PRIVACY MATTERS @ UBC

UBC CORE CYBERSECURITY TOOLS FOR NETWORKS AND ENDPOINTS

Don Thompson, Chief Information Security Officer

Larry Carson, Associate Director, Information Security Management

THE UNIVERSITY OF BRITISH COLUMBIA

Please Note:

The information contained in this presentation is confidential and is not to be reproduced or distributed in any form outside of UBC or UBC-related activities. The use of the information for assigned UBC student work is acceptable.

PART 1 - THREATS

Part 2 – Security, to come at a later date

INCIDENT RESPONSE

SAMPLE

February 2022

Reported IT Security Incidents**

1295

(YTD: 2162)

49%*

	#	YTD
Compromised accounts	4	13
Due to phishing	*0*	*1 (8%)*
Devices reported stolen	2	3
Unencrypted	*1*	*1 (33%)*

** Increase/decrease from last month*

*** Does not include tickets related to Self-Phishing*

Sources: ServiceNow, Information Security Management

INCIDENT RESPONSE

SAMPLE

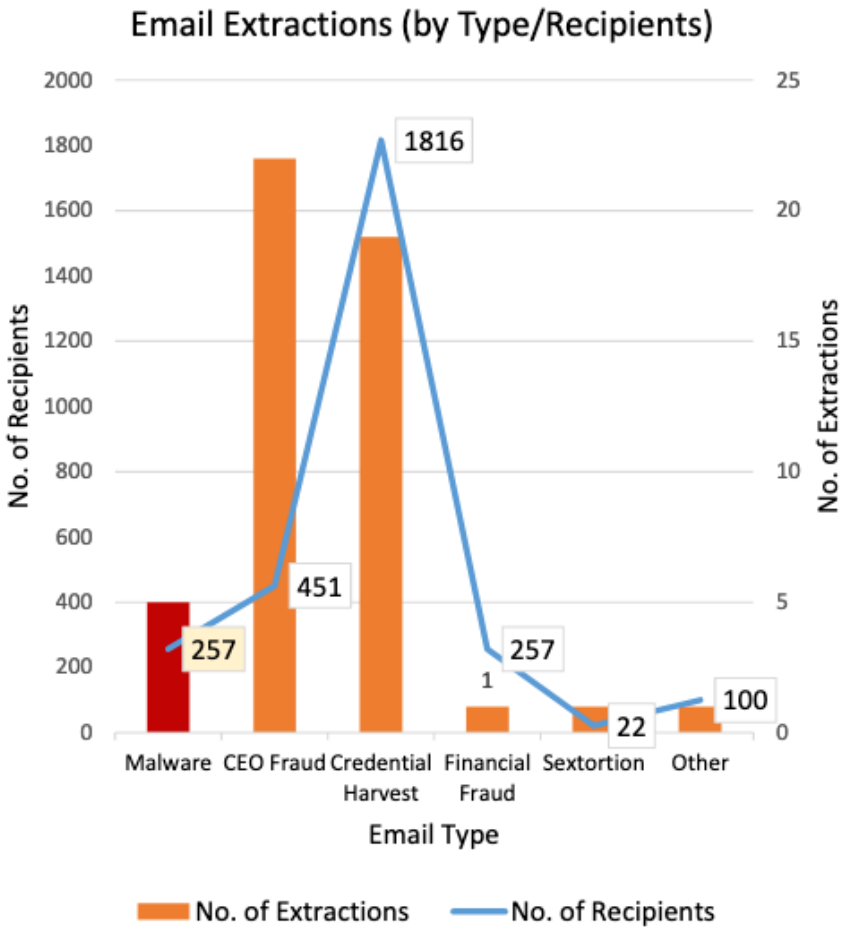
February 2022

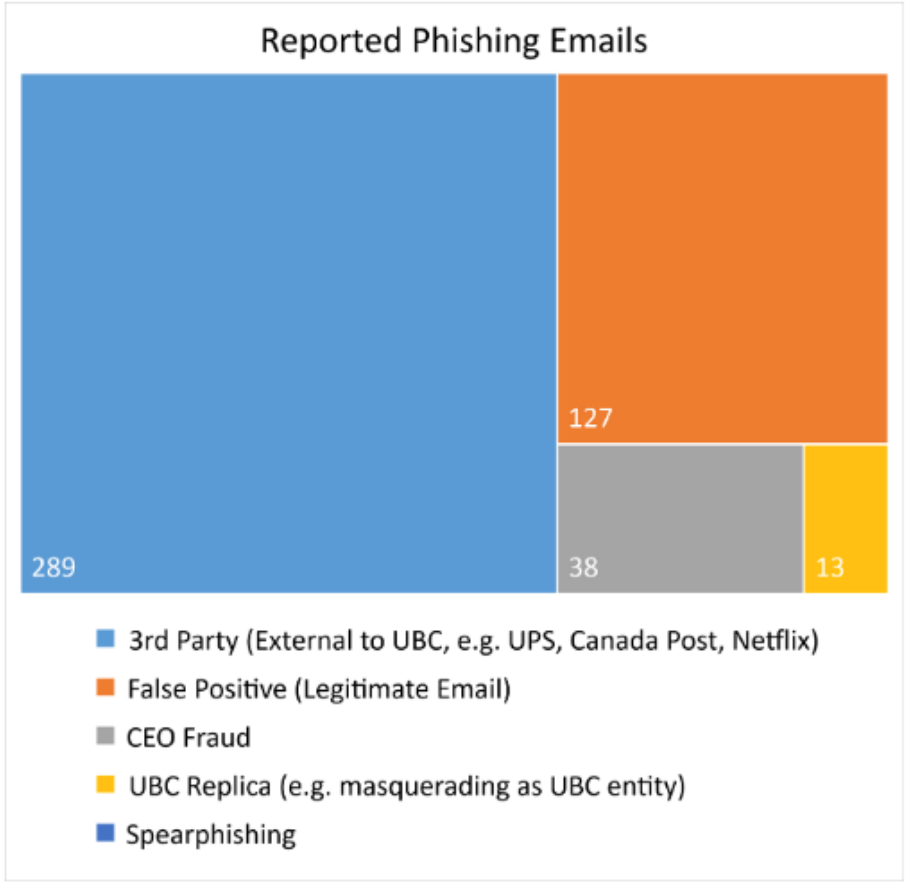
Malicious Email

No. Requiring Automatic Extraction	49 (YTD: 85)
No. of Recipients	2903 (YTD: 16.9K)

Reported Phishing Emails
467 (YTD: 848)

Reported Spam Emails
102 (YTD: 1677)





Sources: ServiceNow, Information Security Management

PRIVACY MATTERS @ UBC

IDENTITY AND ACCESS

Multi-Factor Authentication

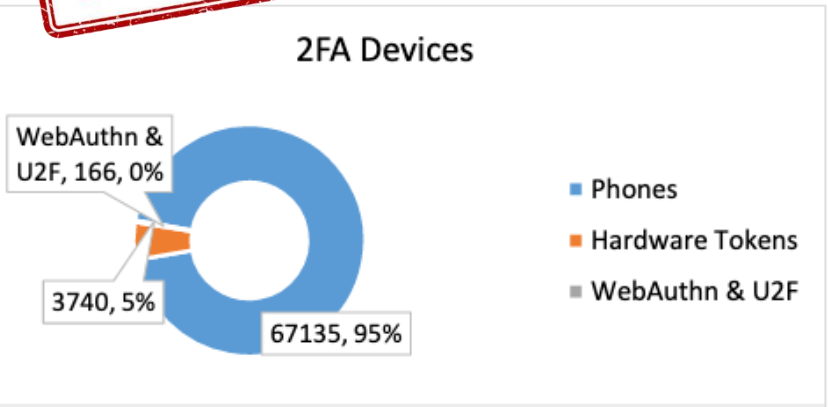
Approved MFA Challenges
3.9 M

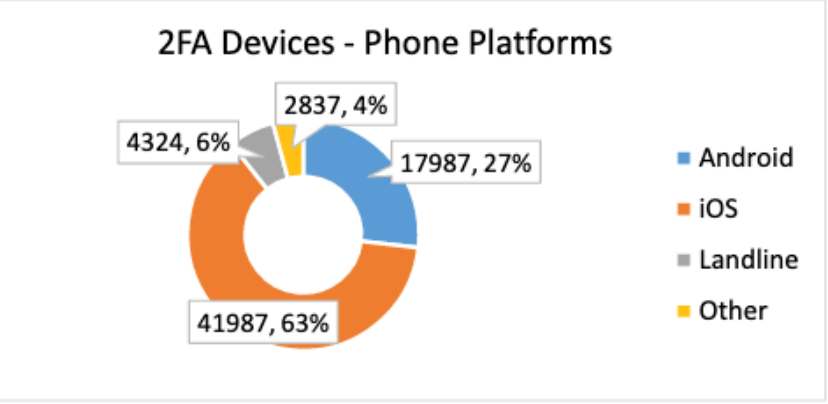
Total Active Users
42.5 K
2%*

Authentication Protocols & Gateways Protected
15

DUO	#	YTD
Fraud Reports	21	48
Lockouts	64	162
Denied authentication requests from anonymous VPNs or Tor	34	135

** Increase/decrease from last month*





Phone Security Warnings	#	%
Screen Unlocked	1565	2.3%
Biometrics Disabled	8369	12.5%
Unencrypted	4743	7.1%

Sources: DUO, Identity and Access Management (IAM)

MALICIOUS INBOUND TRAFFIC

SAMPLE

February 2022

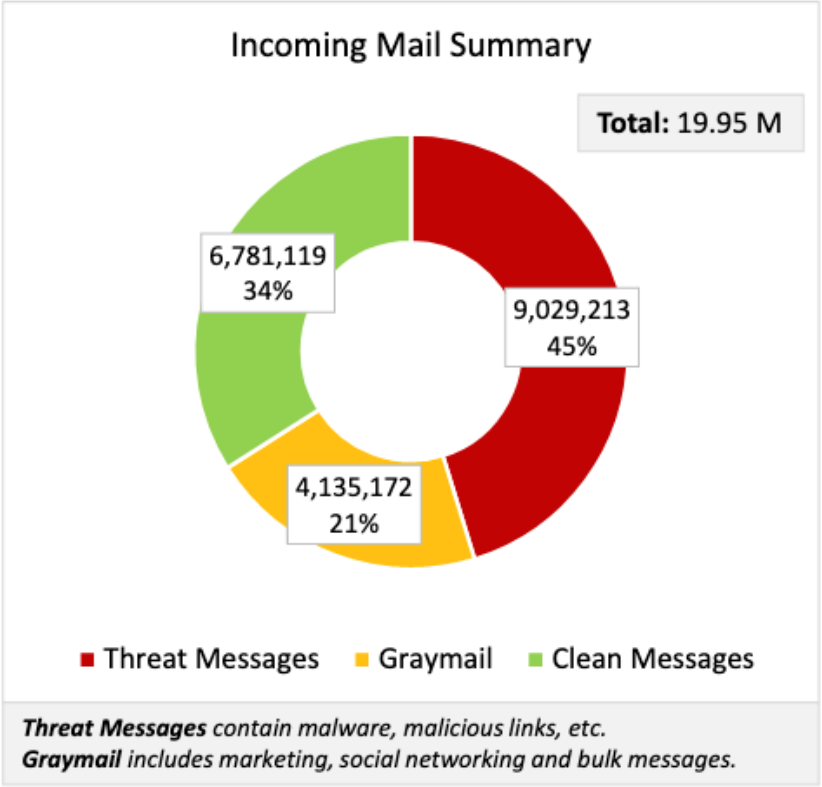
Next Generation Firewall

Malicious Events Blocked at Border
5.2 B

No. of Blocked Connections (by Type)	
Attackers	4.59 B
UBC Blocklist	147.8 M
Malware	415.2 M
Phishing	11.34 M
Command and Control	2.65 M
Blocked Intrusion Events	1.11 M

Email Security Appliance

Malicious Emails Blocked
9.03 M



Threat Messages *contain malware, malicious links, etc.*
Graymail *includes marketing, social networking and bulk messages.*

Sources: Next Generation Firewall (NGFW), Cisco Security Management Appliance (SMA)

PRIVACY MATTERS @ UBC

MALICIOUS OUTBOUND TRAFFIC

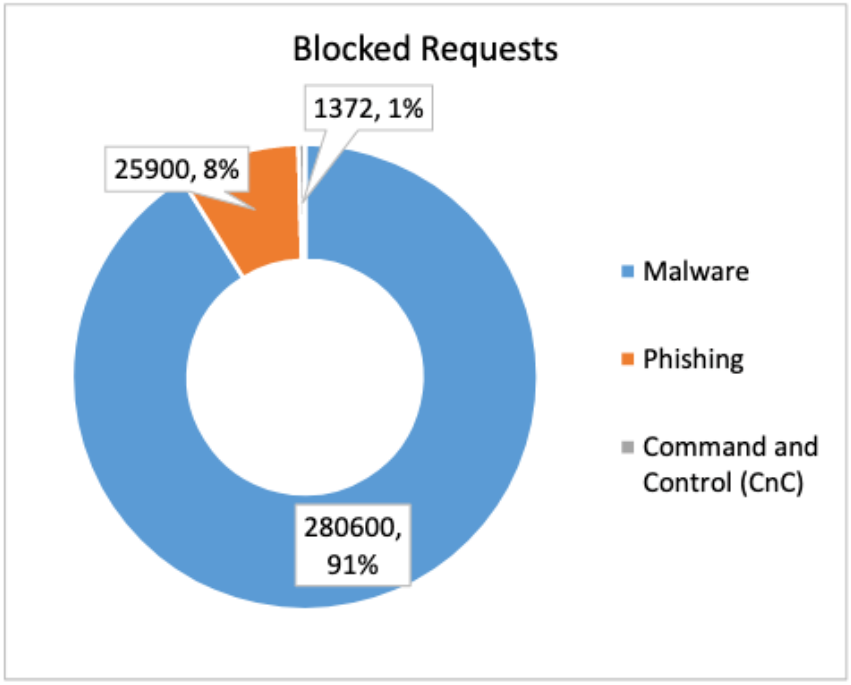
SAMPLE

February 2022

DNS Protection

Cisco Umbrella	
Total no. of requests	1.2 B
No. of blocked requests to potentially harmful websites*	232.5 K (0.02%)

** Blocked sites include known malware, phishing, command & control.*



Sources: Next Generation Firewall (NGFW), Cisco Umbrella, Cisco Security Management Appliance (SMA)

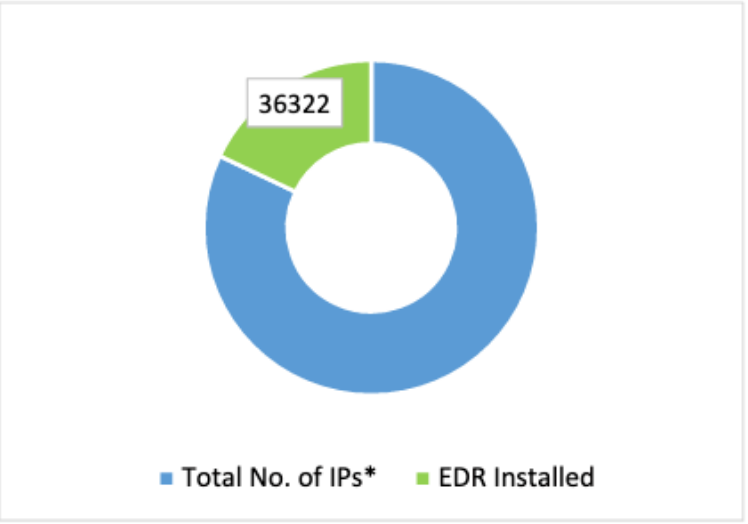
PRIVACY MATTERS @ UBC

ENDPOINT DETECTION & RESPONSE

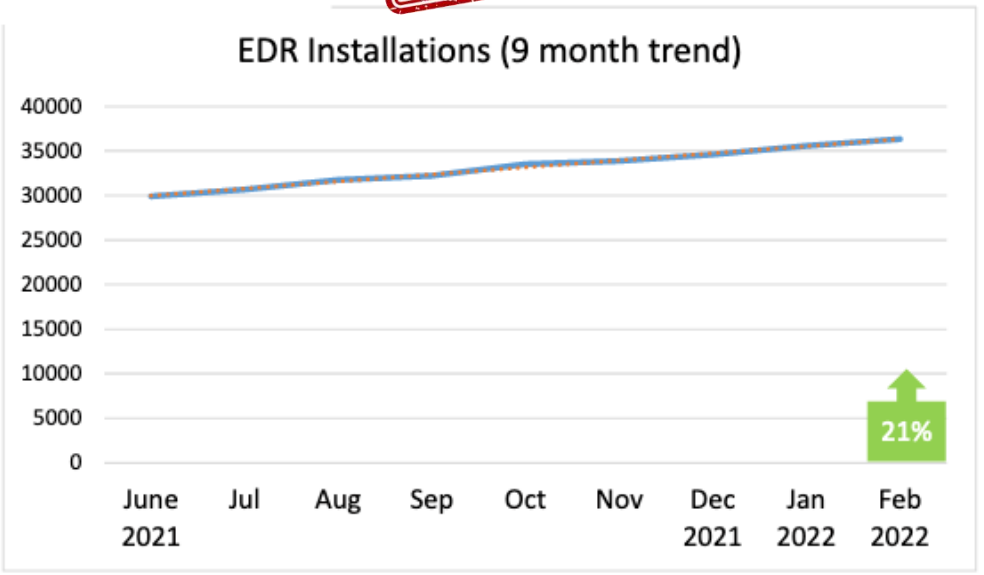
SAMPLE

February 2022

No. of Installations (to date)	
CrowdStrike	**5881**
Workstations	*2145 (+11)*
Servers	*3660 (+156)*
Domain Controllers	*76 (-1)*
Cisco Secure Endpoint (AMP)	**30441**
Workstations	*30183 (+602)*
Servers	*258 (-5)*



** IPv4 address space (Administrative, Teaching and Research networks). Includes routers, switches, IP phones*



Cisco Secure Endpoint (AMP)	#	YTD
Exploits prevented	9600	11510
Malicious files quarantined	4970	13200
Threat Grid submissions	5270	9100
Files scanned	629 M	1.18 B
CrowdStrike Falcon Sensor Detections	**#**	**YTD**
True Positive	10	15
False Positive	54	108

Sources: Cisco Secure Endpoint, CrowdStrike Falcon Sensor

PRIVACY MATTERS @ UBC

VULNERABILITY SCANNING

SAMPLE

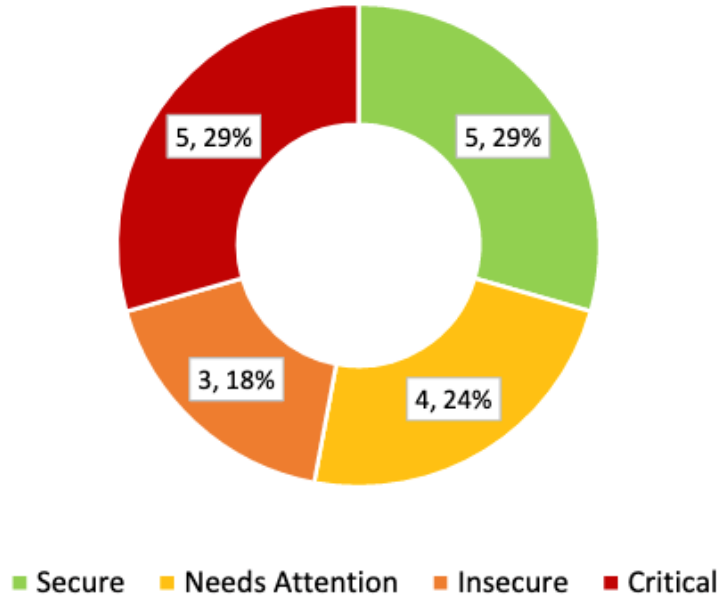
February 2022

Web App Vulnerability Scans (WAVS)

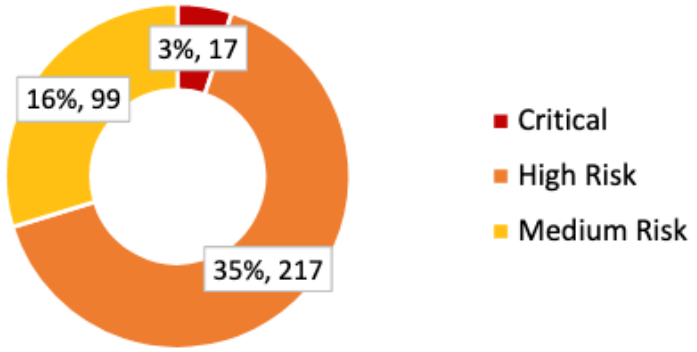
No. of completed scans*	17 (YTD: 40)
No. of active issues (to date)	615
No. of unique websites scanned (to date)	45

** Includes full scans and retests*

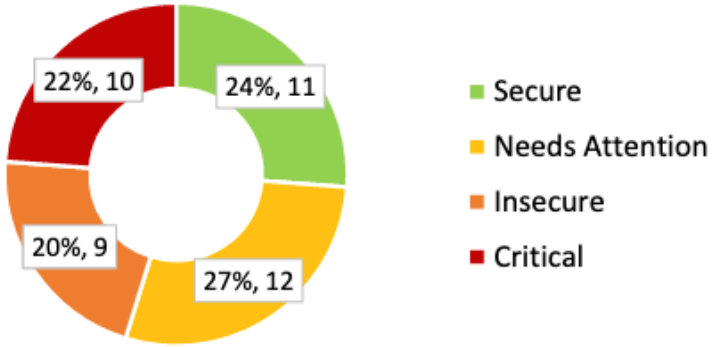
Completed Scans



Active Critical, High & Medium Risk Issues



Vulnerability Status of Unique Websites Scanned (to date)



Sources: Netsparker (WAVS)

PRIVACY MATTERS @ UBC

VULNERABILITY SCANNING

February 2022

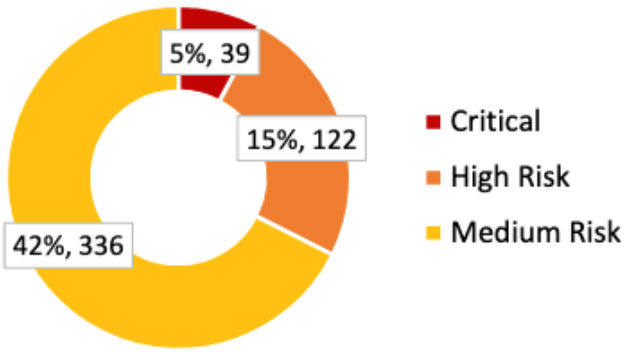
SAMPLE

NESSUS Scans (External)

Vulnerable IPs*	Onboarded Groups
10,831	27

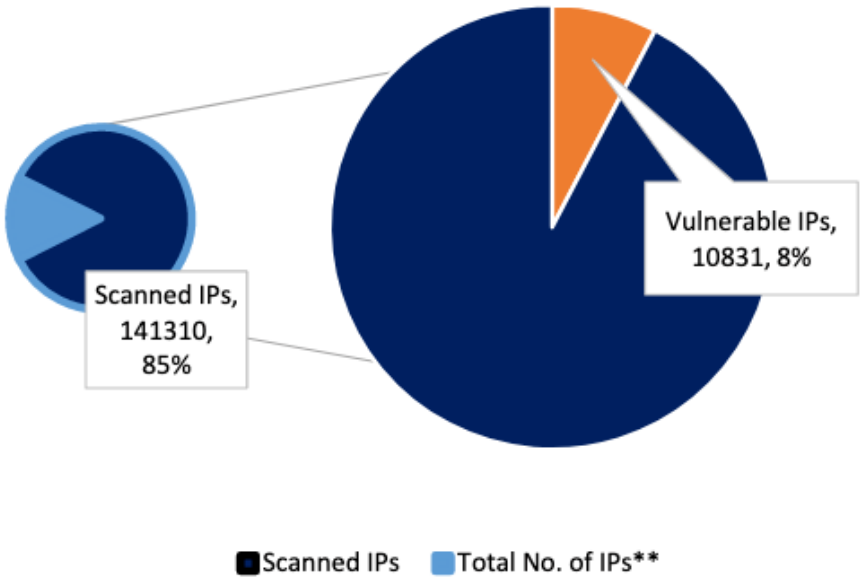
** Internet-facing only. IPs may host multiple websites.*

Unique Vulnerabilities Detected

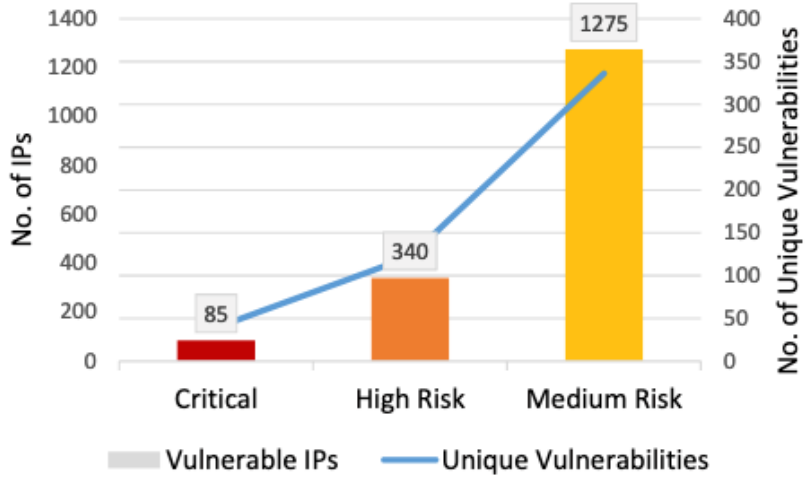


Total: 795

Scanned vs. Vulnerable Internet-facing IPs



Vulnerable IPs



Sources: NESSUS

PRIVACY MATTERS @ UBC

TRAINING

February 2022

SAMPLE

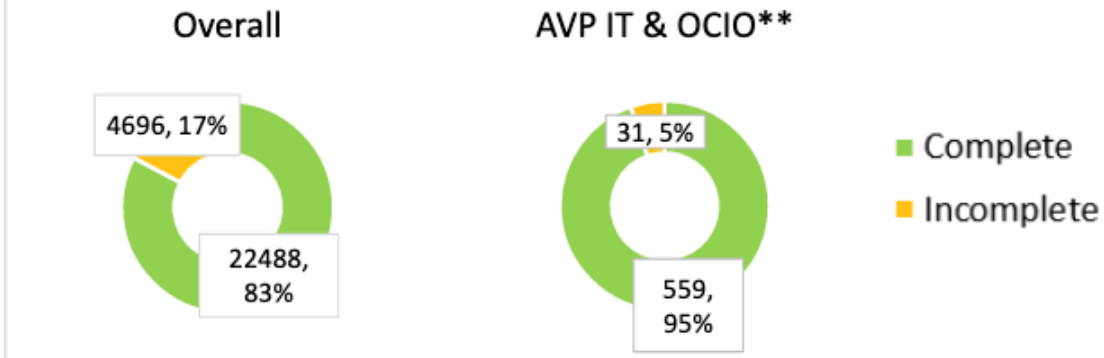
Privacy and Information Security Fundamentals

Target Population	27184
Part 1	
Total Completion	22488
% Complete	83%
Part 2	
Total Completion	16077
% Complete	59%

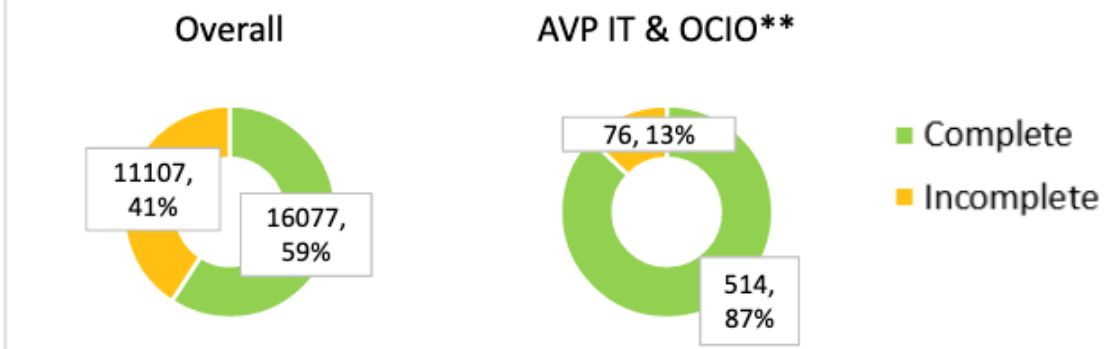
0.4%*

** Increase/decrease from last month*

Part 1



Part 2



*** Includes AVP IT, Office of the CIO, and Okanagan IT.*

Sources: WorkDay, PrISM Safety and Risk Services

PRIVACY MATTERS @ UBC

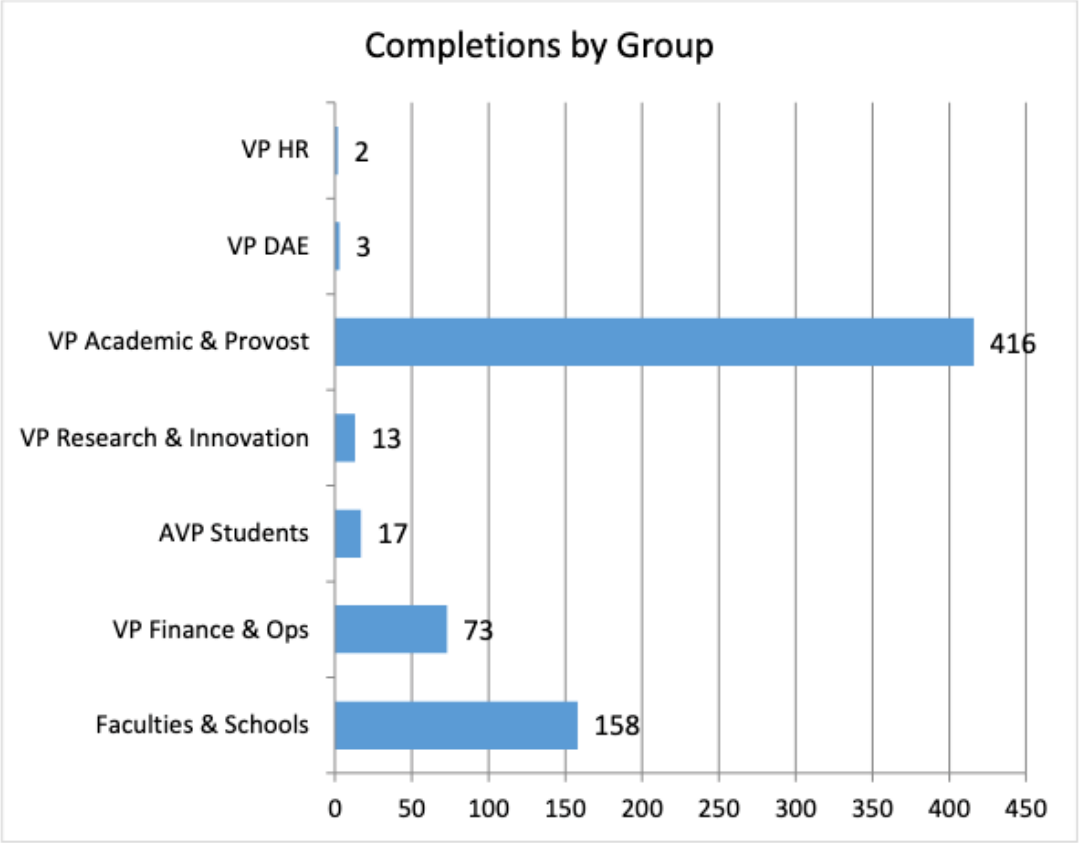
SAMPLE

Privacy and Information Security for IT Professionals

Soft Launch	May 2021
Total Completed	682
AVP IT & OCIO	
Target Population**	590
Total Completed	382
% Complete	65%

** Increase/decrease from last month*

*** Includes AVP IT, Office of the CIO, and UBCO IT.* ***Not all roles are technical – target population to be defined in Workday (pending).***



Sources: WorkDay, PrISM Safety and Risk Services

TRAINING

SAMPLE

Latest Self-Phishing Campaign

Latest campaign

Data current as of: Aug 15, 2022

43,329
users targeted in the campaign

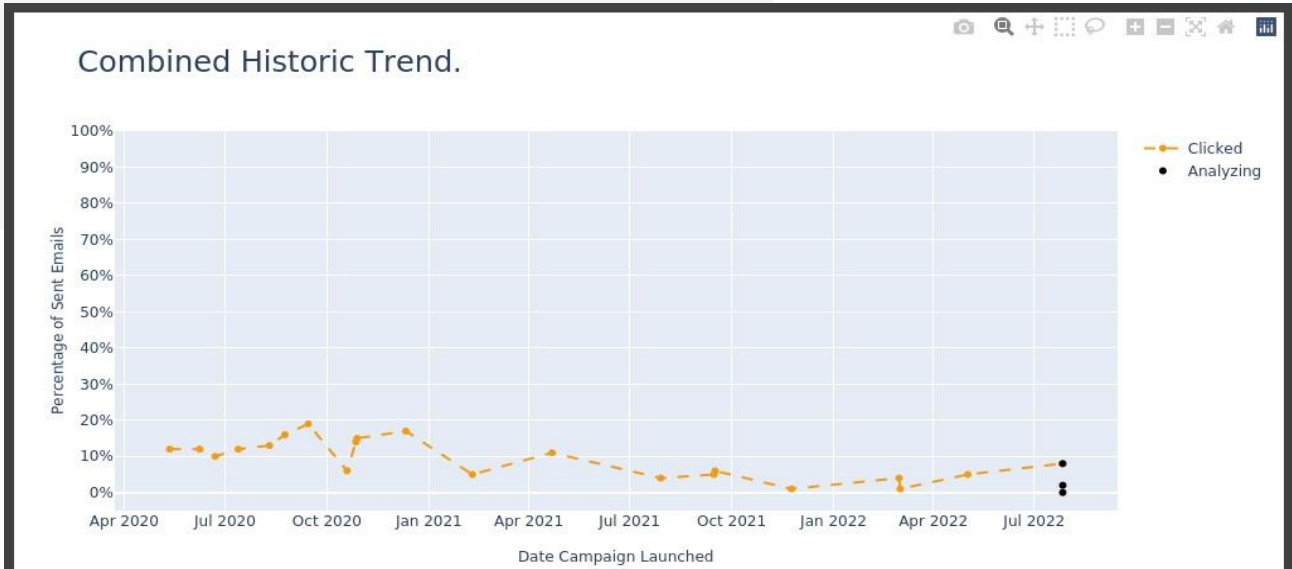
25%
opened the email

8.6%
clicked on the link

0.42%
submitted their data

2.6%
Reported the phish

Date: August 15, 2022
Targets: UBC
Campaign Type: Credential Harvest



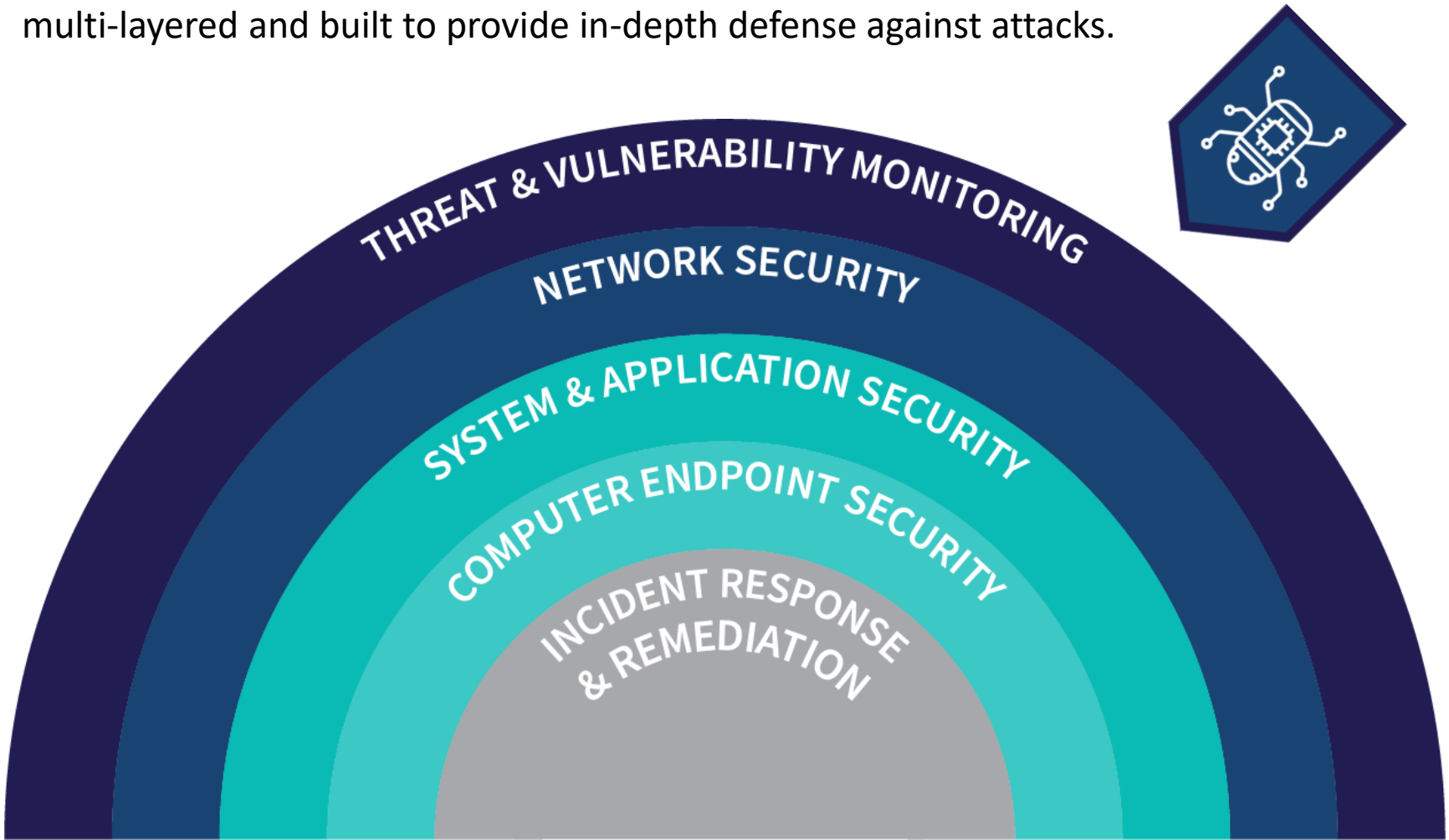
Sources: GoPhish

END OF PART 1 – THREATS
NEXT UP PART 2 - SECURITY

PRIVACY MATTERS @ UBC

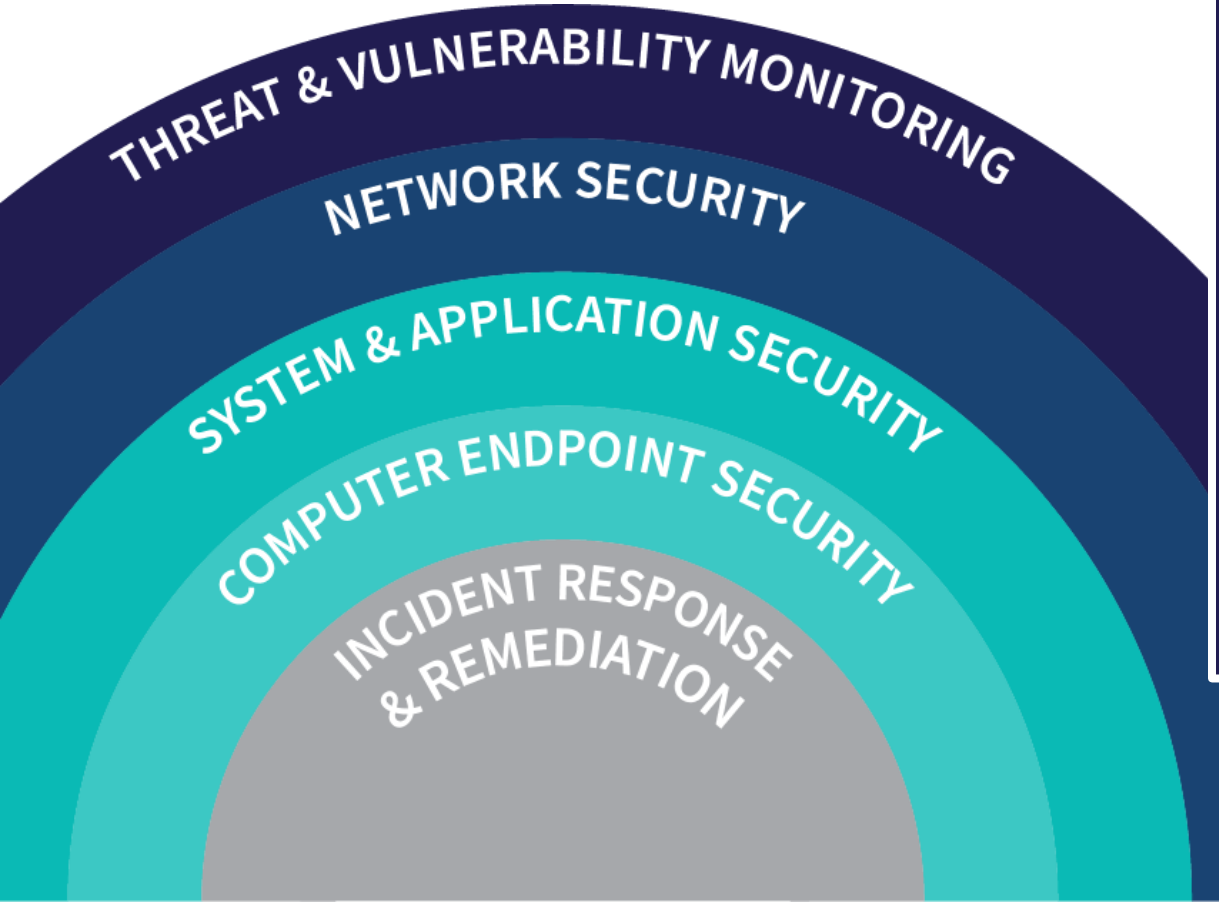
A MULTI-LAYERED APPROACH TO RANSOMWARE PROTECTION

- UBC's **core cybersecurity tools** for protection against ransomware is multi-layered and built to provide in-depth defense against attacks.



PRIVACY MATTERS @ UBC

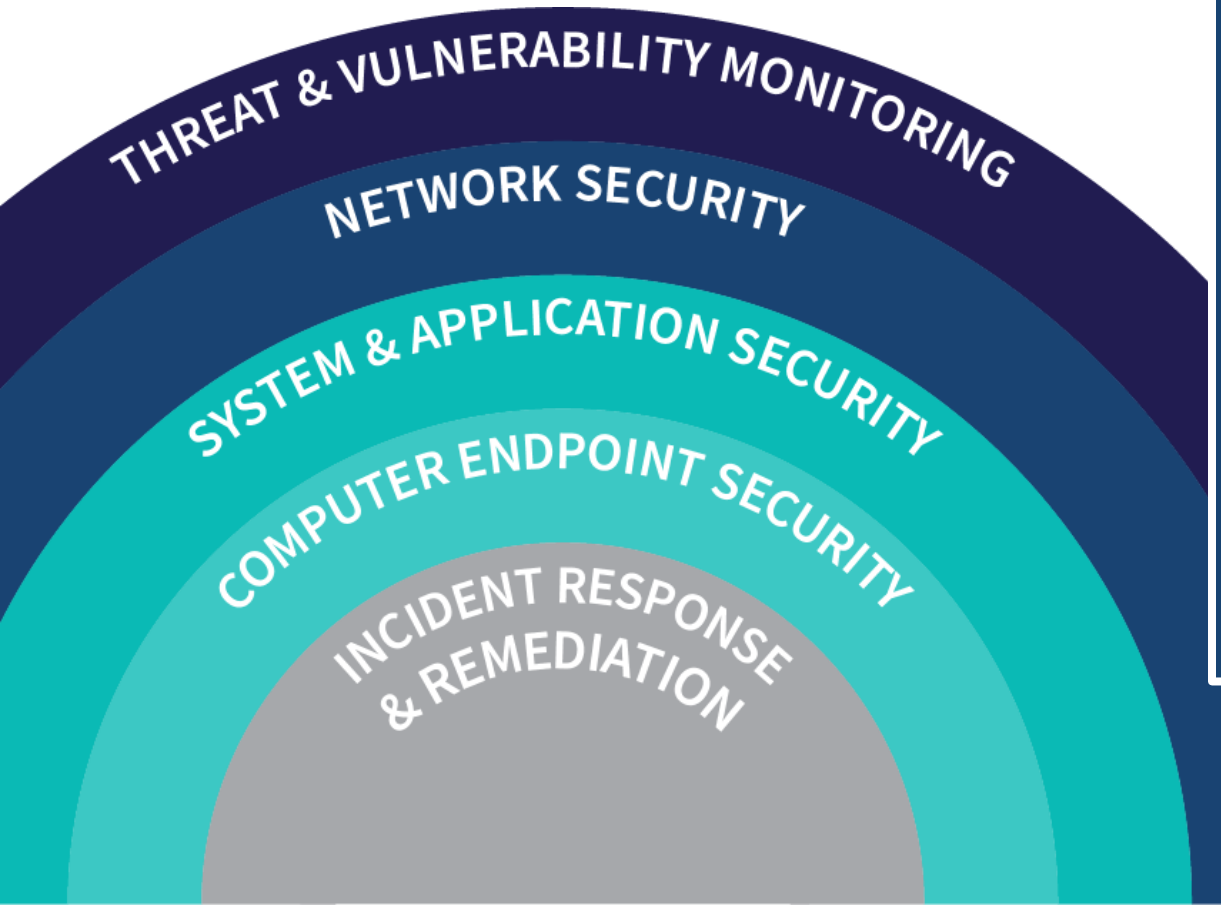
THREAT & VULNERABILITY MONITORING



- Threat feeds
- Threat intelligence
- Real-time monitoring
- Shared Security Operations Centre (SSOC)
- Vulnerability sandbox
- Vulnerability assessment

PRIVACY MATTERS @ UBC

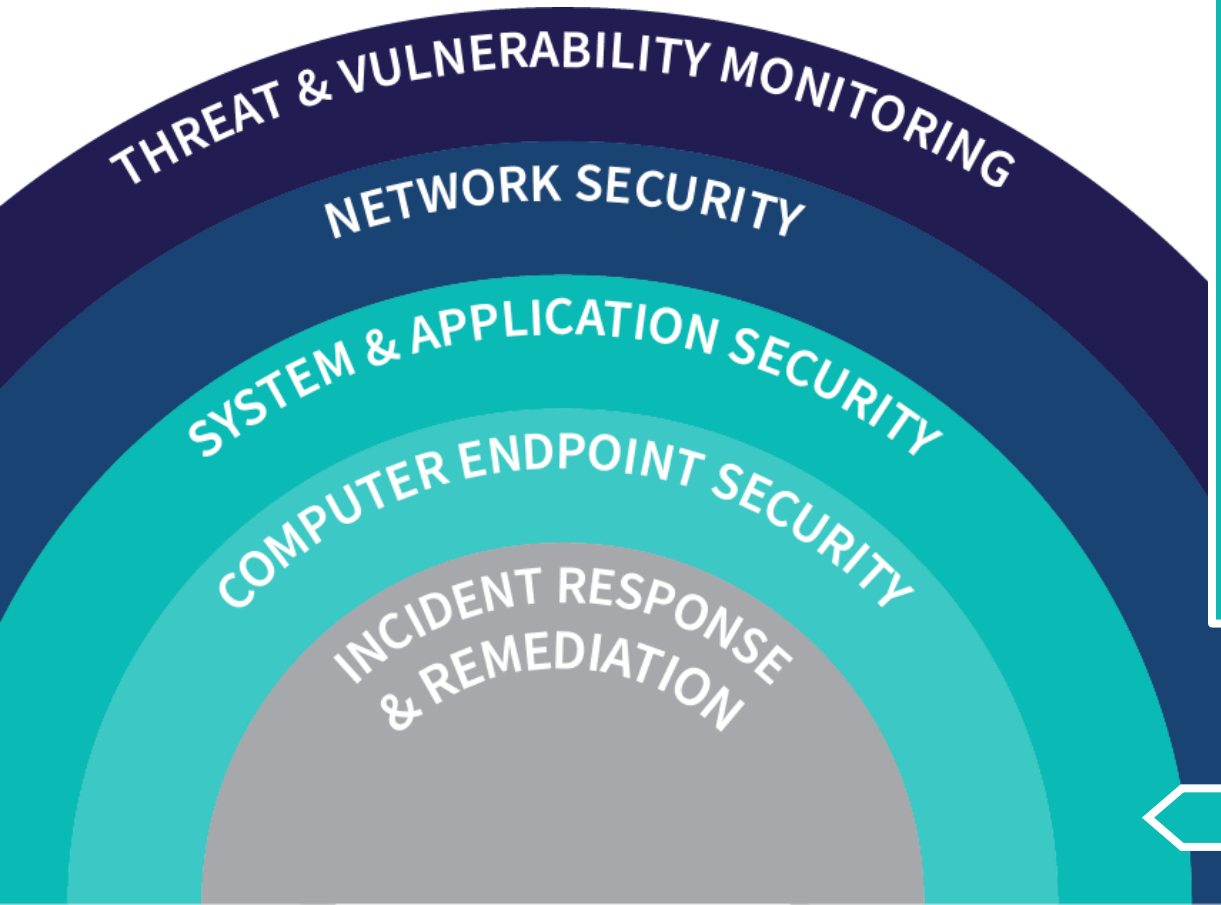
NETWORK SECURITY



- DNS filtering
- Advanced Malware Protection (AMP)
- Next Generation Firewalls (NGFW)
- Port Blocking
- Network Microsegmentation
- Enhanced System Access Management (ESAM)
- Multi-factor Authentication (MFA)

PRIVACY MATTERS @ UBC

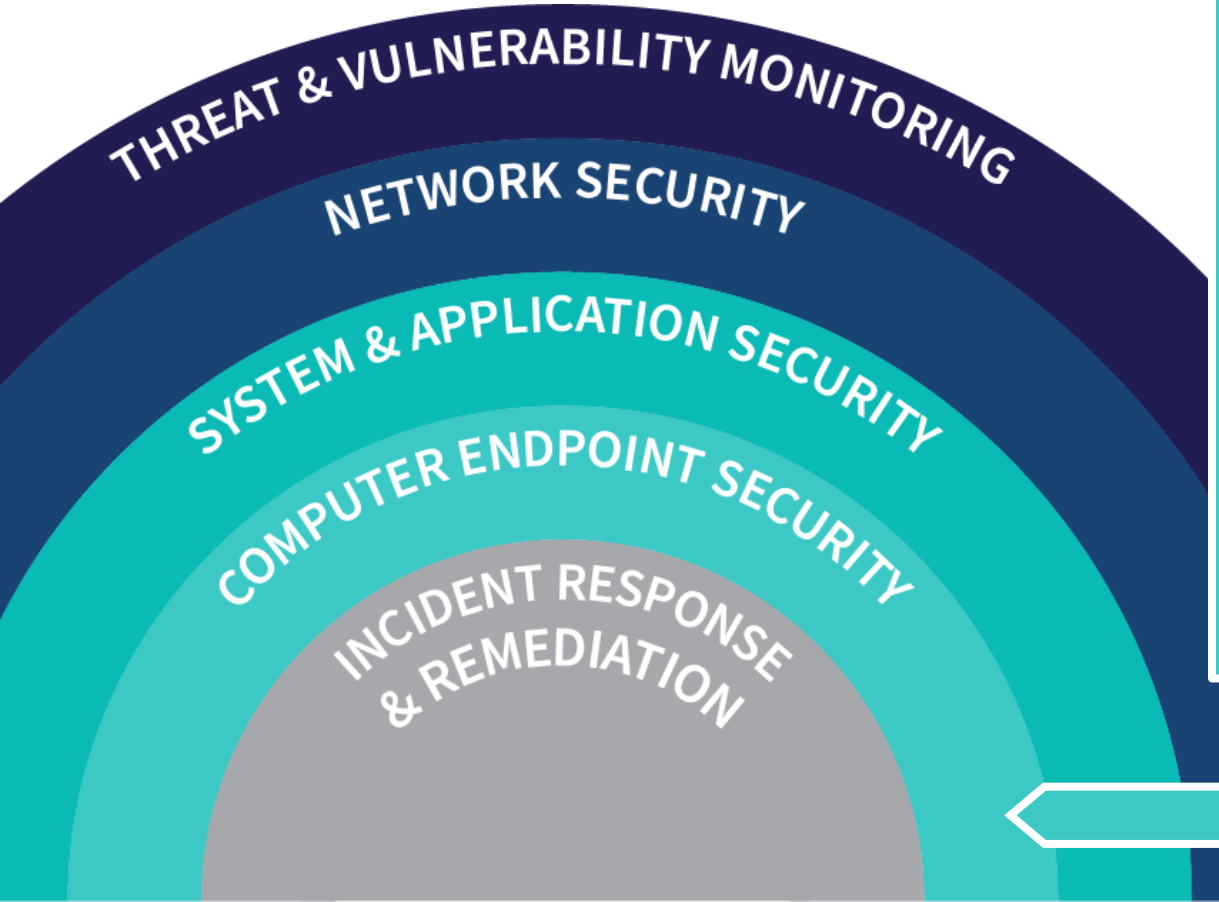
SYSTEM & APPLICATION SECURITY



- Endpoint Detection & Response (EDR) / Advanced Malware Protection
- Email fraud protection
- Centralized Log Management
- Security Information and Event Management (SIEM)
- Vulnerability scanning
- Web Application Protection Service
- Patch Management
- Multi-factor Authentication

PRIVACY MATTERS @ UBC

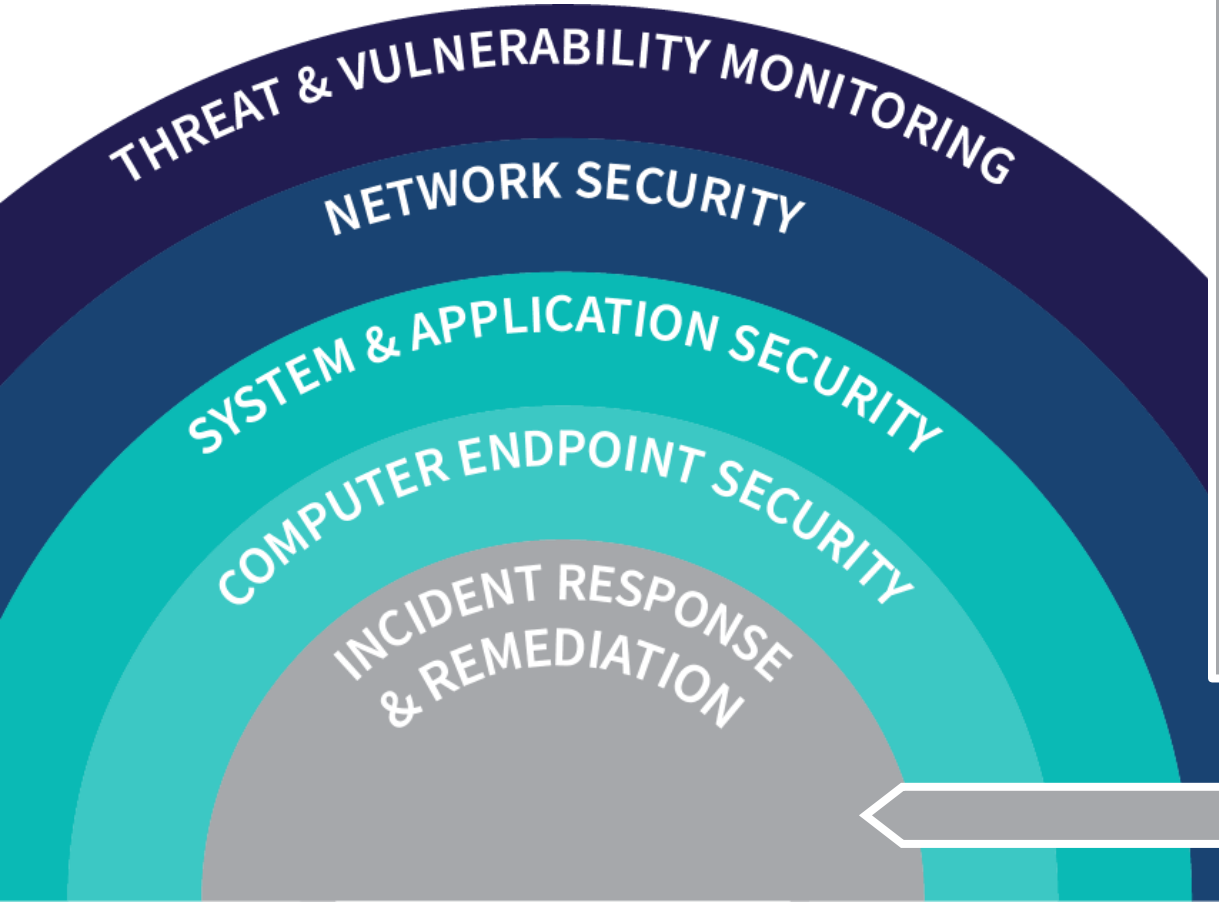
COMPUTER ENDPOINT SECURITY



- Endpoint Detection & Response (EDR) / Advanced Malware Protection
- Network Access Control (NAC)
- Privacy and information security training and awareness

PRIVACY MATTERS @ UBC

INCIDENT RESPONSE & REMEDIATION



- Extractions
- Blocking
- Back-ups
- Disaster Recovery
- Forensics
- Cyber Insurance
- Breach Coach

PRIVACY MATTERS
@ UBC

QUESTIONS?