RESEARCH ADVISORY COUNCIL

RESEARCH ADVISORY COUNCIL AGENDA

November 17, 2022 | 1:30 pm – 3:30 pm | Teams

Welcome and Introductions

1. **Items for Adoption**

1:35 **1.1 Agenda: November 17, 2022**

1:38 **1.2 Minutes: September 29, 2022**

2. **Discussion**

1:45 **2.1 Research Data Management Rollout Plan – Garry Fehr**

2:00 **2.2 Researcher Meet and Greet Event – Mai Anh Doan**

2:15 **2.3 University Press – Mia Anh Doan**

2:30 **2.4 Decolonization Toolkit and Workshop – Garry Fehr**

3. **Information Items**

2:45 **3.1 Research Office report – Ash Lalani**

2:55 **3.2 Human Research Ethics Board report**

- A reminder that beginning in January 2023, all active researchers on ethics applications need to have completed the updated TCPS2 CORE tutorial.
- The HREB will be coming out with some guidelines on research using social media in the coming months. Related to this, any questions that pertain to the use of materials from social media or internet media sites should be directed to **copyright@ufv.ca**.

3.3 Teaching and Learning Advisory Council report – no report

3.4 Senate Research Committee report – no report

4. **Roundtable Discussion (time permitting)**

5. **Adjournment: 3:30 pm**

5.1 Next meeting: January 26, 2023, 1:30 pm to 3:30 pm

Please see Research Newsletters at the bottom of the Research Office website for more information on events and funding opportunities.

RAC Minutes
September 29, 2022 | 2:00pm-3:30pm | Teams

RESEARCH ADVISORY COUNCIL

Present:	Tetsuomi Anzai, Barnabe Assogba, Shelley Canning, Irwin Cohen, Mai Anh Doan (vice-chair), Christine Elsey, Gary Fehr, Gillian Hatfield (chair), Allyson Jule, Masud Khawaja, Lucy Lee, Olav Lian, Mariano Mapili, and Chris Schinckus, Janelle Sztuhar, Cynthia Thomson, Kelly Tracey, and Natalie Vanderleest.
Guest(s):	Crawford Millen and Katie Tuck.
Recorder:	Tracy Morrison.
Regrets:	Peter Geller, Shawn Geniole, Claire Hay, and Amanda Wurz.

Welcome and Introductions –
Gillian Hatfield welcomed everyone to the RAC meeting, and everyone gave a quick introduction of themselves.

1. ITEMS FOR ADOPTION

1.1 Agenda: September 29, 2022

MOTION: THAT the agenda for the September 29, 2022 RAC meeting be approved as presented with changing 3.3 to 3.1.
Tetsuomi Anazi, Christine Elsey CARRIED

1.2 Minutes: May 6, 2022

MOTION: THAT the minutes from the March 11, 2022 RAC meeting be approved as presented.
Irwin Cohen, Barnabe Assogba CARRIED

2. BUSINESS

2.1 Vote for vice-chair: Mai Anh Doan - nominee

- Mai Anh was the only nominee for the role of vice-chair for the RAC for a two-year term.

MOTION: THAT Mai Anh Doan be vice-chair for the RAC 2022-2024 terms.
ALL IN FAVOUR CARRIED

3. DISCUSSION

3.1 Cyber Security – Crawford Millen

- Crawford Millen is the Director of Information Security at UFV.
- Crawford gave a presentation and overview of cyber security at UFV on who the team is and what they do to protect information at UFV.
- Attackers have recently found post-secondary institutions as easy prey as cyber security has not been a main priority until recently.
- Ransomware attacks have become more prevalent in recent years and now has a larger economy than the drug trade.
- Research data does have an economic value as ransomware attackers will demand money and threaten to release your data.
- UFV deals with attacks by monitoring each step of the attack chain. They watch for habits and have blockers in place for certain sites, so they are unable to offload our data.
- Email is responsible for 85% of cyber attacks as it is free, and people are more reliant on email for work. It's a perfect way to steal peoples' credentials when they click on a hacker link.
- UFV tries to confirm an email sender's identity before it is sent to your inbox.

- UFV added a multifactor authentication (MFA) as it is currently the best way to protect our work and data, even though some users find it annoying as an extra step, it is currently our best defense for protecting our work and credentials.
- Slides are attached.

3.2 Terms of Reference annual review and RAC historical timeline

- The timeline was included in the agenda package for reference to what RAC has done in the past.
- The Terms of Reference are being discussed as part of an annual review.
- Garry noted that under membership the faculty names and titles of members need to be updated.
- As Tetsuomi is a designate for the Dean, College of Arts, it was noted to change the line to "other faculty members or their designates are welcome to attend".
  MOTION: To accept the Terms of References with the minor amendments as mentioned above.
  All IN FAVOUR CARRIED

3.3 Researcher meet & greet event

- This event will be similar to a speed dating event for faculty to meet UFV researchers and hopefully spark some collaborations.
- The event will take place in the winter semester, but we would like to have a subcommittee to help with organizing, recruiting and promoting, with support from the Research Office.
- Mai Anh Doan and Cynthia Thomson volunteered.
- Reach out to Mai Anh or Cynthia if you're interested in assisting.

4. INFORMATION ITEMS

4.1 UFV Press update – Mai Anh Doan

- A tentative schedule has been created in order to launch the press early next year.
- There were six members, but a few are on leave now. If anyone is interested in joining, please contact Mai Anh Doan in Communications.

4.2 Research Centres, Labs, and Institutes Showcase – event report

- The event was extremely successful; new faculty expressed wanting to join some of the centres, students became interested in getting experience in research, and administrators became more aware of the breadth of research being done at UFV.
- We are wanting to host another event soon, similar to this one, but with more community members and externals.

4.3 Research Office Report – Garry Fehr

- Sumin Fang and Karun Karki both received SSHRC Insight Development grants valued at $75,000 over two years. Congratulations both!
- ROSA applications are due in Romeo by midnight on Oct. 31. You must have submitted all overdue final reports to be eligible.
- Sabbatical applications are due in Romeo by midnight on Nov. 15.
- Sabbatical reports for leaves during the 2021-22 academic year are due November 1, 2022; based on leaves for September 1, 2021 to August 31, 2022.
- SSHRC Insight grant deadline is Monday October 3, 2022.
- SSHRC Explore grants are due Monday October 3, 2022 – apply through Romeo.

- NSERC Discovery grant deadline is Tuesday November 1, 2022.
- Student Graduate Scholarships – Master's program is due Thursday December 1, 2022.
- The funds for the Faculty/Student Research and Scholarly Activity grant have been exhausted for the 2022-23 year.
- The funds for the Accelerate Grant have been exhausted for the 2022-23 year.

4.4 Human Research Ethics Board (HREB) Report – attached to the agenda package

4.5 Teaching and Learning Advisory Council Report – no report

4.6 Senate Research Committee Report – no report

5. Roundtable Discussion (time permitting)

6. Adjournment – 3:30 pm
MOTION to Adjourn - Cynthia Thompson

5.1 Next meeting: November 17, 2022, 1:30 pm to 3:30 pm on Teams

Please see Research Newsletters at the bottom of the Research Office website for more information on events and funding opportunities.

INFORMATION SECURITY

CYBER SECURITY – UNIVERSITY OF THE FRASER VALLEY

INTRODUCTION & IDENTITY PROTECTION

AGENDA

- Introduction to Team
- Overview of Cyber Security at UFV
- Email (spam, spam, and spam!)
- Identity (who are you?)
- Questions?

INFORMATION SECURITY

Team Introduction

Our Focus

- Professional attackers increasingly targeting Universities.
- Ransomware attacks are increasing in sophistication, cost, and speed.
- UFV increasingly is dependant on IT services for delivering educational services, with increasing expectations from students, faculty and staff.
- Research data attracts more sophisticated, persistent and determined adversaries.

Our Mission

- Secure the University's systems and data in alignment to the institutions risk appetite, and legislation, while respecting individual privacy.

Crawford Millen
Director

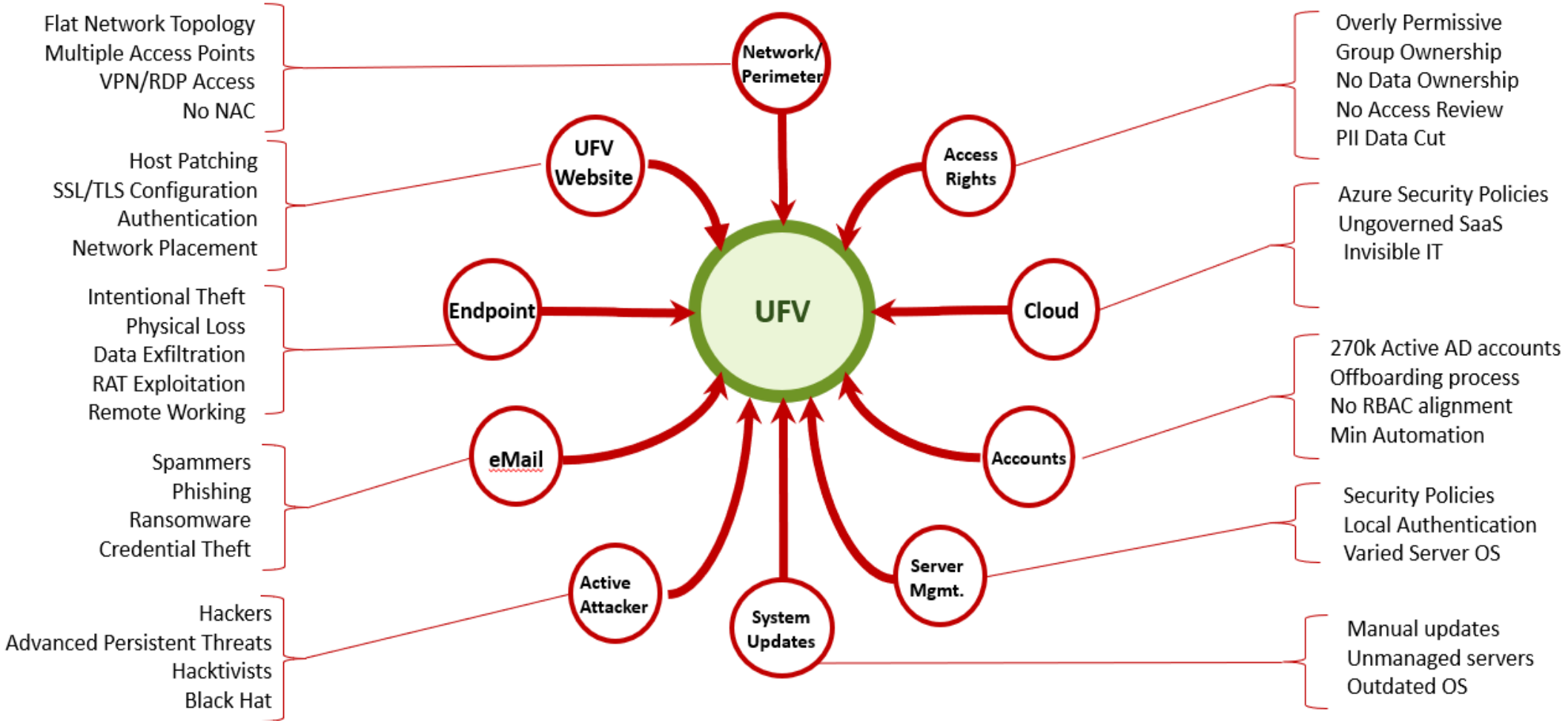
Jun Choe
Network Security Architect

Madison Kemball
Security Analyst

Cameron Fisher
Identity And Access

Jaskiran Mangat
Security Analyst

UFV THREAT LANDSCAPE



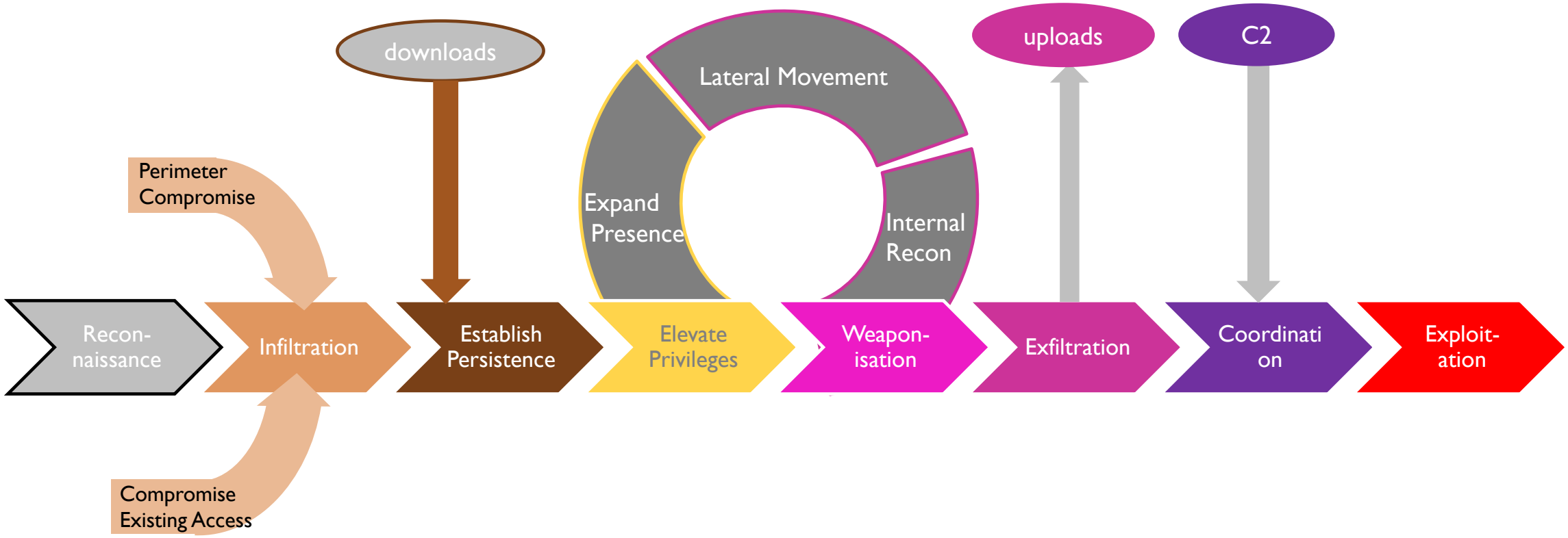
THREAT ACTORS

Sept 2022: Groups Targeting Canada and Academic Institutions

BERSERK BEAR	Russia	State	Dragonfly 2.0, Temp.Isotope, IRON LIBERTY, BROMINE, ALLANITE, DYMALLOY
BITWISE SPIDER	Unknown	Crime	LockBit, LockBitSupp, StealBit
CYBORG SPIDER	Unknown	Crime	Mespinoza, GOLD BURLAP, Pysa
DEEP PANDA (i)	China	State	WebMasters, Codoso, Group 72, PinkPanther, Black Vine, BRONZE FIRESTONE, APT19, …
DOPPEL SPIDER	E Europe	Crime	GOLD HERON
FANCY BEAR	Russia	State	Tsar Team, STRONTIUM, Sofacy Group, Zebrocy, TG-4127, UAC-0028, Fighting Ursa, F…
GHOST JACKAL	Unknown	Hacktivism	AnonGhost
GRACEFUL SPIDER	E Europe	Crime	FIN11
INDRIK SPIDER	E Europe	Crime	Dridex, BitPaymer, EvilCorp, GOLD DRAKE, GOLD WINTER, iEncrypt, WastedLocker,
LABYRINTH CHOLLIMA	North Korea	State	Zinc, HIDDEN COBRA, BeagleBoyz, Lazarus Group, APT-C-26, Black Artemis, TEMP.H
MALLARD SPIDER	E Europe	Crime	GOLD LAGOON, Qakbot, QBot, Quakbot, QakBot, PinkSlip
MUMMY SPIDER	E Europe	Crime	Geodo, GOLD CRESTWOOD, TA542, Emotet
PERCUSSION SPIDER	Turkey	Crime	drumrlu, 3lv4n, @elvan_tarak
PINCHY SPIDER	E Europe	Crime	REvil, Sodinokibi, GOLD GARDEN, GOLD SOUTHFIELD, GandCrab
SCHOLAR KITTEN	Iran	State	Silent Librarian, Cobalt Dickens, Yellow Nabu, TA407, Mabna Institute, spear phishing, spoof
SILENT CHOLLIMA	North Korea	State	Andariel, Lazarus, New Romanic Cyber Army
SPRITE SPIDER	Unknown	Crime	GOLD DUPONT, Defray 2018, Target777, Shifu, PyXie, Vatet, Defray, Defray777
STONE PANDA(i)	China	State	ChessMaster, APT10, menuPass, happyyongzi, POTASSIUM, Cloud Hopper, HOGFISH
VICE SPIDER	Unknown	Crime	Vice Society
VICEROY TIGER	India	State	Operation Hangover, Appin, APT-C-35, Donot, Orange Kala
VIXEN PANDA	China	State	APT15, Mirage, Ke3chang, NICKEL, APT15, Mirage, ke3chang, NICKEL
WIZARD SPIDER	E Europe	Crime	Anchor DNS, BazarLoader, GOLD ULRICK, Ryuk, TotBrick, Kegtap, UNC1878,Conti, Trickbot

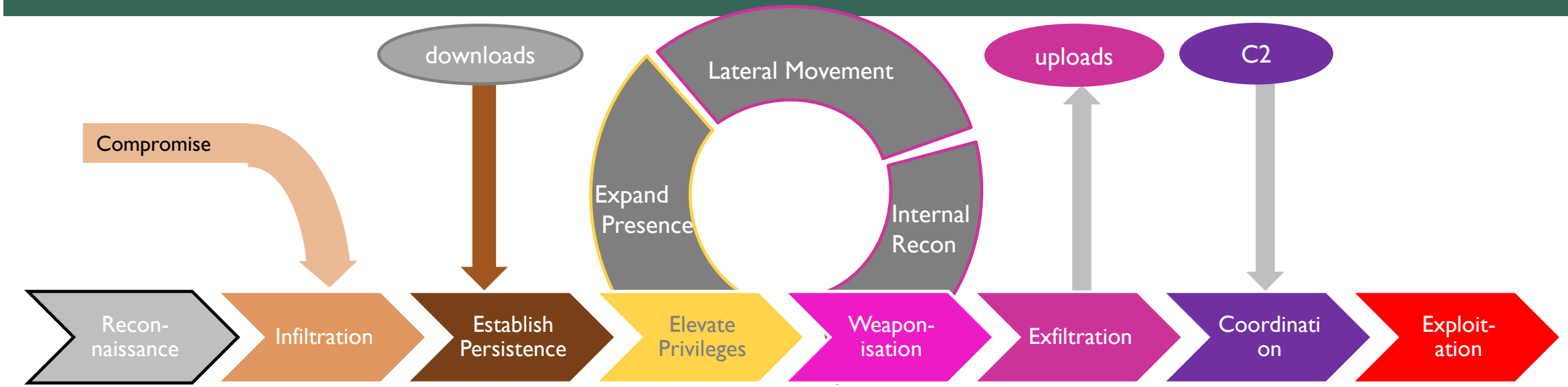
CYBER ATTACK LIFECYCLE

aka: intrusion "kill chain"



CYBER ATTACK LIFECYCLE

UFV's Defense in Depth



Cisco Firewall F5/ WAF Barracuda Exchange (EOP) Defender for Identity (D4I) SPF/DKIM/ DMARC	MFA CrowdStrike Sandboxing URL scanning Defender BAFS Win10 ASR InTune / GPO Varonis	CrowdStrike Email link rewriting D-Zone DNS Auto-Update Defender BAFS Nessus VA Scan	CrowdStrike Local Admin Defender ID Azure Sentinel Domain Admin Varonis Bloodhound	CrowdStrike Sentinel Defender VA Scanning Bloodhound Zeek	CrowdStrike Sentinel DLP Info Protection D-Zone DNS Cisco Firewall	Cisco Firewall CrowdStrike - Firewall control D-Zone DNS	CrowdStrike Bitlocker Incident Response CrowdStrike IR

EMAIL SECURITY:

REMOVING SPAM

Email is the initial vector used in >85% of attacks

Problem: email is ubiquitous and almost free to send.

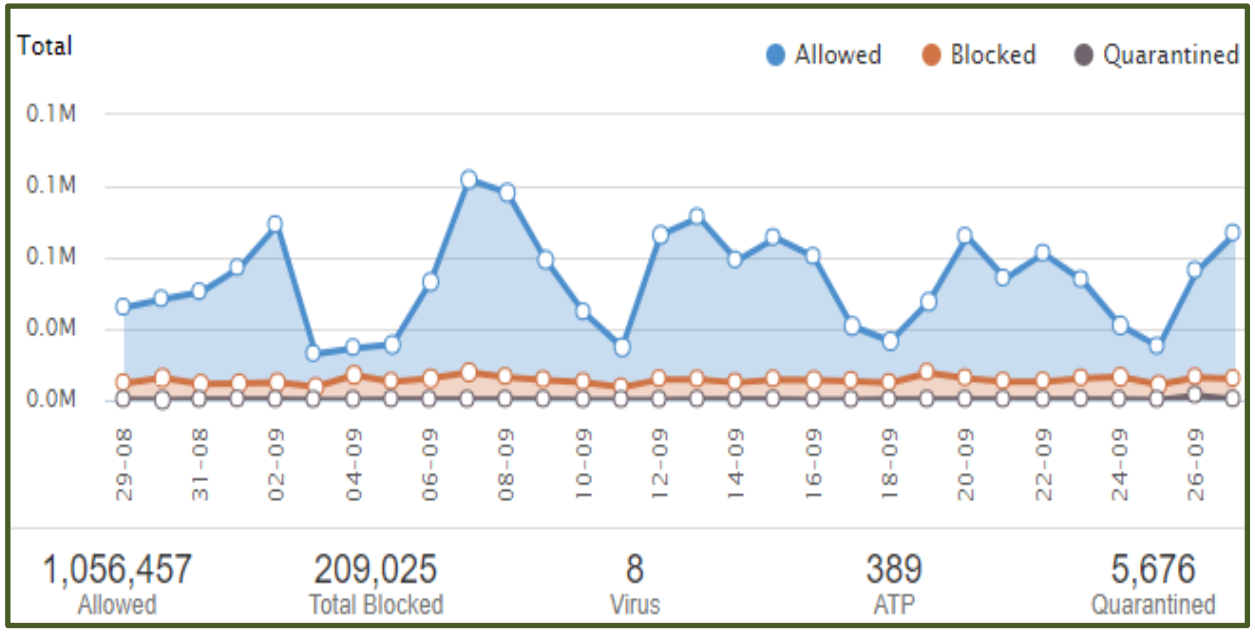
Everyone gets too many messages to be careful.

Step 1: Confirming the Sender's identity

- SPF
- DMARC
- DKIM

Step 2: Verify the Sender's Reputation

- Senders IP
- Domain Reputation
- Reputation Blacklists (RBL)



EMAIL SECURITY:

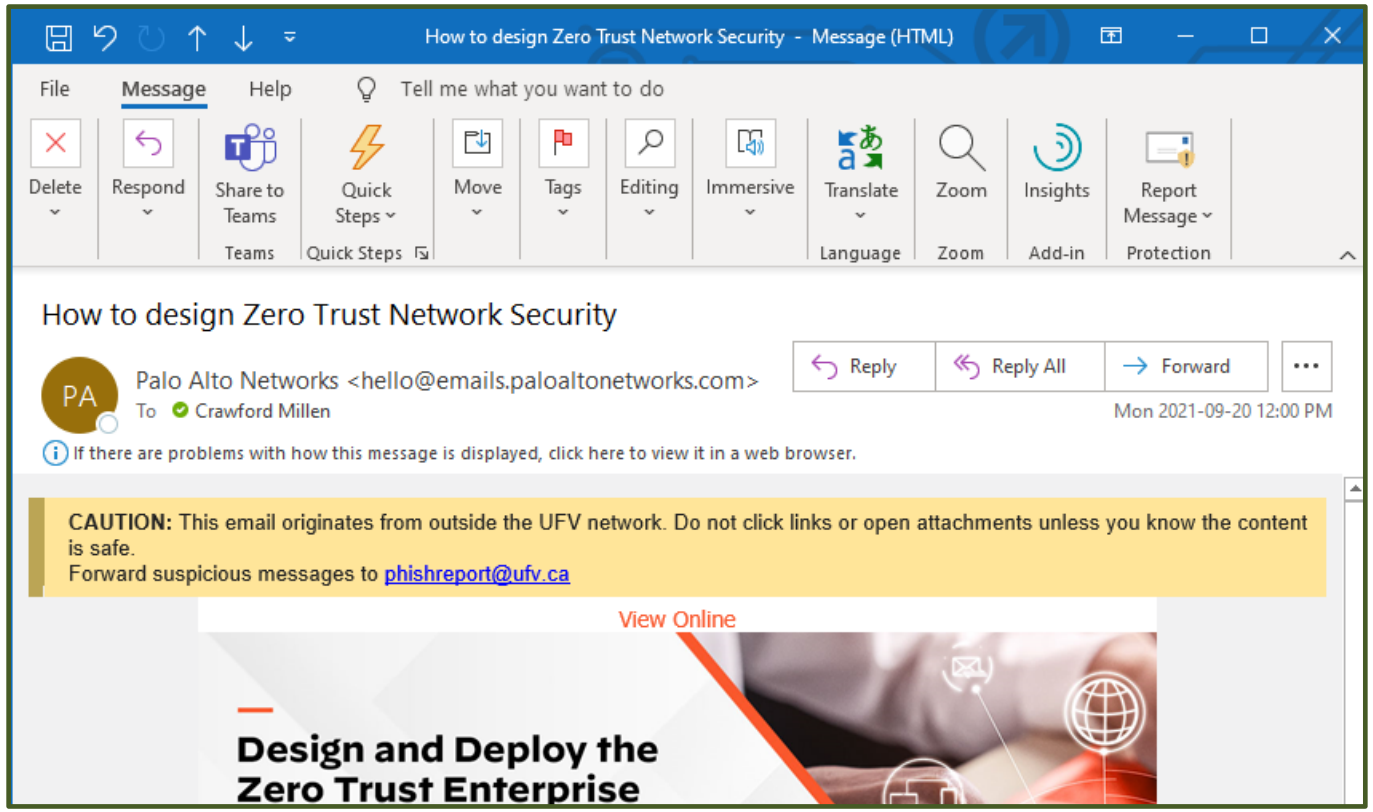
REMOVING MALICIOUS EMAIL

Step 3: Link Address Replacement
- Real time analysis of the URL
- Blocking of malicious sites.

Step 4: Content Scanning for
- Spoofing or impersonation
- Known spam messages

Step 5: Sandboxing
- Signature scanning of attachment
- Attachment (Documents) Detonation

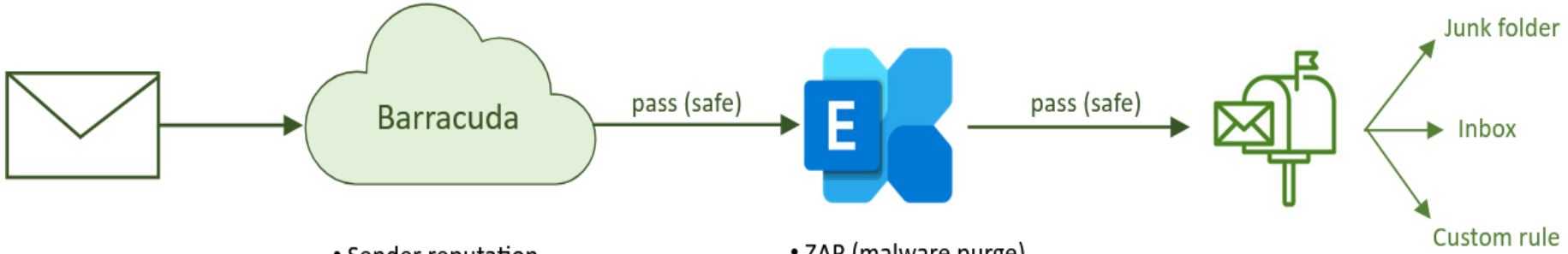
Step 6:
- External Email warning



IDENTITY PROTECTION:

EMAIL SECURITY

UFV utilizes a multi-layered defense against email threats
However it's a constantly evolving opponent



PROTECTING IDENTITY -WHO ARE YOU?

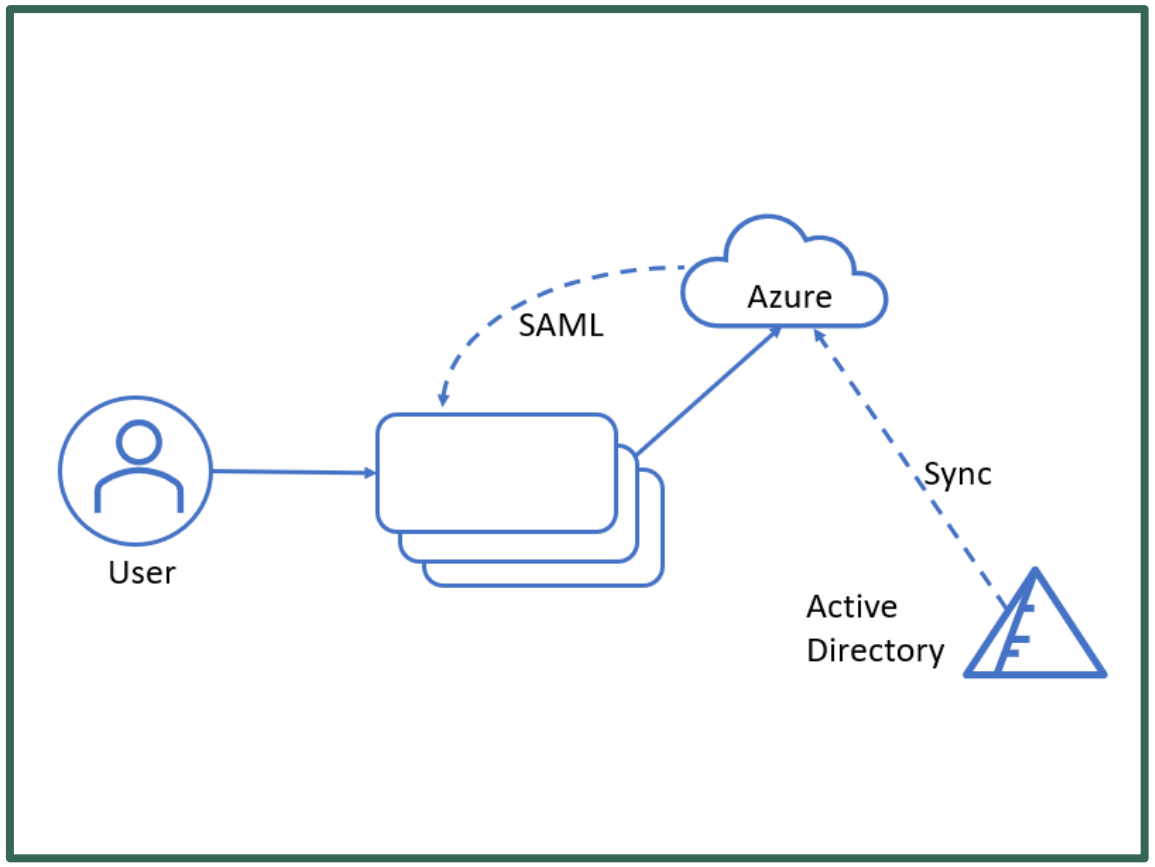
- Halt! Who Goes There?
- *It is I, Arthur, Son of Uther Pendragon, from the castle of Camelot. King of the Britons, defeater of the Saxons, sovereign of all England….*
- I blow my nose at you, so-called "Arthur King," you and all your silly English Knights."

PROTECTING IDENTITY:
-PASSWORDS ARE NOT PROTECTION

WHO ARE YOU?

- We have multiple way to identity people at UFV (AD, 300-id, email, etc)
- We are moving towards consistency (email)
- Passwords are being improved.
- Users equate Passwords as Security.
- Still many people use the same password on multiple systems…

PROTECTING IDENTITY: -SINGLE SIGN ON (SSO)



Single Sign On - single authentication allows access to multiple applications.

- User access application.
- Application forwards user to Azure for authentication.
- User authenticates (MFA optional).
- Azure forwards SAML token to application.
- Application reads token and accepts users identity.
- Other applications can used credentials in browser to offer seamless authentication.
- 40 Applications in Azure

MULTI FACTOR AUTHENTICATION: AN EXTRA LAYER OF SECURITY FOR YOUR ACCOUNT

- Most banking, healthcare, and social media sites have already adopted MFA to protect user accounts
- Recent report at higher education institutions in Canada shows MFA is becoming almost universally adopted

"Multi-factor" refers to using two or more items to verify your identity when you sign in, typically:

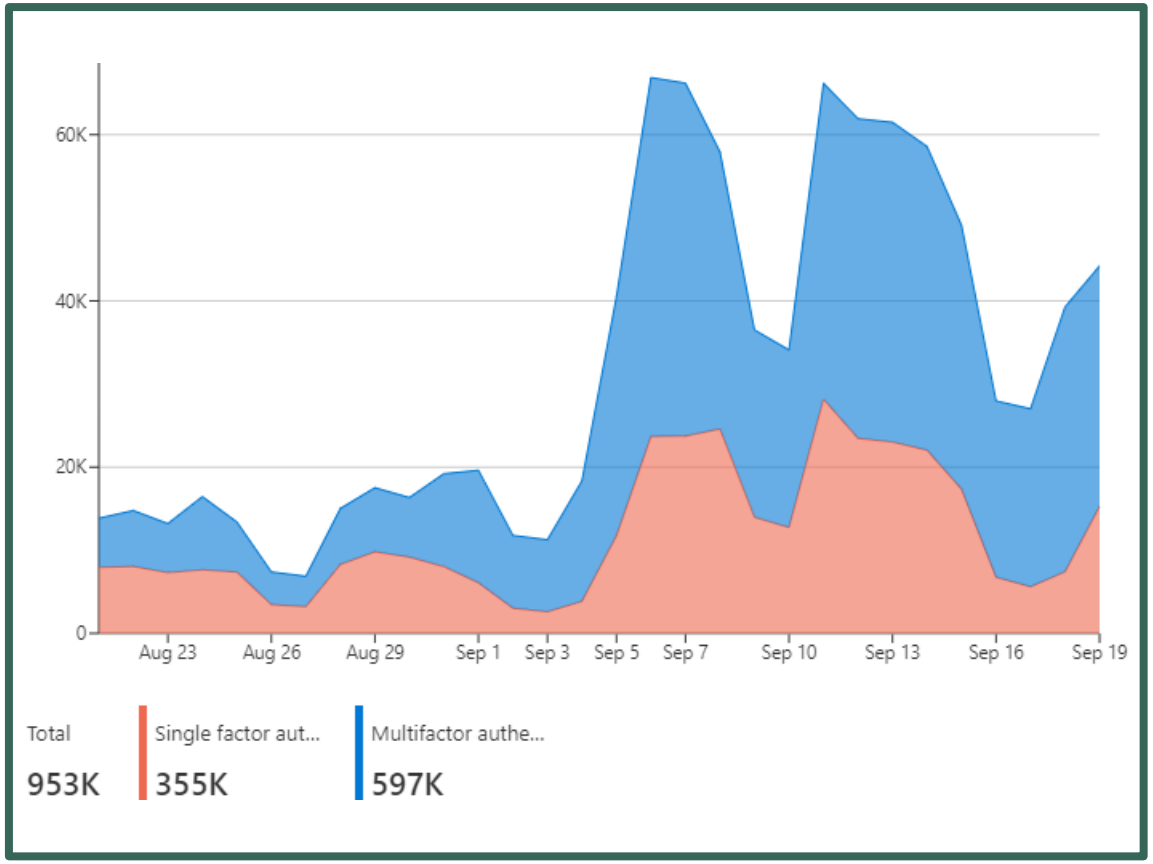
Something you know

(i.e., your UFV email and password.

Something you have

(i.e., your mobile device or email).

PROTECTING IDENTITY: MULTI FACTOR AUTHENTICATION



- Sept 2021 - 12k Students Registered
- Sept 2022 - 21k UFV registered accounts
- MFA required if:
  - User logs in from outside campus
  - User is flagged as high risk
- Currently Integrated into 37 Applications
- Monitored in real time by Sentinel

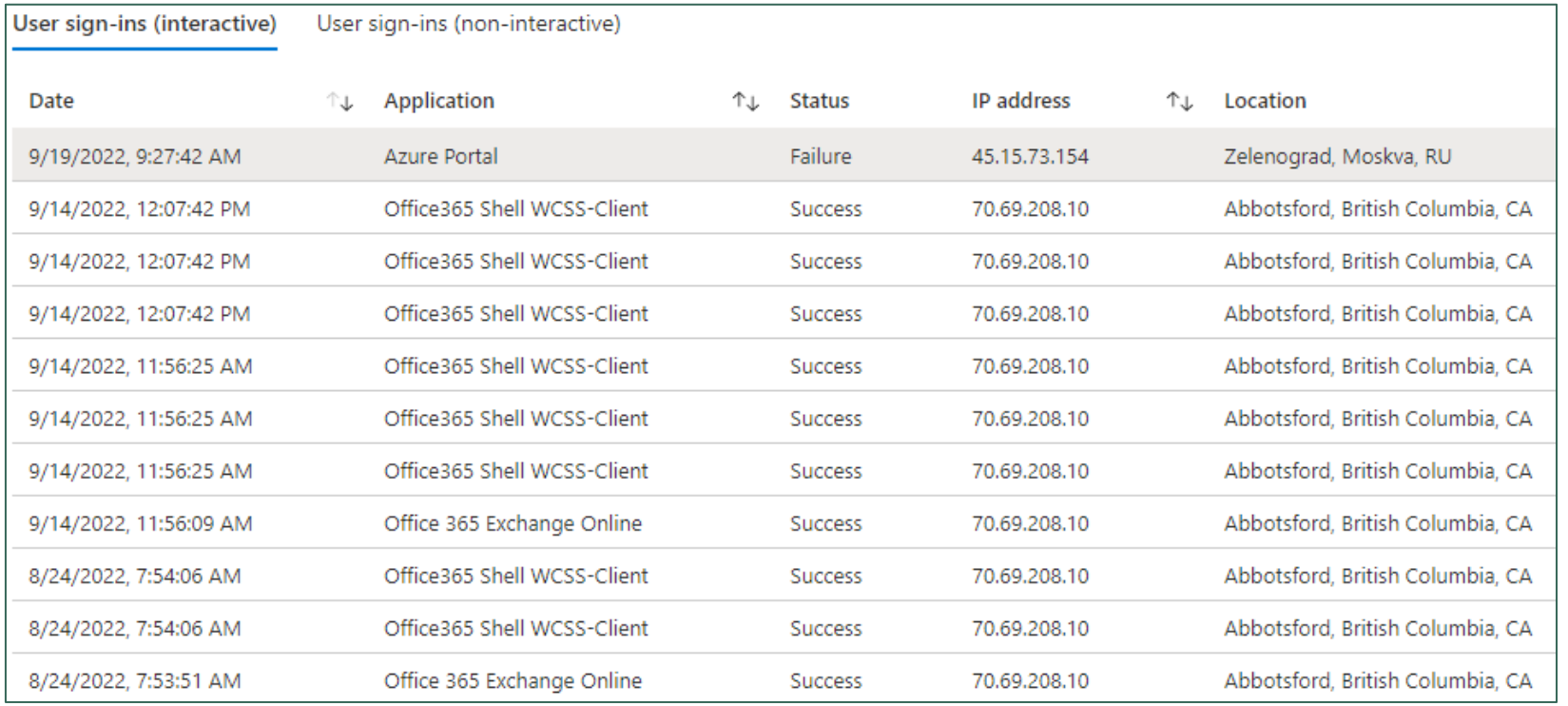
PROTECTING IDENTITY: USER RISK ANALYSIS

User Risk Analysis

- monitors dark web for compromised accounts
- compares typical vs atypical logins
- Impossib;e

For example:
This user is signing in from Abbotsford routinely.

The login from overseas is not typical and is flagged by the system and blocked.



User sign-ins (interactive) | User sign-ins (non-interactive)

Date	Application	Status	IP address	Location
9/19/2022, 9:27:42 AM	Azure Portal	Failure	45.15.73.154	Zelenograd, Moskva, RU
9/14/2022, 12:07:42 PM	Office365 Shell WCSS-Client	Success	70.69.208.10	Abbotsford, British Columbia, CA
9/14/2022, 12:07:42 PM	Office365 Shell WCSS-Client	Success	70.69.208.10	Abbotsford, British Columbia, CA
9/14/2022, 12:07:42 PM	Office365 Shell WCSS-Client	Success	70.69.208.10	Abbotsford, British Columbia, CA
9/14/2022, 11:56:25 AM	Office365 Shell WCSS-Client	Success	70.69.208.10	Abbotsford, British Columbia, CA
9/14/2022, 11:56:25 AM	Office365 Shell WCSS-Client	Success	70.69.208.10	Abbotsford, British Columbia, CA
9/14/2022, 11:56:25 AM	Office365 Shell WCSS-Client	Success	70.69.208.10	Abbotsford, British Columbia, CA
9/14/2022, 11:56:09 AM	Office 365 Exchange Online	Success	70.69.208.10	Abbotsford, British Columbia, CA
8/24/2022, 7:54:06 AM	Office365 Shell WCSS-Client	Success	70.69.208.10	Abbotsford, British Columbia, CA
8/24/2022, 7:54:06 AM	Office365 Shell WCSS-Client	Success	70.69.208.10	Abbotsford, British Columbia, CA
8/24/2022, 7:53:51 AM	Office 365 Exchange Online	Success	70.69.208.10	Abbotsford, British Columbia, CA

QUESTIONS