

RSA[®]Conference2022

San Francisco & Digital | June 6 – 9

SESSION ID: **PART3-W02**

Practical Learnings for Threat Hunting and Improving Your Security Posture

Jessica Payne

Security Person
Microsoft
@jepayneMSFT

Simon Dyson

Cyber Security Operations Centre - Lead
NHS Digital

TRANSFORM



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

©2022 RSA Conference LLC or its affiliates. The RSA Conference logo and other trademarks are proprietary. All rights reserved.

Advanced

Persistent

Threat



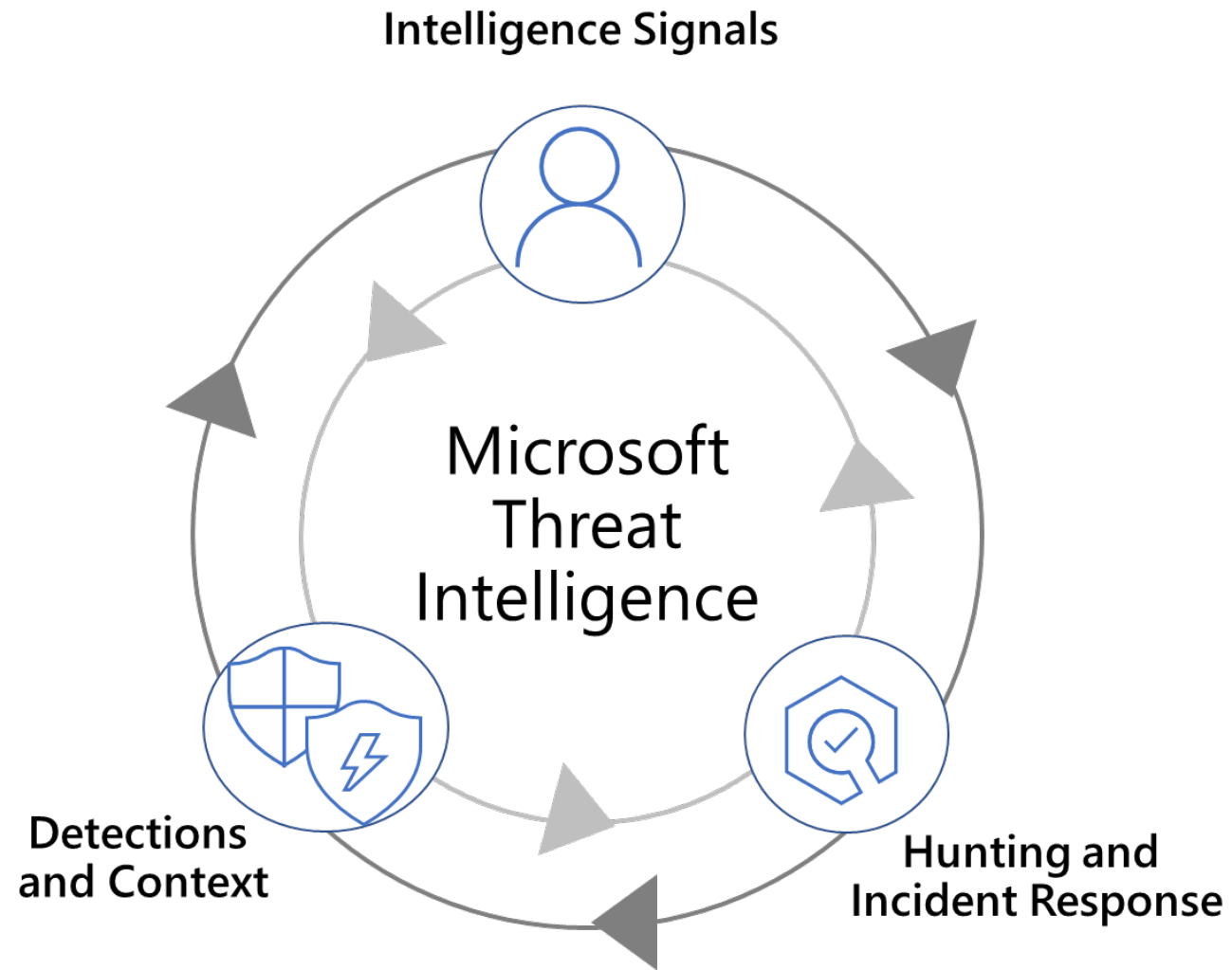
Sophisticated Attackers

DEV-0193 UNC1878 ADJECTIVE + ANIMAL

**Moderately
skilled people
who know slightly
more about your network
than you do.**



**Threat Intelligence should be as much about
telling you what you don't have to worry about**



Demystifying Ransomware attacks

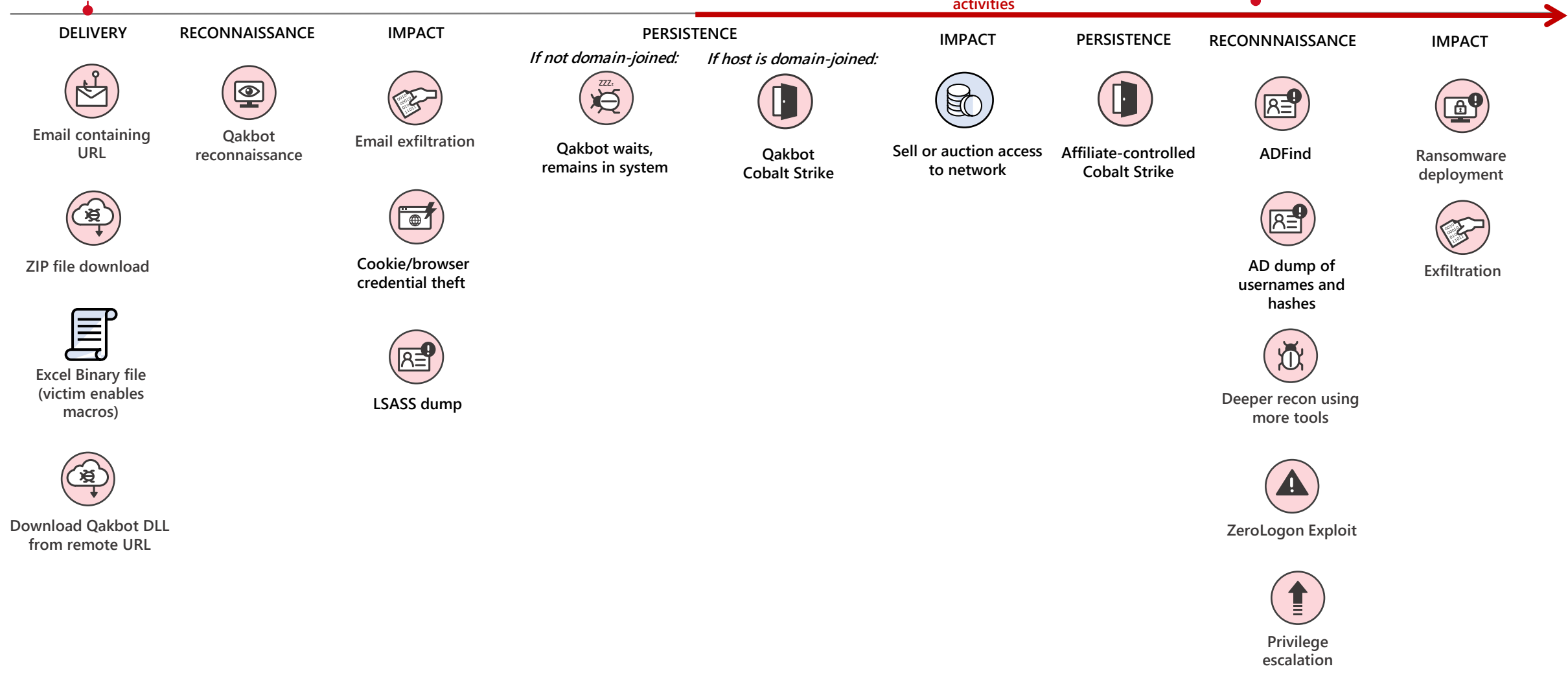


DEV-0226 User's device

Start of DEV-0504 RaaS affiliate's hands on keyboard activities

Multiple devices

#RSAC

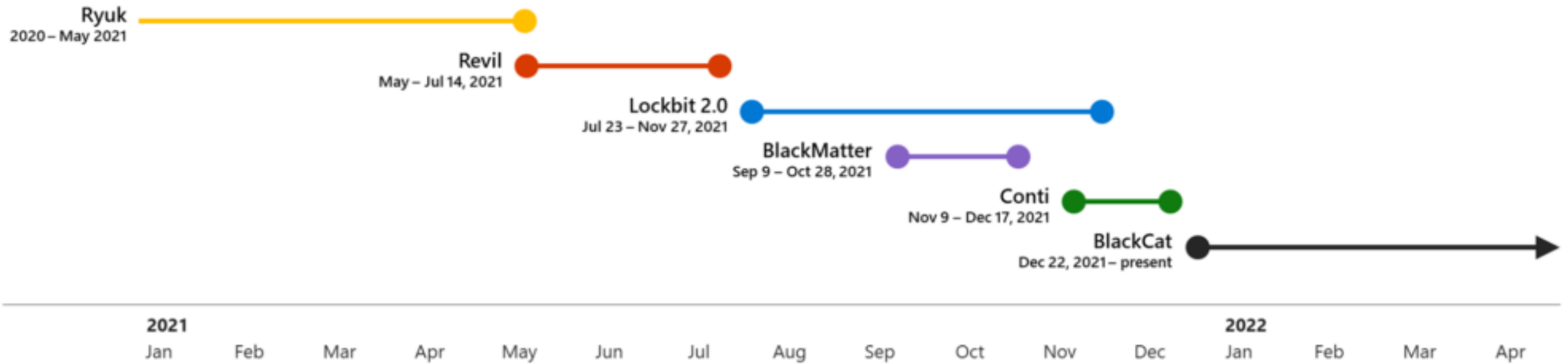




DEV-0226 and DEV-0504

- DEV-0226 Qakbot distributor and access broker
 - Qakbot developers are DEV-0303
 - Often sells access to DEV-0504, a prolific RaaS affiliate
 - DEV-0504 has used many payloads including REvil, Egregor, and LockBit
 - DEV-0226 now with a new backdoor, which has been dubbed SquirrelWaffle by the internet
- TTPS:
Macros – usually excel, often 4.0
 - Built with the help of EtterSilent
Multiple Cobalt Strike beacons
 - Qakbot exfiltrates a TON before it's caught by AV

DEV-0504 ransomware payloads over time



DEV-0252 / Bazaloader

- DEV-0252 most known for the “Baza” malware
 - Provides access to many RaaS groups
 - Will perform their own ransomware work from time to time
 - Most strongly associated with Conti/Ryuk
 - Has now moved on to Bumblebee/COLDTRAIN
- TTPS:
Macros – often excel
 - Attached script files in containers such as isos
 - “Stolen Images” campaign
Distinctive Cobalt Strike imports
 - Direct exe payloads in various hosting providers
 - Replacing Cobalt Strike with the Sliver implant from BishopFox



DEV-0206 / DEV-0243 cluster

- FakeUpdates and “SocGholish” operated by DEV-0206
 - Provides access to DEV-0243 who have distributed many payloads, not just WastedLocker
 - Moves fast to hands on keyboard when a “quality” network checks in
 - Some Zloader runs delivered this way too – different operator
- TTPS:
Malvertising/popups impersonating software installed
 - Zip->script file
 - Technique works because of default file handlers for scripts

ELBRUS

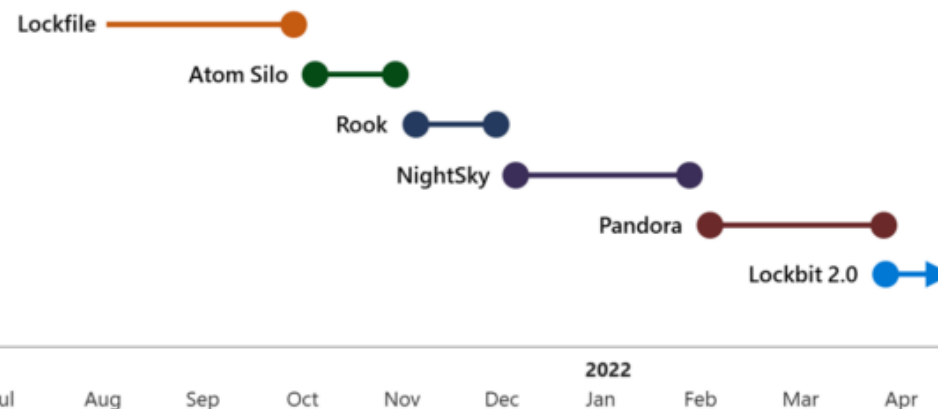
- Aka FIN7
 - Recruits “pentesters” as Bastion Secure
 - Behind DarkSide and Blackmatter
 - Able to run multiple concurrent campaigns
 - Espionage/Finance operations as well as ransoms
 - RaaS as well as “owner operated”
- Use of Sharepoint/OneDrive
 - Macros and script files for entrance
 - Custom tools and off the shelf

DEV-0401

- Constantly rebranding this payloads in an attempt to look like a RaaS
- Switched to an actual RaaS and deploying LockBit in April of 2022
- Probably have links to a state sponsored group

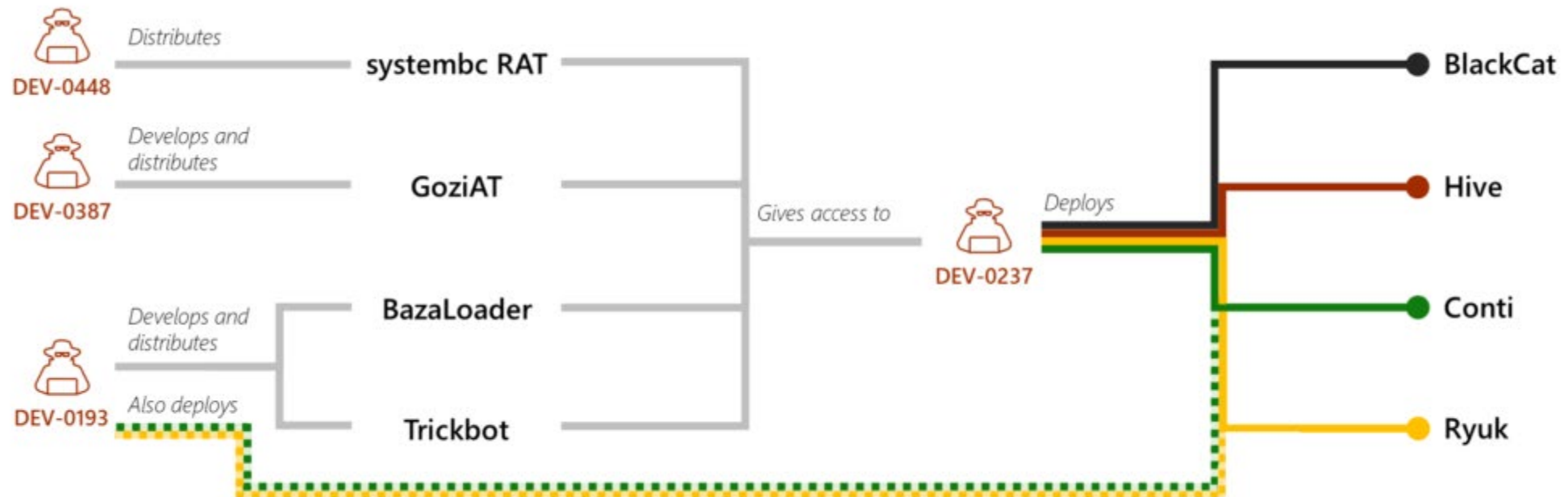
- Love a good internet vuln
- Adopted log4j within a couple days of disclosure
- Used recent Confluence vuln *before* disclosure
- Still need creds to move laterally and rely on implants/industrialized tools like Cobalt Strike
- Have also adopted Sliver

DEV-0401 ransomware payloads over time



Commonalities

- Office abuse
- Account abuse
- Script abuse
- Security product tampering
- Industrialized attack tools



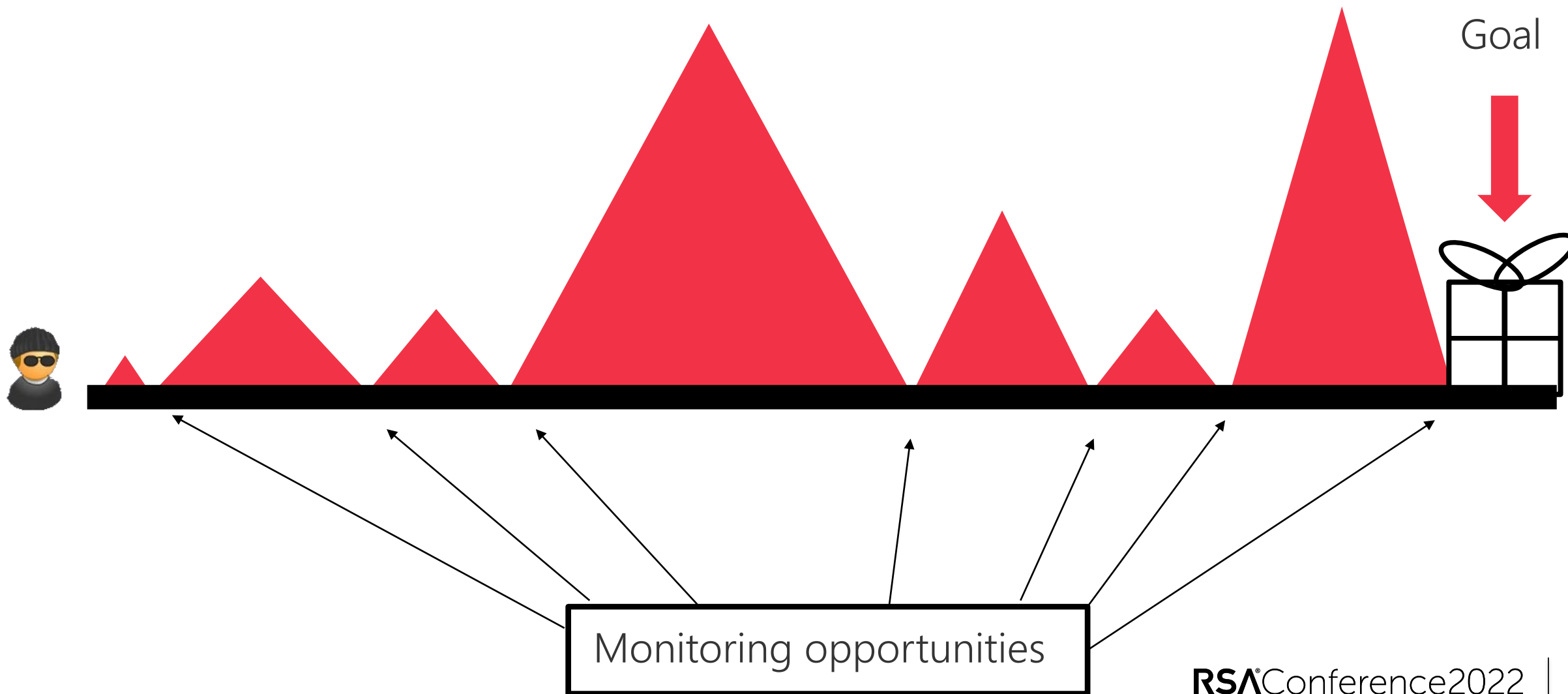
Ransomware is a preventable disaster

Network Design



A “flat” network does little to hinder the attacker discovering and reaching goal

Network Design



So why doesn't
everyone do this?



You can't just buy this,
you have to build it.

Legacy Settings

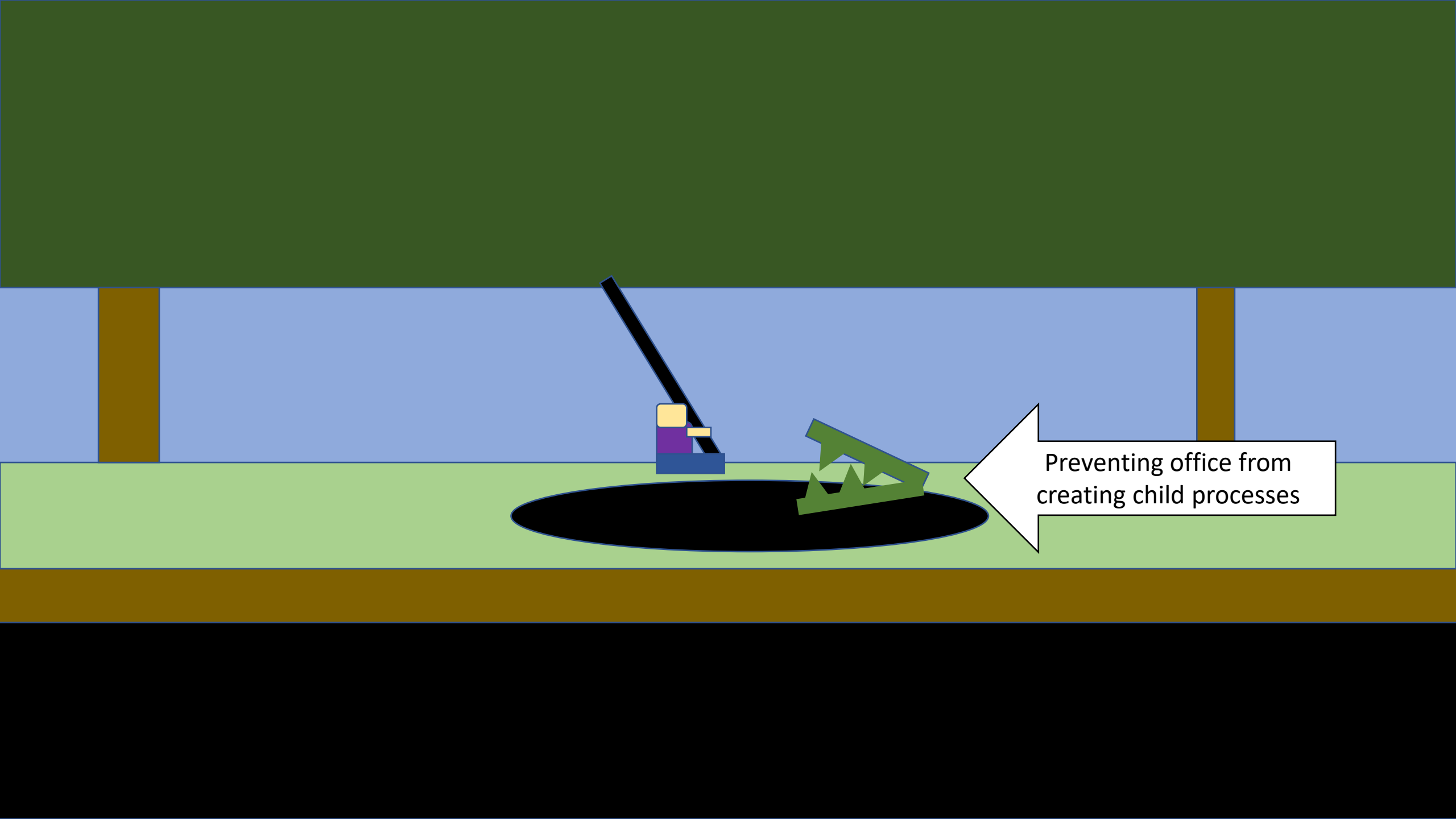
Technical Debt

We have always done it this
way

Fear

What if I told you being secure could save you money?





Preventing office from
creating child processes

Answering difficult questions

What you need is a spreadsheet

Problem	Controls	Security Gain	Technical Difficulty	Political Difficulty
Macros/Office abuse	Prevent Office from Creating Child Processes	high		
Perimeter vulns/abandoned systems	Scanning and isolation	medium		
Lateral movement	Credential hygiene	high		
Script abuse	Change default script handler/enable ASR Rules	high		
Industrialized attack tools	Enable cloud mode AV/tamper protection/ASR rules	high		

The 8000-word version of this research is available at
<https://aka.ms/ransomware-as-a-service>



Simon Dyson (MSc) (CISSP / CCSP)

Cyber Security Operations Centre Lead at NHS Digital

- An Editor / reviewer of Healthcare & Cybersecurity with **JBBA The Journal British Blockchain Association**
- Published papers on blockchain & cryptocurrencies, contributing author to **Blockchain impact!**.
- Certified Cloud Security Professional (**CCSP**)
- Certified Information Systems Security Professional (**CISSP**)
- Received an **MSc** in Advanced Security & Digital Forensics
 - from Edinburgh Napier University
- **Law enforcement** – Police officer / Detective
- Regional Cyber Crime Unit (UK) –Regional Organised Crime Unit UK as Cybercrime investigator / forensic practitioner



Digital

The big number slide

NHS Digital's Data Security Centre is the lead partner on data security across the NHS.

1.9 million endpoints on Endpoint monitoring

23.2 billion on our boundary solution over a 5 day period

21 million blocks for malicious items

NHS COVID PANDEMIC



Hospital&Trusts

Continue to support health organisations to operate with minimal disruption from cyber events and support incidents.



Nightingale's

Large temporary units to treat large numbers of COVID patients in temporary hospitals.
Support monitoring and incident support.
7 across the country.



Test & Trace

Support and provide services for the partner agencies involved in the test, trace and contain space.



Vaccination

Provide monitoring and incident support to the vaccination roll-out effort.



STAY HOME ► PROTECT THE NHS ► SAVE LIVES



Digital




Global threat & Incidents of note

- Feb 2020 Redcar & Cleveland
- Sep 2020 – Dusseldorf University Hospital
- Dec 2020 – Solarwinds
- 2020 Significant attacks across US & French healthcare
- 2021 Hackney Council
- 2021 Colonial Pipeline Ransomware
- 2021 Irelands (HSE) Health Security Executive



Digital



Failure is the
key to
success; each
mistake
teaches us
something

THE ART OF PEACE –
Morihei Ueshiba

A phrase that makes me sad

- “It’s just “Commodity malware””

What should we be interested in;

- Threat actors
- Campaigns
- Tangled web of affiliates & groups
- What have we seen before
- Static (still can be helpful)
- Behaviours, TTPS



Threat hunting Interactions

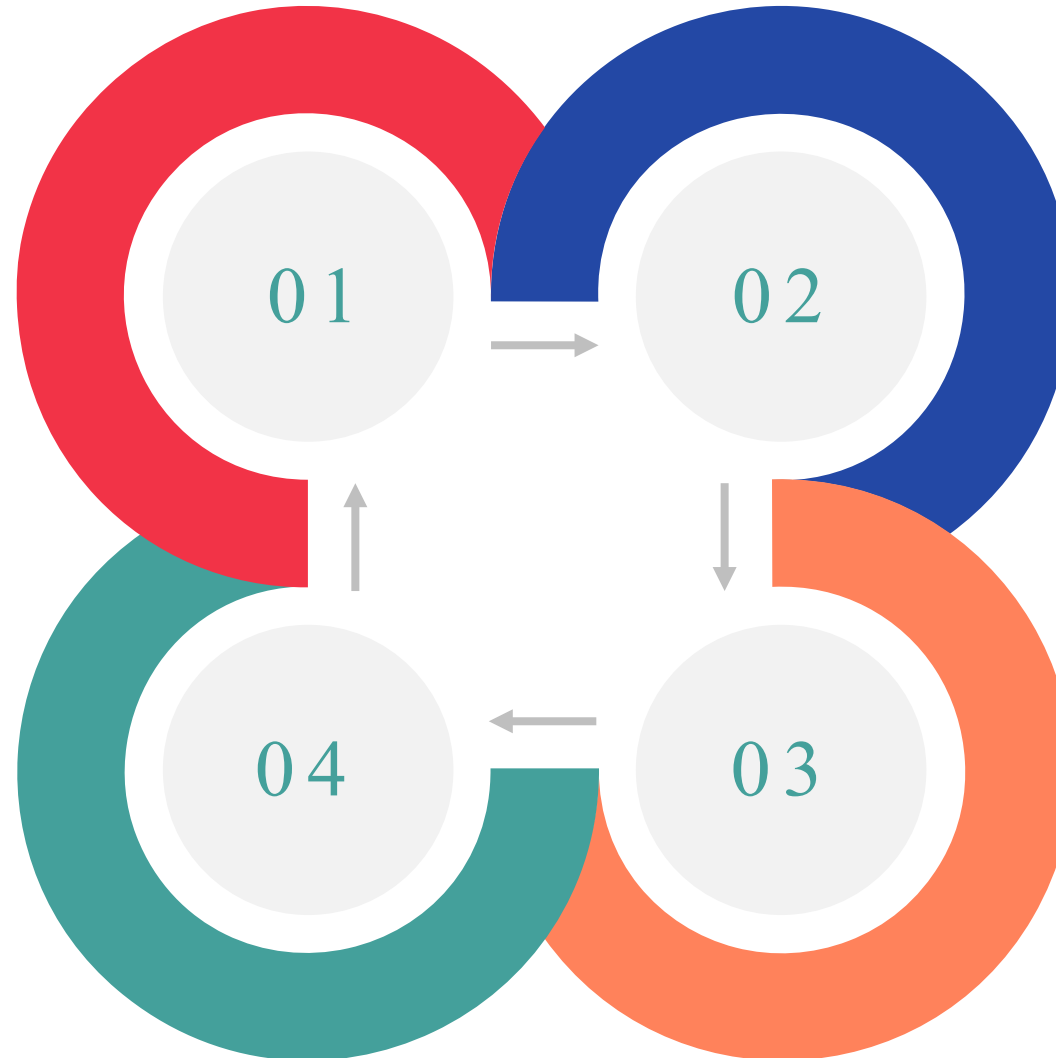
Common flow of threat intelligence

Threat Intelligence

Gathering TI from open and commercial sources to discover activity IOCs.

Cyber Incident Response

Deployed to put resource to assist in contain phases and gather evidence on-site. Provides further forensic support.



Threat Hunting

Dedicated resource to develop hypotheses around TTPs. Creates hunts based on potential sources and visibility from tooling

Incident Management

Work to contain, investigate and supporting the organisation to mitigate and recover.

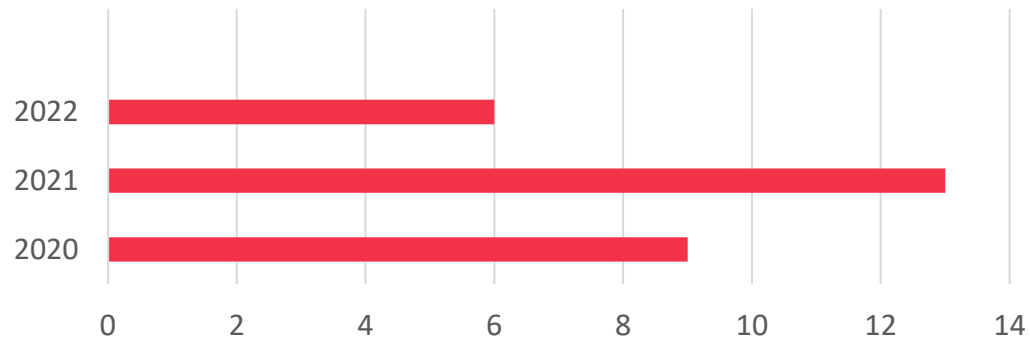
Rule creation and governance

- Create content & test
- Automated workflows
- Promote rules into protective monitoring
- Review rules efficiency performance & effectiveness

High Severity Alerts

- Triage intelligence
- Impact and Probability
- Communicate to all organisations

Number of High Severity Alerts



Beneficial activities

- Do everything to reduce the dwell time
- Attack Surface Reduction Rules
- Utilise Mitre Att&ck to describe TTPS
- Maps TTPs to alerts and controls
- Use Cyber kill chain for SLT / Board level
- Perform adversary emulation & lab work

The team is your greatest asset

- Keep diverse – not just protected characteristics
- Different backgrounds, technical, sector and skills
- Pure cyber – beware group think or CTF mentality
- Recognise human ingenuity criminal and defender
- Automation will save time and effort but the human element is so important.