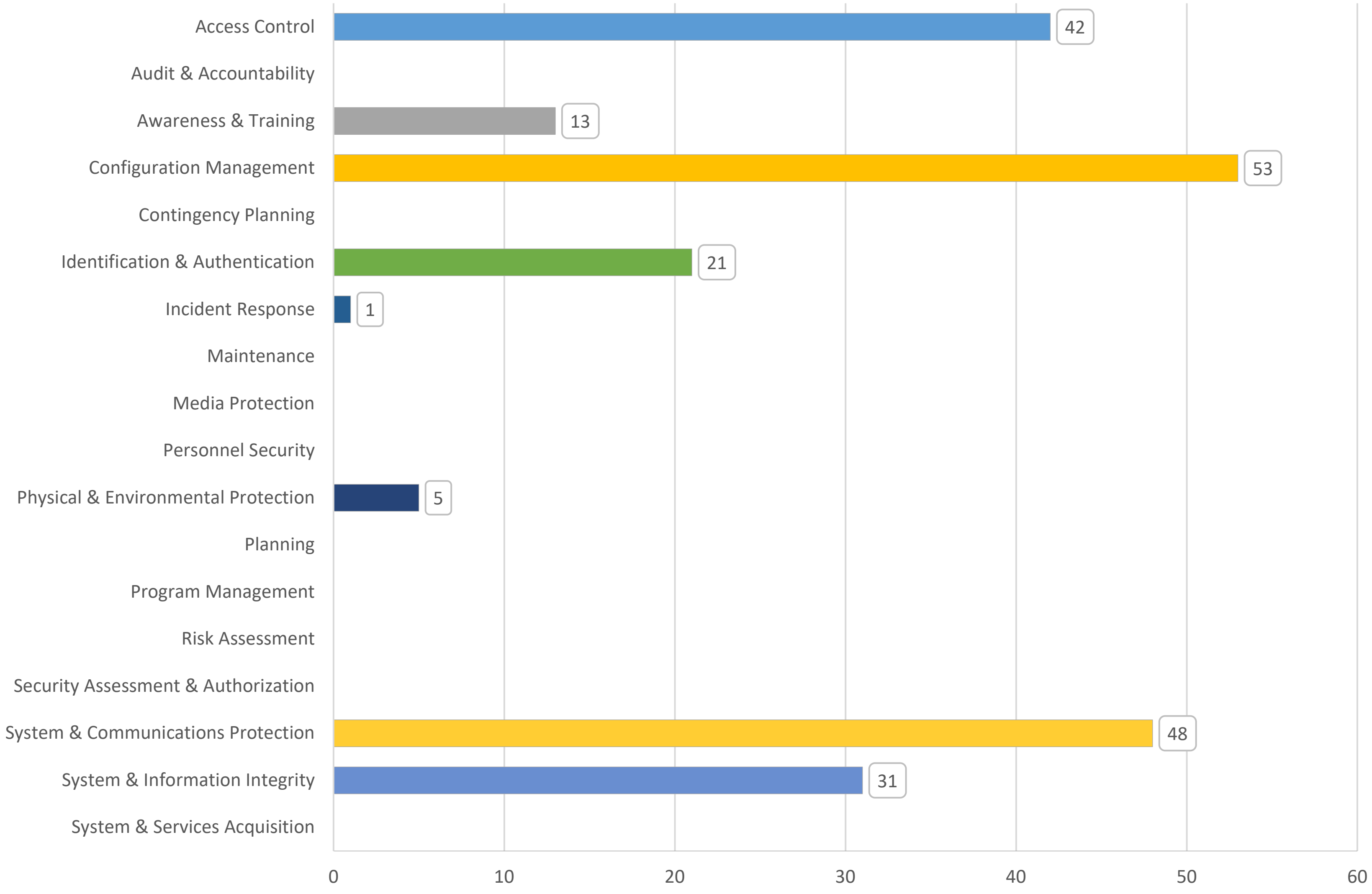
DISTRIBUTION OF FINDINGS BASED ON PRIMARY AND SECONDARY NIST CONTROL FAMILY ASSIGNMENTS, GROUPED BY LOCATION.

8.6. LINE GRAPH (RISK LEVEL)



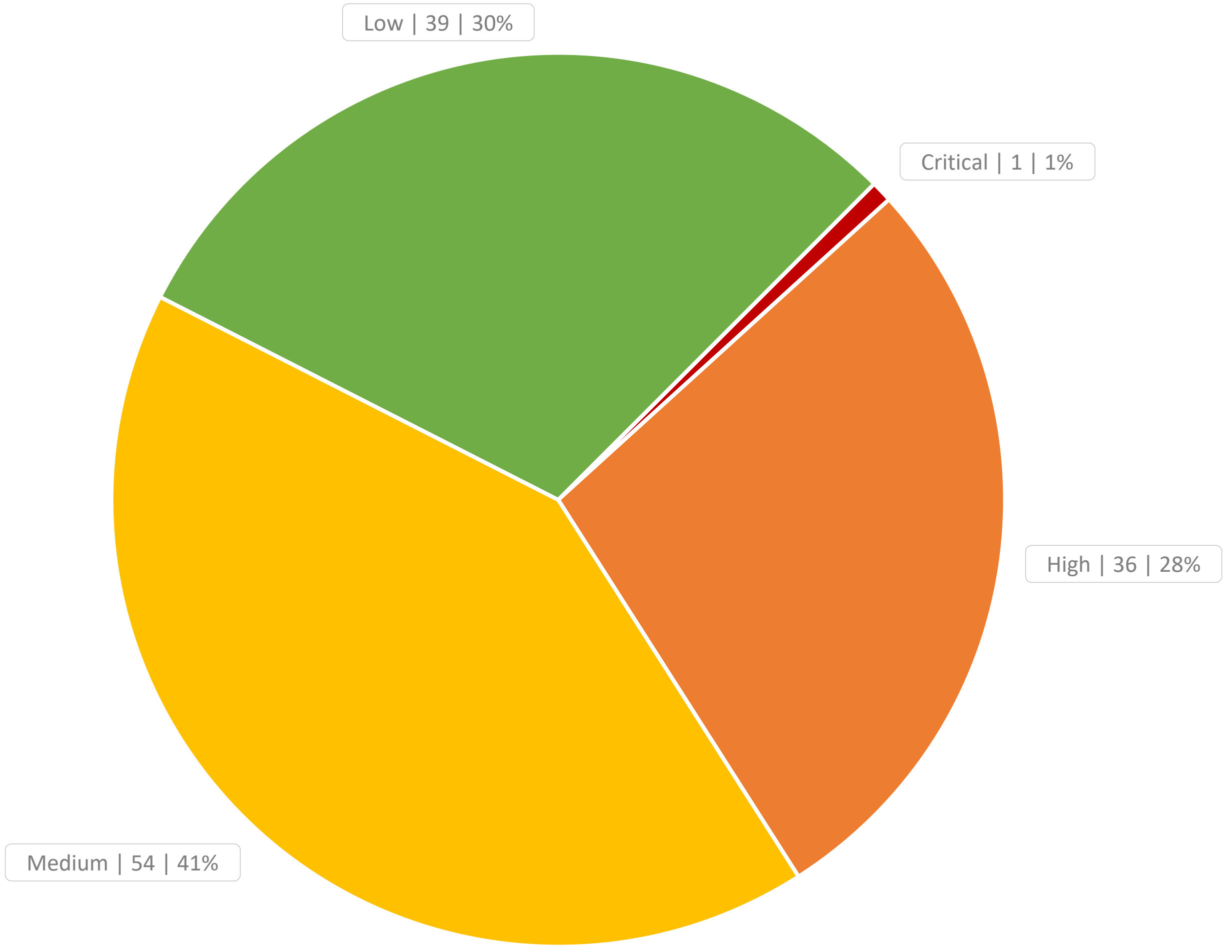
NUMBER OF FINDINGS PER RISK LEVEL.

8.7. LINE GRAPH (NIST CONTROL FAMILIES)



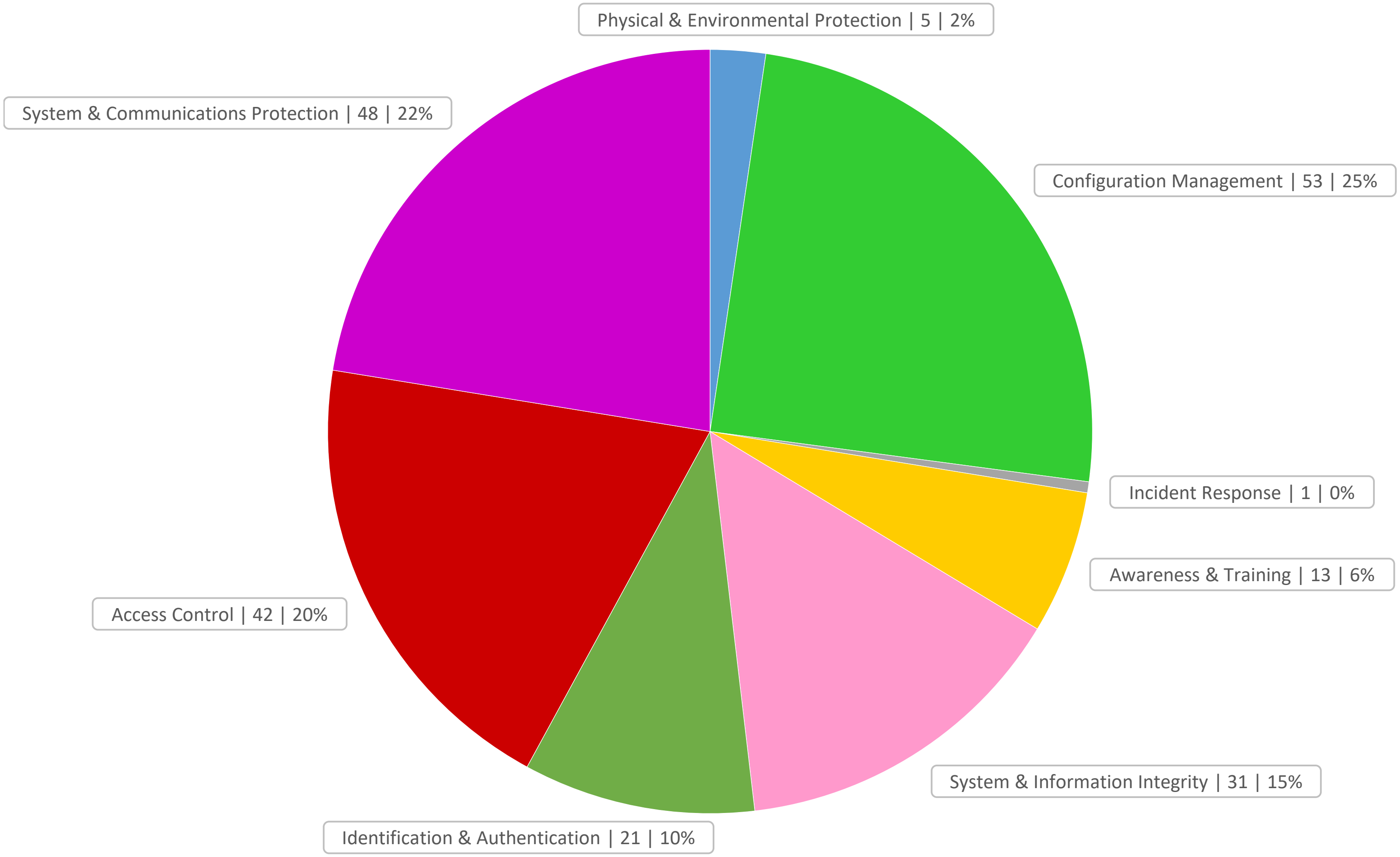
NUMBER OF FINDINGS PER NIST CONTROL FAMILY (INCLUDES PRIMARY AND SECONDARY).

8.8. PIE CHART (RISK LEVEL)



PERCENTAGE OF FINDINGS PER LEVEL OF RISK.

8.9. PIE CHART (NIST CONTROL FAMILIES)



PERCENTAGE OF FINDINGS BASED ON PRIMARY AND SECONDARY NIST CONTROL FAMILY ASSIGNMENTS.

8.10. KEY FINDINGS

The findings listed below represent the ten most significant issues (based on risk or frequency) discovered during the assessment. These issues typically have wide-spread impact and pose the greatest risk to the overall environment.

Prioritizing the remediation of these findings will provide the greatest benefit to the organization's security posture:

#	Finding	Risk
ES01	Intrusion Monitoring, Detection, and Response *(Category: Incident Response)*	Critical
ES02	Insecure Firewall Configuration (Google Cloud IP Space) *(Category: System & Communications Protection + Access Control)*	High
ES03	Excessive Permissions for Workstation Users *(Category: Access Control + Configuration Management)*	High
ES04	Digital Verification/Authentication of Network Traffic Not Enforced *(Category: System & Communications Protection)*	High
ES05	Insecure Legacy Protocols *(Category: System & Communications Protection + System & Information Integrity)*	High
ES06	Insecure Password Policy *(Category: Identification & Authentication + Access Control)*	Medium
ES07	Phishing Campaign Stats *(Category: Awareness & Training)*	Medium
ES08	Patching and Configuration Management *(Category: System & Information Integrity)*	Medium

8.11. KEY FINDINGS (DETAILS)

ES01: INTRUSION MONITORING, DETECTION, & RESPONSE

What we observed:	The Secure Yeti assessment team performed penetration testing activities with the purpose of measuring detection and response times of the NDUS Security Operation Center (SOC). Although the NDUS SOC team demonstrated tremendous improvements in their operational capabilities since last being assessed, they 1) were still greatly under-staffed considering the sheer size of the networks being monitored, and 2) not adequately staffed to monitor the network on a 24/7/365 basis. This meant a considerable amount of the assessment team's "malicious activities" continued to go undetected or had a delayed response.
What is the risk:	Today's networks are constantly under siege from external attackers, malicious insiders, and even errant and unintentional actions of end users. A successful attack is usually the culmination of a series of small events that test the configuration and rigidness of the network. Attackers will "poke and prod" the network looking for ways to obtain access until one is found. Some attacks take months to be successful, while others can occur in a matter of seconds. These events provide key indicators, and often indisputable evidence, that a system is under attack, or has already become compromised. Rapid detection and response to these indicators is a vital part of protecting the network and preventing a series of malicious attacks from turning into a full-blown system compromise or ransomware attack. Failing to detect these attacks in a timely manner has the potential of putting the records and information of every student and employee within the university system at risk. As a brief example, the assessment team encountered financial aid applications, tax returns, medical histories, and driver's licenses during this engagement. Documents containing personal and financial information are exactly what threat actors are trying to obtain.
How do we remediate:	First, our assessment team would like to acknowledge a night-and-day difference in detection and response capabilities of the NDUS team since we last worked with them. We feel it is important to recognize the resources and hard work state officials have put toward further securing the NDUS network and can certainly confirm a substantial increase in security posture. However, there does not appear to be enough resources to adequately monitor a network of this size on a 24/7/365 basis. Attackers will always strike when and where it is least expected. That is why it is important to ensure the entire NDUS network is adequately monitored around-the-clock. We recommend increasing SOC resources so they can adequately handle the volume of detected incidents regardless of when (day/hour) they occur.

ES02: INSECURE FIREWALL CONFIGURATION (GOOGLE CLOUD IP SPACE)

What we observed:	The assessment team discovered a misconfiguration in an NDIT firewall rule that allowed excessive public access to various internal NDIT and NDUS resources. A firewall rule was errantly entered as a "/1" when it should have been entered as a "/21." Instead of granting access to a block of 2,048 individual IP addresses, this typo gave 2,147,483,648 addresses (or half of the public Internet) the ability to access various NDIT and NDUS resources.
What is the risk:	The most effective way to protect a resource is to limit its access. Allowing internal resources to be accessed by 2.15 billion IP addresses exponentially increased the attack surface of internal resources.
How do we remediate:	Implement a process workflow that requires all firewall modifications to be reviewed/approved by at least two people before being "committed." Please note that NDIT immediately corrected this issue as soon as it was brought to their attention.

ES03: EXCESSIVE PERMISSIONS FOR WORKSTATION USERS

What we observed:	Workstation configurations for both ITD and CTS allowed users to install “backdoor” software that created a persistent connection that allowed the assessment team to access internal ITD and NDUS resources remotely. ITD users were able to modify the registry of their Windows workstation in a way that allowed them to schedule custom tasks, add startup items, or create arbitrary registry keys. Third-party vendors using "shared" or "hoteling" workstations within the CTS data center had excessive permissions that gave them the ability to install programs or modify registry settings. The assessment team was able to perform the following actions: 1. successfully installed a remote-listener application on a shared CTS workstation and ITD workstation 2. modified registry settings to ensure the listener remained persistent and started after every reboot 3. confirmed connectivity from a remote site after rebooting
What is the risk:	By installing remote access software on both ITD and CTS workstations, a threat actor could remotely access internal state resources. This access could allow threat actors to view content displayed on the user’s monitor(s), spy on users by taking control of attached webcams or microphones, exfiltrate sensitive data, or drop and execute additional malware on network resources.
How do we remediate:	Configure domain wide group policies that limit a user’s ability to add scheduled tasks and startup items. Restrict access to registry settings, especially to keys that deal with executing software at the time of boot or logon. Restrict outbound access for these machines For shared workstations, configure these machines to PXE boot so that a fresh image can be easily deployed after each use.

ES04: DIGITAL VERIFICATION/AUTHENTICATION OF NETWORK TRAFFIC NOT ENFORCED

What we observed:	Testing observed workstations and servers on ITD and NDUS networks that did not require network traffic to be digitally verified/authenticated before being processing.
What is the risk:	Unverified/Unauthenticated network traffic is susceptible to Man-in-the-Middle (MiTM) attacks that can allow attacker to modify or steal sensitive data. This type of traffic can also be “replayed” to gain access to network resources.
How do we remediate:	Enable group policies or configurations that require network traffic to be digitally verified and authenticated before being accepted or processed.

ES05: INSECURE LEGACY PROTOCOLS

What we observed:	Testing observed the wide-spread use of insecure legacy protocols on NDUS networks.
What is the risk:	These protocols are susceptible to Man-in-the-Middle (MiTM) or spoofing attacks where valid credentials are captured or stolen before being relayed to the original network destination, completely unbeknownst to the end-user. Testing efforts consistently exploited these protocols throughout the entire assessment. Ten of the 13 networks tested during this assessment utilized these protocols and are 100% vulnerable to this attack.
How do we remediate:	Remediating this attack requires these legacy protocols to be disabled. In order to disable these protocols, all computers on the network must be correctly configured and capable of using DNS to perform lookup and name resolution requests.

ES06: INSECURE PASSWORD POLICY

What we observed:

Testing discovered insecure or non-existent password policies on various NDUS networks that allowed users to create insecure passwords. We observed password policies that:

- Allowed passwords as short as 3-characters
- Did not enforce sufficient password complexity
- Did not enforce minimum or maximum age or expiration of passwords
- Did not enforce password history
- Did not enforce an account lockout
- Allowed clear-text storage of passwords

What is the risk:

Weak password policies greatly increase the probability that brute-force or password-cracking attacks will be successful, should they occur.

Specially designed password-cracking servers can crack the hashed value of any 9-character Windows password in under 30 seconds - regardless of complexity.

Password Length	Average Time Required to Crack
≤ 9-characters	24 seconds
10-characters	10 minutes
11-characters	4.5 hours
12-characters	4.5 days
13-characters	120 days
14-characters	N/A - results in error

Over the course of this and the previous assessment, the use of weak passwords allowed the assessment team to capture and successfully crack approximately 20,000+ user passwords. Additionally, the use of a weak password by a System Administrator allowed malicious users to compromise several internal systems.

How do we remediate:

Enforce a strong password policy for all users.

Password policies are not one-size-fits-all. To be effective, password policies must be tailored to meet specific requirements of each department/division, while simultaneously providing adequate protection for the entire network.

When considering a password policy, it is critical that it is consistently applied to all users of the network. Think of the old analogy of “a chain is only as strong as its weakest link.” This means your network’s overall password strength will only be as strong as the strength of your weakest password policy.

A password’s entropy, or the measurement of its predictableness, is primarily measured by its length and complexity. Complexity is achieved by using a variety of upper and lower-case characters as well as numbers and symbols.

Other factors that increase entropy are:

- Password Age / Expiration
- Password Reuse
- Account Lockout
- Account Lockout Duration

While we cannot dictate a password policy specific to your organizational needs, Secure Yeti's suggested password policy is defined below:

Password Length:
Since the success-rate of password-cracking drastically decreases when passwords reach 13-characters in length, we suggest enforcing the following minimum password length:

- Normal Users: 14-character minimum
- Privileged Users: 16-character minimum
- Service Accounts: 25-character minimum

Password Complexity:
Passwords should contain at least 3 of the 4 following character sets:

- Upper Case
- Lower Case
- Number
- Symbol

Password Expiration:
Since 13-character passwords can be cracked in 120 days, we suggest passwords used for both normal and privileged accounts expire after 90-days. Service accounts, due to their nature, are not required to expire.

Password expiration is vital in protecting the network. Should a password become unknowingly compromised, the password expiration policy limits the amount of time a compromised password can be used.

Password Re-use:
Users should not be allowed to reuse a password previously used within the last two years.

Account Lockout:
Accounts should be locked and/or disabled after 3 to 5 consecutive unsuccessful authentication attempts.

Account Lockout Duration:
Accounts should remain locked and/or disabled for at least 30-minutes or until a System Administrator manually unlocks the account after verifying the user's identity.

** NOTE: Third-party software can also be deployed in order to ensure that the user's desired password doesn't match commonly used or known phrases, and isn't included on popular breeched-password lists.

ES07: PHISHING CAMPAIGN STATS (NDUS/CTS)

What we observed:	The assessment team observed employees approving Multi-Factor Authentication (MFA) pushes they did not initiate. Privileged users were targeted with a phishing email claiming it was from the NDUS Help Desk with the message that their account would be locked out if they did not authorize the MFA push request. Once email delivery was confirmed, NDUS/CTS Duo administrators sent the MFA push to the users.
What is the risk:	MFA fatigue occurs when employees become desensitized to the frequent occurrence of push notifications. This phishing campaign was designed to test MFA fatigue inside the NDUS/CTS user base and determine the likelihood that a user would authorize a push triggered by a malicious source.
How do we remediate:	Continue to educate end users on how to detect phishing emails and to deny MFA pushes that they did not initiate.

	# of Emails Sent	Approved Duo Push	Denied Duo Push	Reported Phishing
NDUS / CTS TOTAL	164	21 (13%)	18 (11%)	25 (15%)

ES08: PATCHING AND CONFIGURATION MANAGEMENT

What we observed:	While it was obvious that coordinated vulnerability scanning and patch management programs were in place, testing still uncovered a considerable number of critical, high, and medium vulnerabilities and security misconfigurations while scanning the network. While we were able to successfully exploit a handful of discovered vulnerabilities, a solid defense-in-depth strategy rendered many of our attacks unsuccessful. Even though several devices and services were confirmed to have known vulnerabilities, additional protection mechanisms such as firewalls, anti-virus, and endpoint protection software were responsible for halting the attack.
What is the risk:	Known vulnerabilities and flaws are one of the largest avenues of compromise. Out-of-date and unpatched software/firmware contain known vulnerabilities that can be easily compromised. A compromised device could allow malicious insiders or external attackers to gain unauthorized access to network resources.
How do we remediate:	Although the assessment team observed a considerable improvement in the patching efforts demonstrated by each entity, there still needs to be additional resources allocated to patching and flaw remediation efforts. Isolate and restrict access to devices that are unable to be patched or updated. Decommission / retire devices or software that are unable to be patched.

8.12. ACKNOWLEDGMENTS

When analyzing the results of the current assessment, it's important to reflect upon North Dakota's overall cybersecurity posture as opposed to solely focusing on the total number of critical and high findings.

RISK LEVEL	2021 FINDINGS	2023 FINDINGS	DELTA
CRITICAL	5	1	-4
HIGH	57	36	-21
MEDIUM	33	54	+21
LOW	33	39	+6
INFO	0	0	0
TOTAL	128	130	+2

By looking at the table above, one could infer only nominal improvements had been made between the 2021 and 2023 assessments. However, this is not the case.

While numbers alone can be quickly interpreted as better or worse, they often do not represent the true narrative of the assessment.

It is also important to understand that the existence of critical or high findings does not necessarily equate to a failure. Today's threat landscape is extremely volatile and features the constant emergence of new threats, exploits, and vulnerabilities that put organizations at risk. This means that the status of a protected network resource could change to pose a significant risk to your environment in the matter of hours. The constant evolution of the threat landscape highlights the importance to conduct in-depth testing on a consistent basis.

When contrasting the above statistical representation to the true narrative of the 2023 assessment, the assessment team is happy to report that it observed a night-and-day difference in the state's overall security posture. Of the numerous improvements observed, the following two stood out above the rest:

North Dakota University System:

It is difficult to protect yourself from an attack if you are not aware that it is occurring. This sentiment is why we consider the North Dakota University System's adoption and deployment of a robust endpoint detection and response solution the single largest improvement observed during this assessment.

During the previous 2021 assessment, our team was able to consistently launch successful attacks against NDUS resources that were never detected.

With the rollout of Palo Alto's "Cortex XDR" endpoint protection product, NDUS was not only able to proactively thwart the majority of the attacks launched by the assessment team, but it also gave the NDUS staff the much-needed visibility and awareness to detect and respond to these attacks.

While additional staffing is still needed to improve overall detection and response times, the infrastructure for this system is in place and operational, which effectively sets the stage for easy growth and improvement.

8.12. ACKNOWLEDGMENTS (CONTINUED)

North Dakota Information Technology Department:

> Since it is nearly impossible to hack what you cannot access, we felt it was important to recognize ITD's efforts to adopt a "zero-trust" security framework. Make no assumptions, the implementation of a zero-trust framework was no small undertaking and now provides a cutting-edge security model for the state network.
>
> In the previous 2021 assessment, our team easily accessed and pivoted between internal networks by simply connecting our devices. We freely discovered and attacked resources as we moved through the network segments of each respective state office.
>
> Under the new "zero-trust" model, no access was provided by default. Instead, each user was dynamically granted access to specific network resources based on their job role and individual network login. In theory, if a user did not need access to a specific network resource, they would never know that resource existed.
>
> While we can confirm the "zero-trust" model functioned as ITD intended, the assessment team was not aware that access to each individual state office would not be provided. This significantly hindered the assessment team's ability to conduct a thorough and in-depth assessment of each state office as previously done in the 2021 assessment.
>
> Although the assessment team was eventually given the access needed to test resources within the Office of Management and Budget (OMB), ongoing personnel changes within ITD created a 10-month delay (January - September) that prevented the testing of additional state offices as originally planned.
>
> The assessment team cannot stress the importance of conducting penetration testing activities from inside each state office network. Going forward, the scope of this assessment needs to be modified to accommodate the changes associated with transitioning to a "zero-trust" security framework.

When comparing North Dakota's current security posture to what was observed during the 2021 assessment, the respective changes to the NDUS and ITD networks detailed above, represent huge improvements to North Dakota's overall security posture.

Keeping the people and resources of North Dakota safe from cyberattacks is no easy task. A feat of this size is only accomplished with years of hard work, commitment, and planning. While ITD and NDUS are ultimately responsible for the successful execution of these security projects, none of their efforts would be possible without the vision and support provided by the State's Information Technology Committee.

Members of this committee deserve kudos for recognizing the need to stay current with emerging cybersecurity trends and standing behind these projects to ensure they received the necessary resources to be successful.
It has been refreshing to witness the vision, continued support, and improvements made possible by this committee.

On behalf of Secure Yeti, it has been a pleasure to work with the individuals from the State Auditor's office, NDUS, and ITD during this assessment. Stay vigilant and keep up the good work.