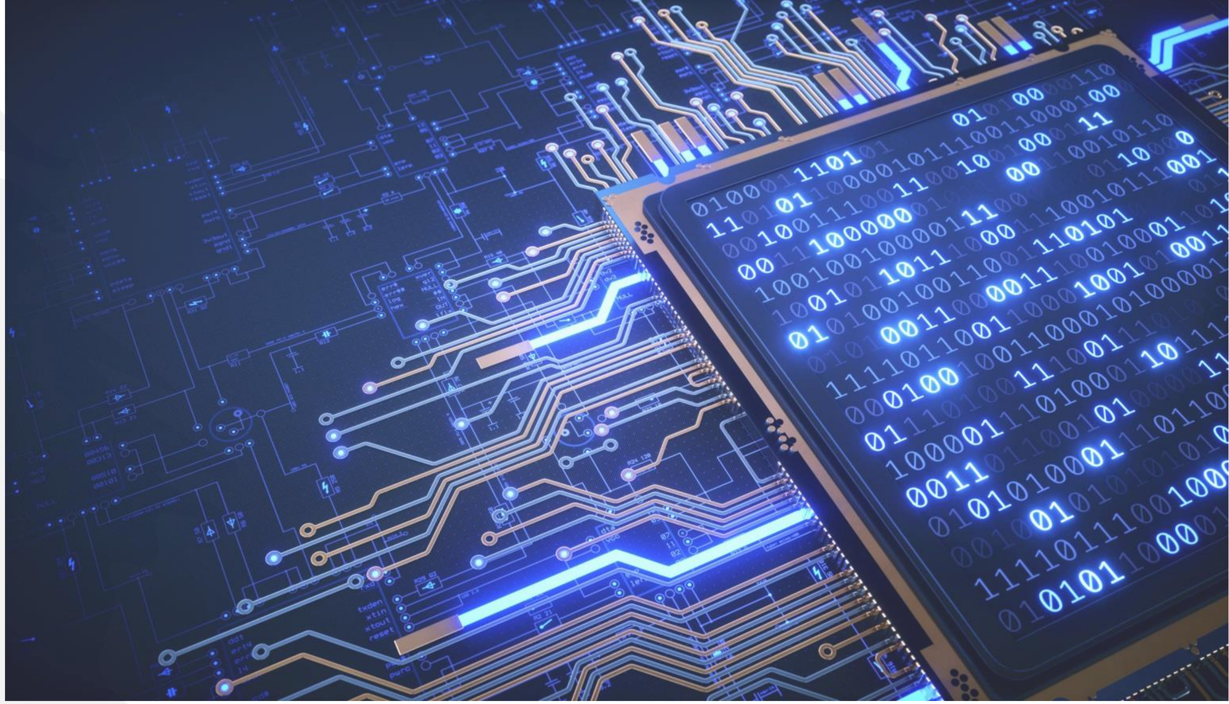
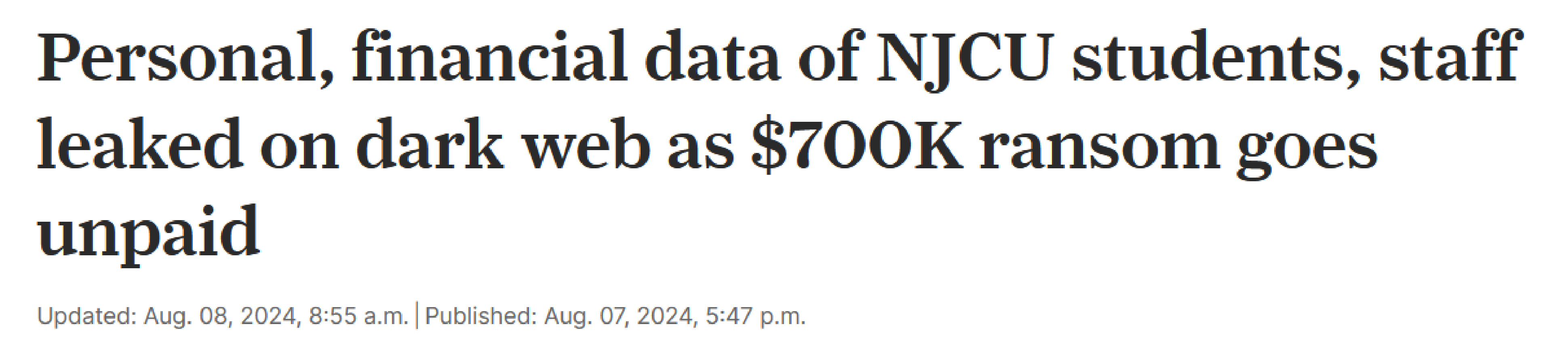
Hudson County Community College Cybersecurity Update

- Introductions
- What and Why?
- Concepts and Strategies
- Activities and Reviews
- Security Awareness, Training, and Planning
- GLBA Compliance
- Future Roadmap



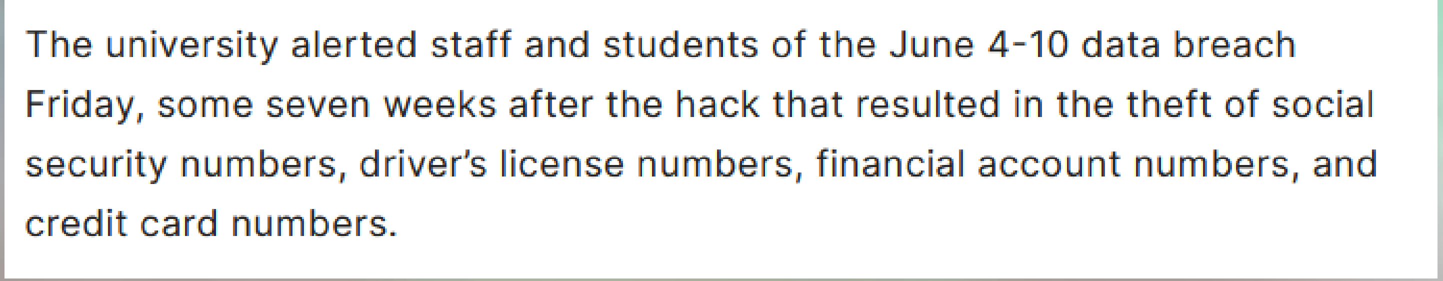
HUDSON COUNTY COMMUNITY COLLEGE

Why?
Recent Cybersecurity Incidents



Personal, financial data of NJCU students, staff leaked on dark web as $700K ransom goes unpaid

Updated: Aug. 08, 2024, 8:55 a.m. | Published: Aug. 07, 2024, 5:47 p.m.



The university alerted staff and students of the June 4-10 data breach Friday, some seven weeks after the hack that resulted in the theft of social security numbers, driver's license numbers, financial account numbers, and credit card numbers.

Higher Education Cybersecurity Focus

CyberSecOp

Only some of the recent attacks that made their way to the media

2024 EDUCAUSE Top 10 listed **"Cybersecurity as a Core Competency"** as the #1 factor in the drive to develop institutional resilience.

New Jersey institutions are still recovering from attacks months ago.

A staggering 79% of schools reported facing attacks and 56% paying a ransom to get their data back.

2023 was the **worst ransomware year** on record for the education sector.

A 105% increase in known ransomware attacks against K–12 and higher education

- Attacks were up 70% (68 vs 116 in 2023)
- Based only on incidents in which a ransom was not paid, the actual number of attacks was probably significantly higher

Higher Education Needs Cybersecurity Focus

CyberSecOp

Average of 277 Days

Time to Breach Detection

Approximately 84%

of all events are caused by humans

Nearly 90%

of ransomware attacks are preventable

"The biggest risk to higher ed continues to be ***reputational damage*** *from data breaches, especially for tuition-based schools. Enrollment competition is so significant that a data breach or loss of student data could tip the scales for a small- to medium-sized institution. Also, many small- to medium-sized schools are being attacked with business email compromise. This can result in* ***financial losses*** *that are a real problem."*

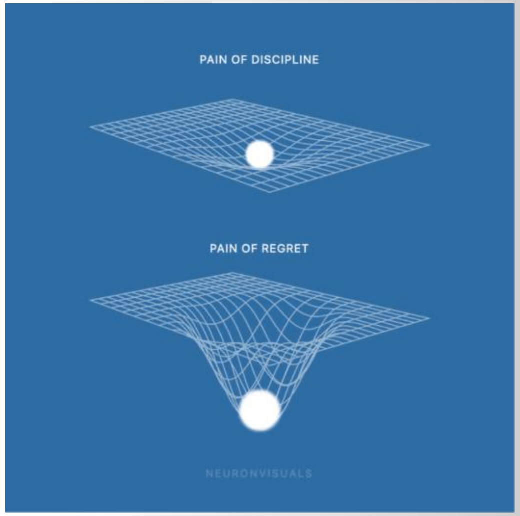
"Schools need to make ***investments in security tools*** *and the people to manage them….. the security landscape is too complex for many small institutions to manage. The current threat landscape requires tools to monitor and report threats, and protocols need to be in place to respond.* ***Without these, it is only a matter of time before real damage is done.****"*

Jason Nairn VP of Information Technology and Security
Collegis Education

Cybersecurity is a Journey, NOT a Destination

No one can reach a 100% cybersecurity level because of four factors:

1. Risk changes constantly
2. Cybercriminals and their tools are continuously getting more sophisticated and better financed
3. Human error is always in play
4. Technology constantly evolves



Overall Approach

CyberSecOp

Enterprise Security

Improve HCC's Cybersecurity and Incident Response capabilities, data security, cloud security, and Identity and Access Management (IAM).
Continue:

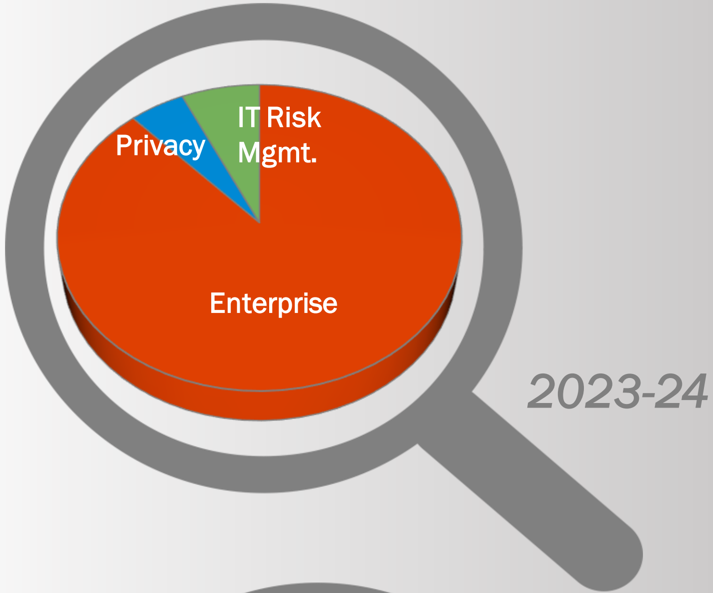
- Internal vulnerability management
- Security awareness training and phishing campaigns
- Computer and server assessment
- Defensive measures via PC and firewall/cloud security controls
- External and web penetration testing
- Dark web scanning

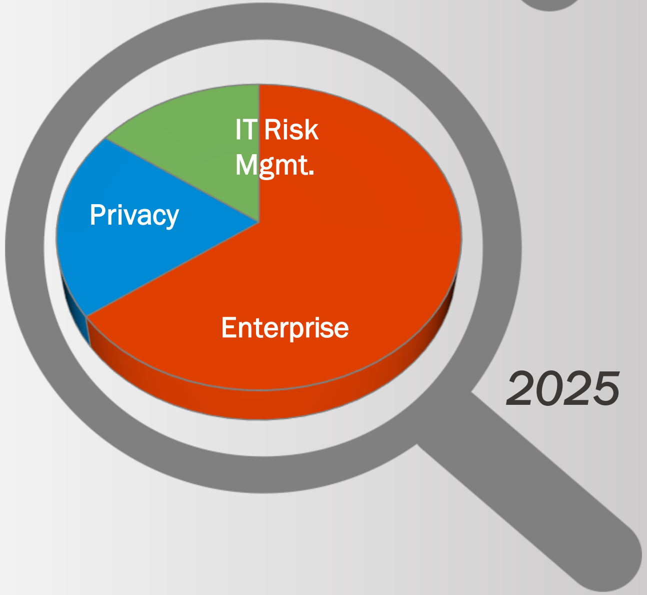
Privacy

Privacy is increasingly regulated and contractual compliance with a focus on federal and State regulations. A solid privacy program is a must for any Higher Education in the U.S. receiving federal or state funding.

IT Risk Management

Risk reduction via Information Technology begins with complete asset management; moves into continued integration of governance, risk, and compliance controls and processes, and requires continuous assessment. IT risk management aims to use security measures and enterprise technology capabilities to prevent or reduce financial or reputational loss to HCCC.



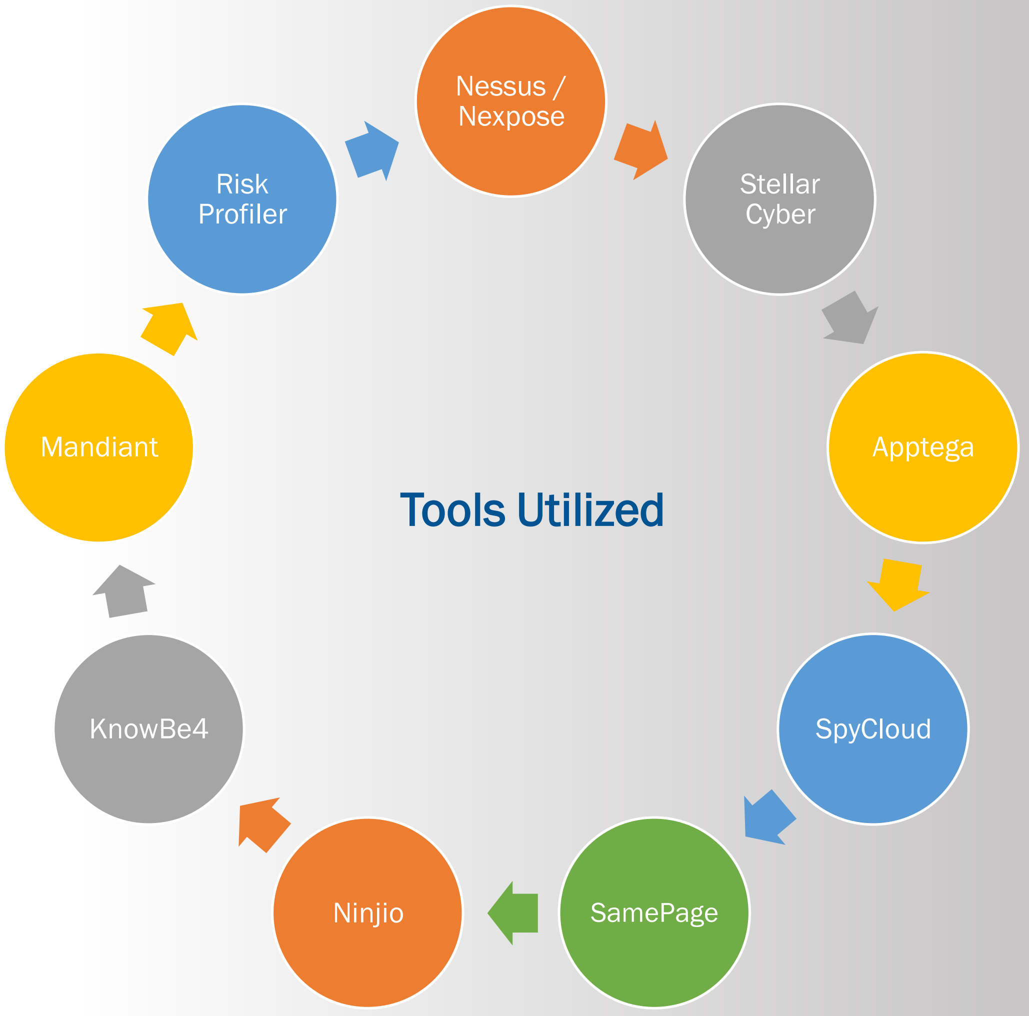


Cybersecurity is a continuous endeavor focused on gradual improvement and risk-based approaches.

Security Program Activities

CyberSecOp

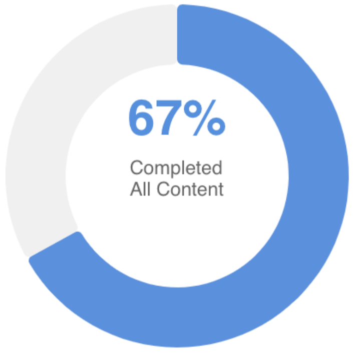
- All Policies and Plans required by Federal and Privacy regulations
- Continued Risk Assessment
- Dark Web Analysis
- Email Security and Review
- External Pen Testing
- Governance, Risk, and Compliance System
- Incident Responders – 24X7
- Internal Vulnerability Scanning
- Phishing Campaigns
- Privacy Program – All Policies and plans
- Security Awareness and Training
- Security Reviews
- Vendor Security
- Vulnerability and Systems Security Team



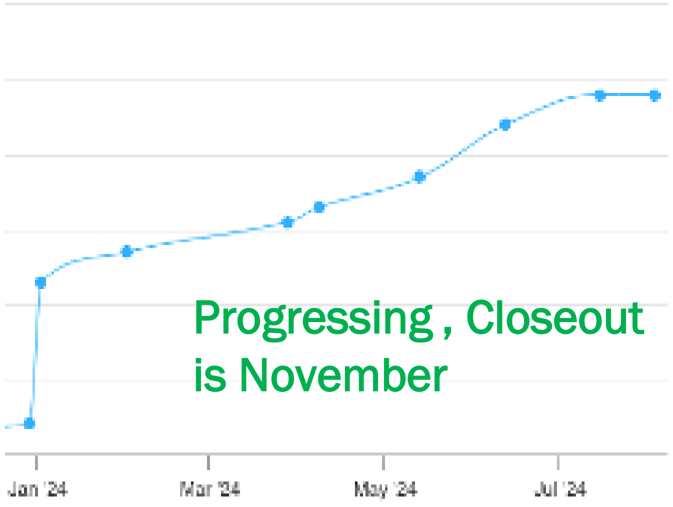
Security Awareness

CyberSecOp

WORK IN PROGRESS

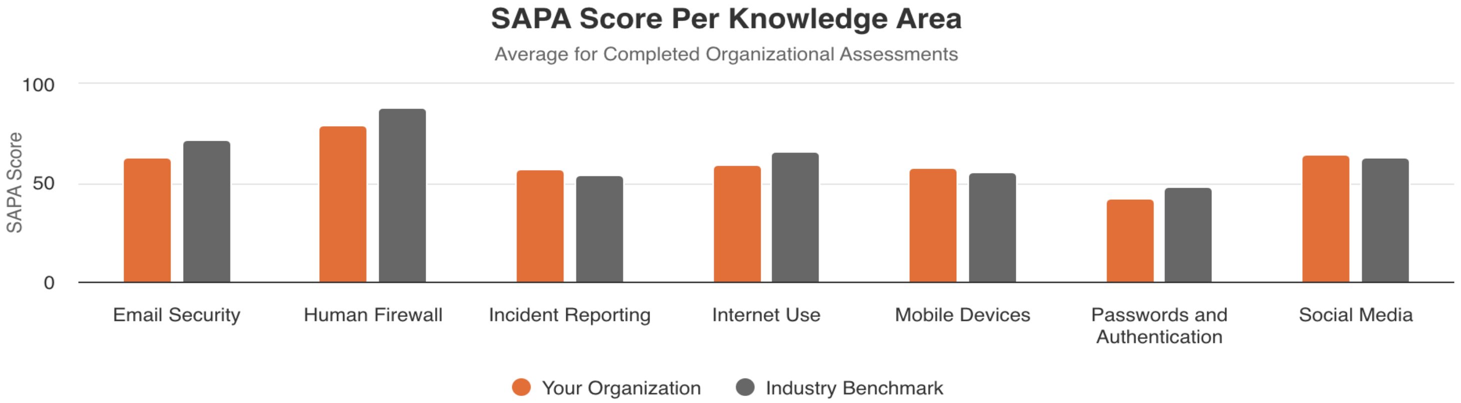


Status **In Progress**



Progressing , Closeout is November

Security Awareness Proficiency Assessment (SAPA)



On Par with Education Industry

Reminder:

Approximately 84%

of all events are caused by humans

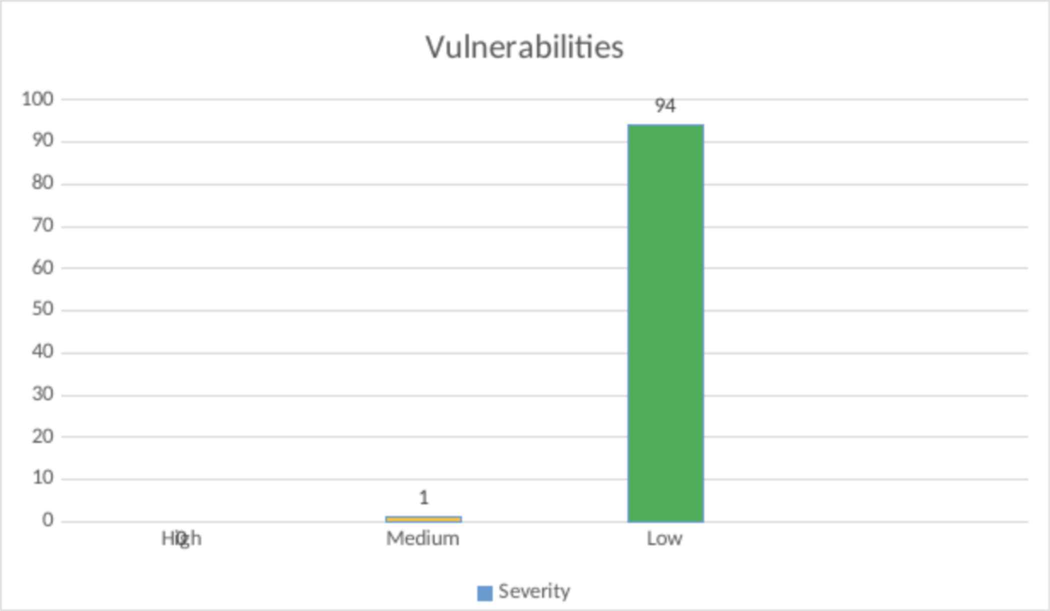
Nearly 90%

of ransomware attacks are preventable

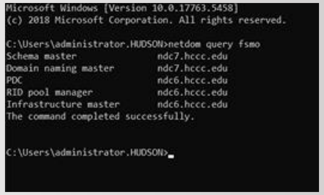
Risk Assessment and Reaction

✓ THOROUGH ANNUAL PENTESTING CONDUCTED

WORK IN PROGRESS THOROUGH ANNUAL INTERNAL SCANNING IS IN PROGRESS



✓ THOROUGH ANNUAL ACTIVE DIRECTORY AUDIT CONDUCTED



```
Microsoft Windows [Version 10.0.17763.5458]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\administrator.HUDSON>netdom query fsmo
Schema master               ndc7.hccc.edu
Domain naming master        ndc7.hccc.edu
PDC                         ndc6.hccc.edu
RID pool manager            ndc6.hccc.edu
Infrastructure master       ndc6.hccc.edu
The command completed successfully.


C:\Users\administrator.HUDSON>_
```

Recommended Changes Made:

- Create a LAPS policy - This helps set a unique complex password for the local administrator account in all domain-joined devices.

- The maximum password complexity has been increased, and password age reduced, per security best practices.

Policy and Plans

CyberSecOp

Professionally reviewed, produced, and updated policies are essential to any security and privacy program and a required part of any higher education institution. CyberSecOp continuously reviews and assists us to create essential HCCC policies.

Some benefits of having proper policies and plans in place:

- Ensuring the confidentiality, integrity, and availability of data.
- Helping to ensure vulnerabilities are remediated quickly.
- Ensuring the proper responsibilities, resources, plans, and programs are in place for cybersecurity.
- Preventing inappropriate, insecure, and unauthorized access and use of HCCC resources.
- Helping to reduce successful phishing attempts.
- Ensuring network, systems, and application changes are secure and do not cause problems.
- Ensuring data is secure and protected at rest, in transit, and in use.
- Ensuring a proper and rapid response to incidents.

100% Improvement of Goal ✓

Current Proposed Policies

- ✓ CYBERSECURITY POLICY
- ✓ VENDOR MANAGEMENT POLICY
- WORK IN PROGRESS ACCESS AND AUTHORIZATION POLICY
- ✓ DEVICE MANAGEMENT POLICY
- ✓ RISK ASSESSMENT POLICY
- WORK IN PROGRESS BUSINESS IMPACT ANALYSIS
- ✓ DATA CLASSIFICATION AND PRIVACY
- ✓ VULNERABILITY MANAGEMENT PROGRAM
- ✓ SECURITY AWARENESS AND TRAINING POLICY

Mature Incident Response Readiness

CyberSecOp

The main goal of HCCC's Incident Management is to manage actual or perceived incidents in a structured manner.

- Restore standard operational service as quickly and efficiently as possible
- Minimizing the adverse impact on business operations
- Responsibilities and the first point of contact may differ and will be determined by the nature of the incident and potential breach.

Severity	Explanation
Severity 1 - Critical	A Severity 1 Incident has a critical impact on HCCC's day-to-day functions, including but not limited to loss of access/control of data and functionality of multiple System/Network infrastructure components. This Severity of incident would have a broad impact, with considerable resources to identify/remediate.
Severity 2 - Moderate	A Severity 2 Incident would be an event/incident impacting a limited group/user or network/system infrastructure. Generally, it is an immediately identifiable/remediated event. Loss/theft of a device containing Hudson CCC content should be considered a Severity 2
Severity 3 – Isolated	A Severity 3 Incident would be considered an incident impacting a single individual or event limited to an isolated instance.

Incident Response Plan, Program, & Process Managed by Security Professionals

		Severity		
		Low	Medium	High
Urgency	Low	5	4	3
	Medium	4	3	2
	High	3	2	1

Urgency	Description
High	Process stopped; organization(s) cannot work
Medium	Process affected; organization(s) cannot use certain functions
Low	Process not affected; change request, new/extra/optimised function

100% Improvement of Goal ✓

✓ INCIDENT RESPONSE PLAN

Now Covering:

- ✓ INCIDENT REPONSE PLAN REVIEW
- ✓ INCIDENT MANAGEMENT PROCESS
- ✓ ROLES AND RESPONSIBILITIES
- ✓ COMMUNICATION FRAMEWORK
- ✓ MONITORING NETWORK/SYSTEMS
- ✓ REMEDIATION AND RECOVERY
- ✓ INCIDENT CLASSIFICATION

HUDSON COUNTY COMMUNITY COLLEGE

Impacts of GLBA Safeguards Rule

The Gramm-Leach Bliley Act (GLBA), enacted in 1999, is a regulation under the Federal Trade Commission (FTC) that requires financial institutions to be transparent about information-sharing practices and to safeguard sensitive information. While GLBA has been around for years, it has impacted colleges and universities more recently within the last couple of years.

GLBA applies to higher education institutions specifically to collect, store, and use student financial records containing personally identifiable information.

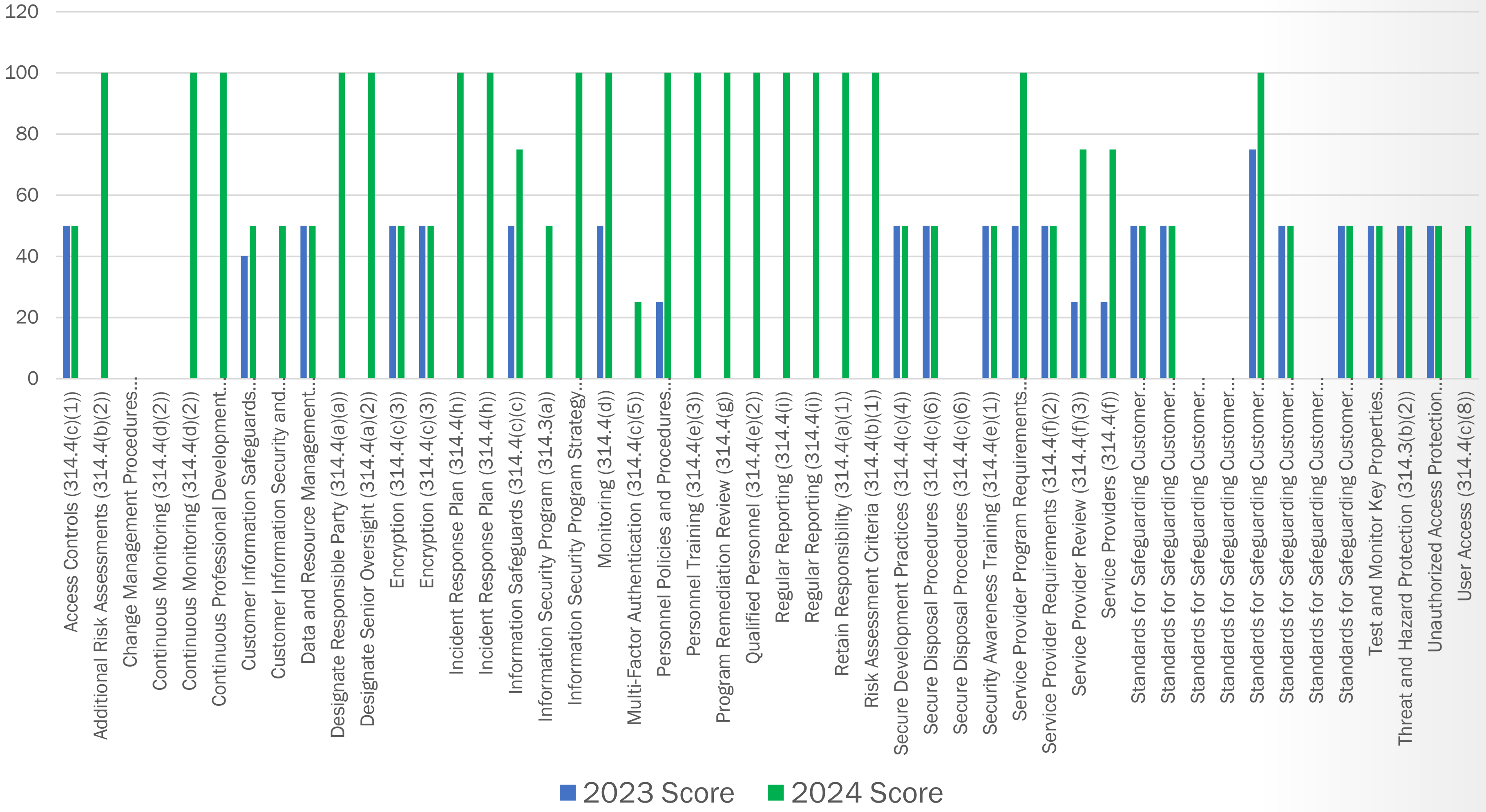
The GLBA Safeguards Rule requires HCCC to have measures to keep customer (**student**) information secure, including with affiliates and service providers.

GLBA Compliance

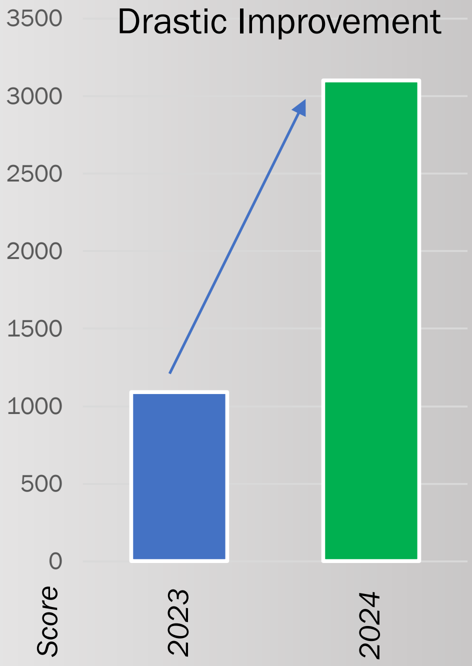
CyberSecOp

2023 - 2024 Security Program Progress

Constant Improvement



Drastic Improvement



2024-2025 Focus Areas on the Roadmap

HUDSON COUNTY COMMUNITY COLLEGE

INTERNAL VULNERABILITY SCANS 🟢

Identifying vulnerabilities and ensuring proper patching

EXTERNAL PEN-TESTING 🟢

Scanning external and web systems for potential weaknesses and vulnerabilities, followed by remediating activity

DATA SECURITY 🟡

Ensure Data mapping, Data classification, and Data security

IT RISK MANAGEMENT 🟠

Governance, Policy, and Compliance

PRIVACY 🟠

Building a mature Privacy program inclusive of regulatory compliance

CYBER DEFENSE 🟡

Proactively defending the organization at all layers

INCIDENT RESPONSE 🟢

Reacting and responding to security threats monitoring for malicious anomalies

SECURITY ASSESSMENT 🟡

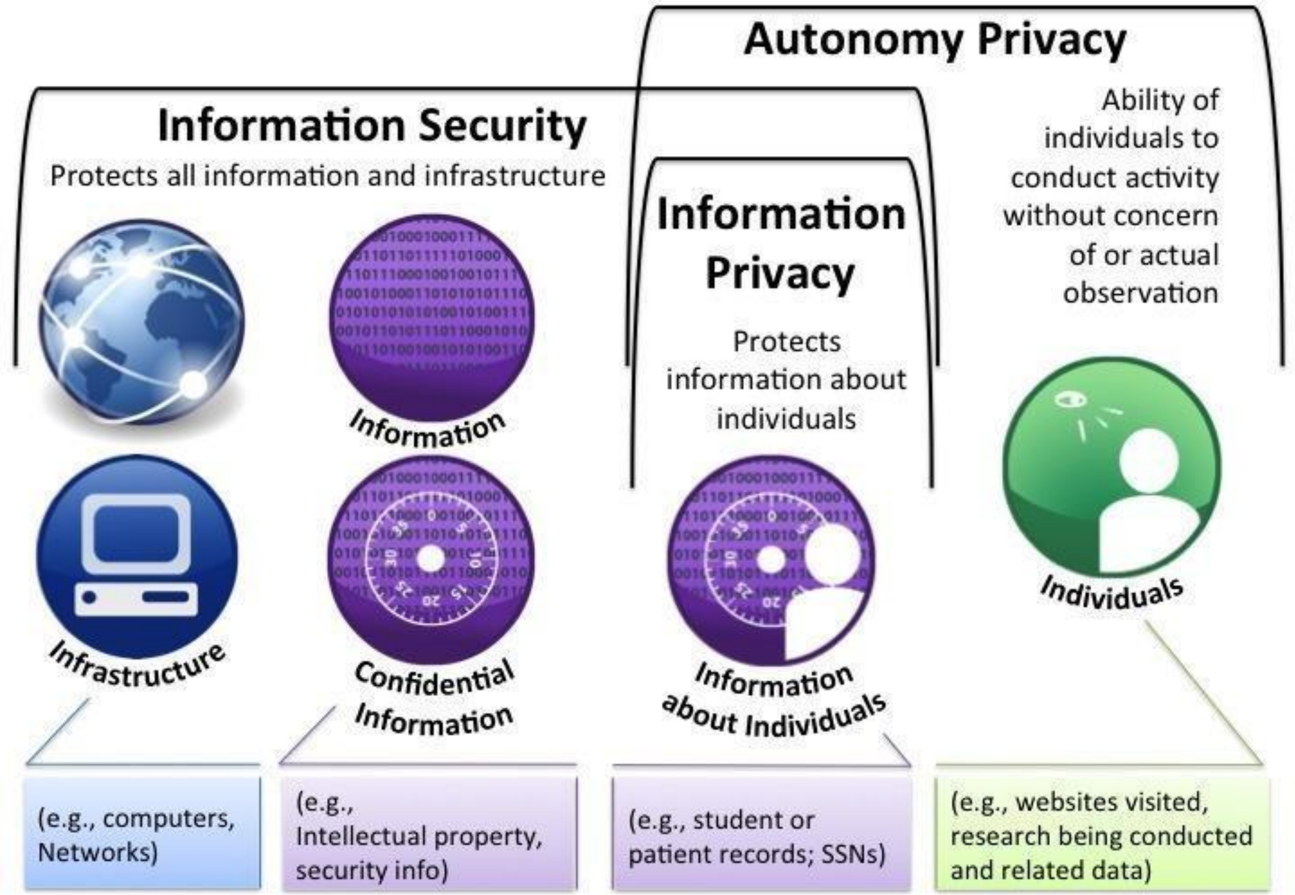
Vendor security, Endpoint assessment, server assessments, and continuous capability assessment

2024-2025 Security Roadmap - Privacy

Defining institutional balance, often facilitating conversations around privacy's importance for students, faculty, staff and the institution.

To protect privacy, institutions should develop their own approach within the bounds of the law. Key considerations include:

- Fostering an environment for free inquiry
- Vigilance against cyber threats
- Individuals' data control
- Collaborative data governance



Autonomy Privacy

Ability of individuals to conduct activity without concern of or actual observation

Information Security

Protects all information and infrastructure

Information Privacy

Protects information about individuals

(e.g., computers, Networks)

(e.g., Intellectual property, security info)

(e.g., student or patient records; SSNs)

(e.g., websites visited, research being conducted and related data)

2024-2025 Security Roadmap – Vendor Risk Management

Evaluate our vendors’ cybersecurity and compliance practices as they can directly impact HCCC’s security, minimizing HCCC’s exposure to preventable risks while performing due diligence on each critical and high-risk vendor.

Vendor Portfolio

Unify all vendors to our portfolio for ease of use.

Vendor Ratings

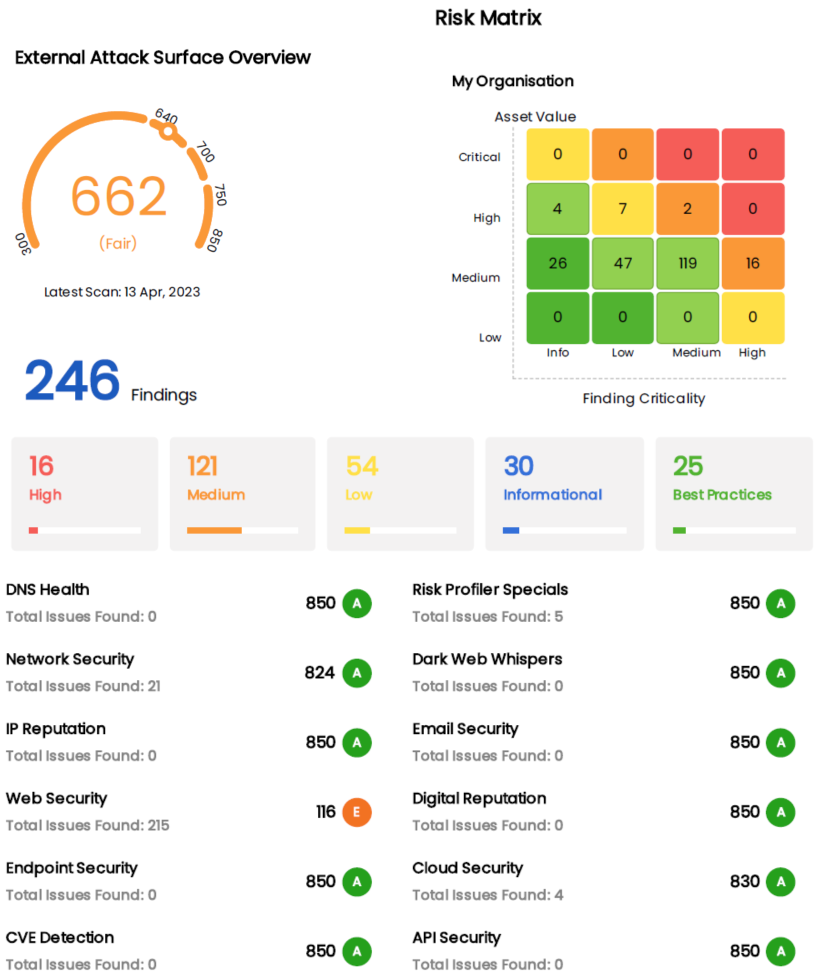
Enables in-depth vendor ratings in near real-time.

Compliance

Includes mappings to most industry compliance standards including GLBA, NIST, SOC, ISO

Remediation

Mitigate risks by automating risk notifications.



External Attack Surface Overview

662
(Fair)

Latest Scan: 13 Apr, 2023

246 Findings

Risk Matrix

My Organisation

Asset Value	Info	Low	Medium	High
Critical	0	0	0	0
High	4	7	2	0
Medium	26	47	119	16
Low	0	0	0	0

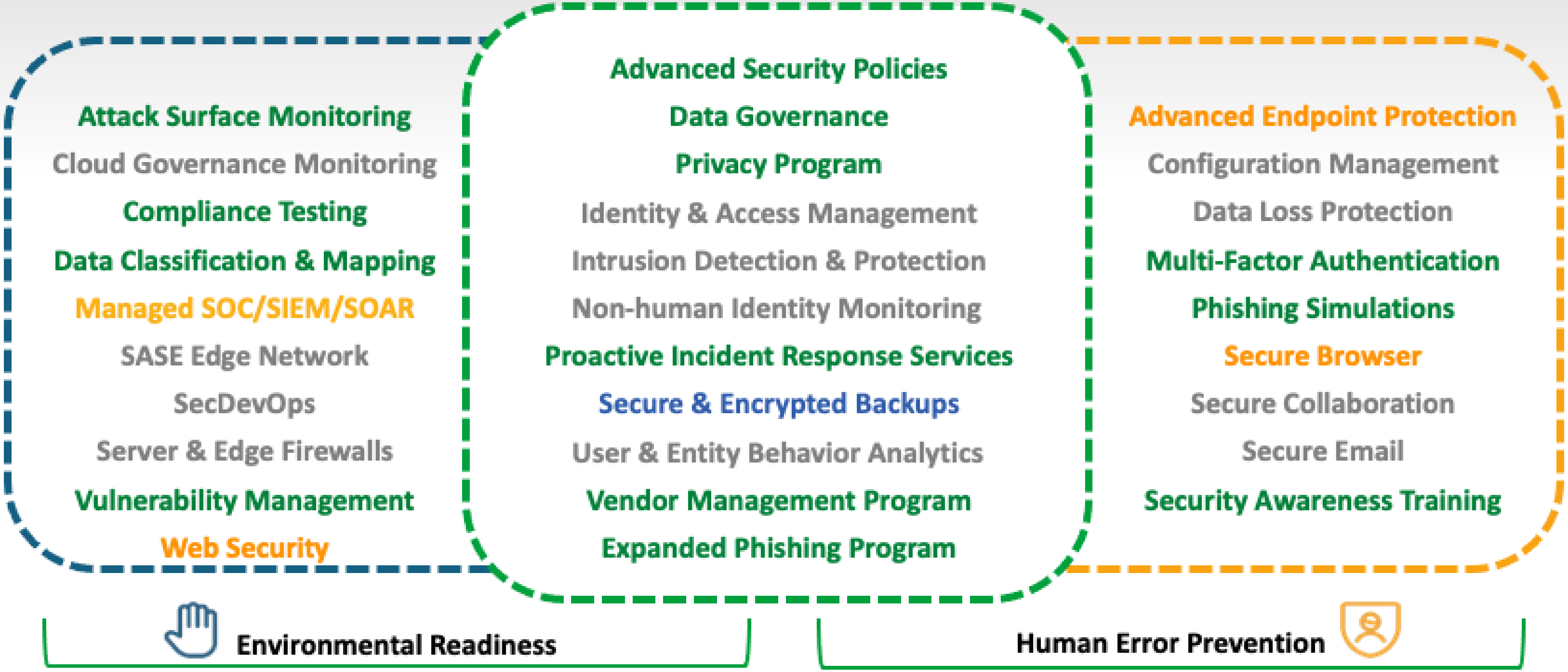
Finding Criticality

16 High	121 Medium	54 Low	30 Informational	25 Best Practices

DNS Health Total Issues Found: 0	850	A	Risk Profiler Specials Total Issues Found: 5	850	A
Network Security Total Issues Found: 21	824	A	Dark Web Whispers Total Issues Found: 0	850	A
IP Reputation Total Issues Found: 0	850	A	Email Security Total Issues Found: 0	850	A
Web Security Total Issues Found: 215	116	E	Digital Reputation Total Issues Found: 0	850	A
Endpoint Security Total Issues Found: 0	850	A	Cloud Security Total Issues Found: 4	830	A
CVE Detection Total Issues Found: 0	850	A	API Security Total Issues Found: 0	850	A

A Different View of Current and Planned activity

Previously In Place
Currently in focus
In Focus next year



Attack Surface Monitoring
Cloud Governance Monitoring
Compliance Testing
Data Classification & Mapping
Managed SOC/SIEM/SOAR
SASE Edge Network
SecDevOps
Server & Edge Firewalls
Vulnerability Management
Web Security

Advanced Security Policies
Data Governance
Privacy Program
Identity & Access Management
Intrusion Detection & Protection
Non-human Identity Monitoring
Proactive Incident Response Services
Secure & Encrypted Backups
User & Entity Behavior Analytics
Vendor Management Program
Expanded Phishing Program

Advanced Endpoint Protection
Configuration Management
Data Loss Protection
Multi-Factor Authentication
Phishing Simulations
Secure Browser
Secure Collaboration
Secure Email
Security Awareness Training

Environmental Readiness

Human Error Prevention

HUDSON
COUNTY
COMMUNITY COLLEGE

CYBERSECURITY IS A JOURNEY, NOT A DESTINATION.
STAY COMMITTED TO CONTINUOUS IMPROVEMENT
www.newpush.com

Thank you!

Trisha Clay
Associate Vice President for ITS and
Chief Information Officer
pclay@hccc.edu
201-360-4351
https://www.hccc.edu/administration/its/index.html