Advantage®

Agenda

18:00 – 18:05 – Welcome – Steve Smith

18:05 – 18:25 – Red team – Brett More

18:25 – 18:35 – Break for food and drinks

18:35 – 18:55 – Blue team – Brad Pearpoint

18:55 – 19:15 – Data protection – Richard Wells

19:15 – 19:30 – Q&A

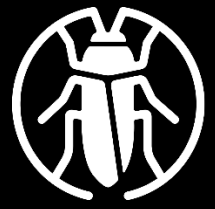
19:30 – Close – Networking

Advantage®

Questions

https://sli.do
Event ID: 6610

GAIN THE BUSINESS ADVANTAGE



INSOMNIA
SECURITY SPECIALISTS :: REST SECURED

Red Teams

What. Why. When.

Brett Moore
Insomnia Security

If your network was compromised

Would you know?

What is a Red Team?

Differs from standard Penetration Testing

- Red Team works towards meeting goals or objectives

Holistic view of an organisation

- Not confined to any application, project or location

Makes use of a wide range of attacks

- Internet, Wireless, Physical, Phishing

Red Team Exercise Types

Time Limited Red Team

- Runs over a consecutive period for a finite amount of days

Persistent Red Team

- Allowed to run over an extended period of time, but not always active

Assumed Breach

- Removes the variable of first point of compromise

Why Red Team?

Simulates an attack using the techniques and methodologies of real-world attackers

Provides a realistic assessment of your organisation's ability to protect against and respond to modern adversaries

Allows your security team to practice detection and response within your own environment

Why Red Team?

Improve security in both technical and process

- Broad recommendations to be implemented across an organisation

Continuous improvement of security

- Repeated Red Teams should become more difficult

Not focussed on the initial breach

- There will always be a vulnerability, or a staff member tricked

When Red Team?

What is your current security maturity?

- Should have an established security program

What is your current detection and response capability?

- Must have some existing detection capability

Do you know what business assets and services would cause a "nightmare scenario" if compromised?

- Be able to set objectives and goals

When Red Team?

Are you comfortable with testing in production environments?

- A Red Team is real-time attacks in a production network

Are you open to setting minimal scoping restrictions?

- "anything goes"

Aligns with key objectives of your security strategy?

- What will the outcome of the Red Team be used for

Why Not Red Team?

Red Team exercises answer a specific question

- If your network was compromised, would you know?

Afraid of outages or damage to production networks

- Your attackers aren't

If you want to control the Red Team

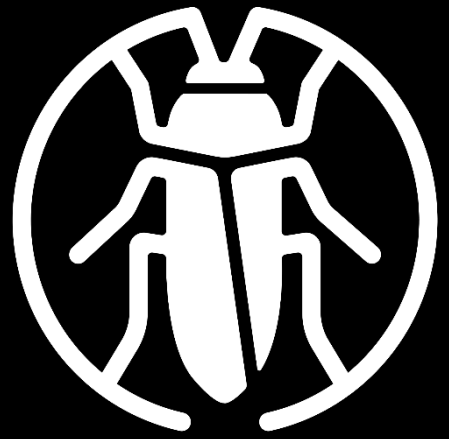
- There are different training mechanisms for this

Summary

Differs from standard Penetration Testing

Provides a realistic assessment of your organisation's ability to protect against and respond to modern adversaries

Allows your security team to practice detection and response within your own environment



INSOMNIA

SECURITY SPECIALISTS :: REST SECURED

www.insomniasec.com

Advantage®

Questions

https://sli.do
Event ID: 6610

GAIN THE BUSINESS ADVANTAGE

Advantage®

TAILORED TECHNOLOGY SOLUTIONS

Reality of Today's Hackers

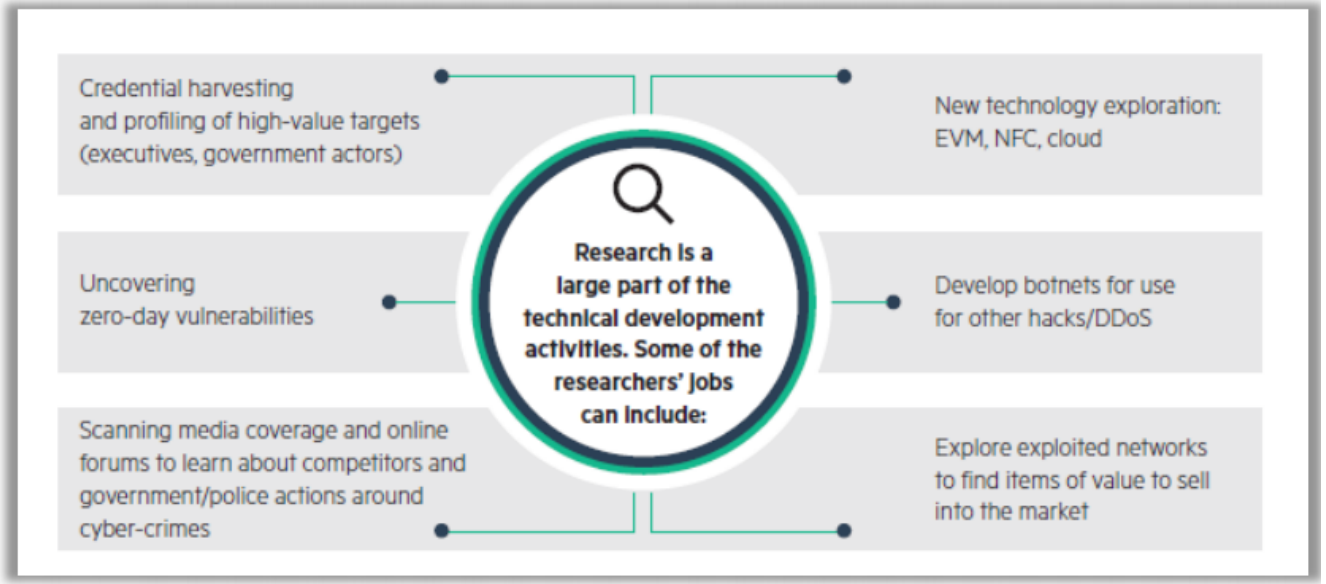
May look more like this . . .

. . . than like this

Advantage®
TAILORED TECHNOLOGY SOLUTIONS

Today's Adversary: Not always the Lone Wolf

- Structured organization with roles, focus
- Premeditated plan for targeting, exfiltration, monetization of data/assets
- Multi-layered trading networks for distribution, obfuscation



Source: HPE: the business of hacking

Why? Because increasingly, CRIME PAYS!

Advantage®
TAILORED TECHNOLOGY SOLUTIONS

Cyber criminal - What is their motivation

- State sponsored cyber attacks
- Russia cyber attacks US during the elections
  - Multi-vector attacks, fake news, propaganda attacks, financial leverage
  - 60,000 emails from Hillary Clintons was accessed and leaked to WikiLeaks
  - DNC server breech and info leak
- Australian Political party hack
  - Feb 2019 discovered
  - ASD leak recently told reporters that China was responsible
- APT28 (Fancy Bear) targeting EU and UK parties throughout 2019

Advantage®
TAILORED TECHNOLOGY SOLUTIONS

Cyber criminal - What is their motivation

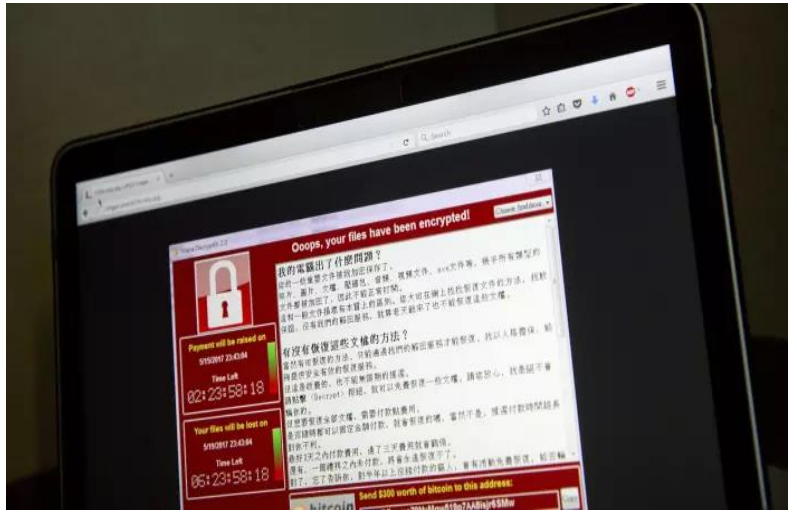
- Hactvism (anonymous – hacking group)
- 32 million accounts were hacked
- Details included credit cards, names, addresses, email addresses and dates
- 50K+ were .nz email addresses
- 15K were .mil and .gov email addresses
- Including 2 * Homeland security and 12 * DOJ employees
- Hackers motivated by morality issues

Your country or your marriage and half your fortune!

Advantage®
TAILORED TECHNOLOGY SOLUTIONS

Cyber criminal - What is their motivation

- **Wannacry – Ransomware!**
  - **Origins from North Korean hacking group called Lazarus (Sony Pictures)**
  - **300,000 computers infected in the UK NH**
  - **Exploit originated from NSA**
  - **Surgeries and hospital care cancelled**



Critical healthcare effected in the UK!

Advantage
TAILORED TECHNOLOGY SOLUTIONS

Sophisticated Understanding of Value

Monetizable criminal enterprise

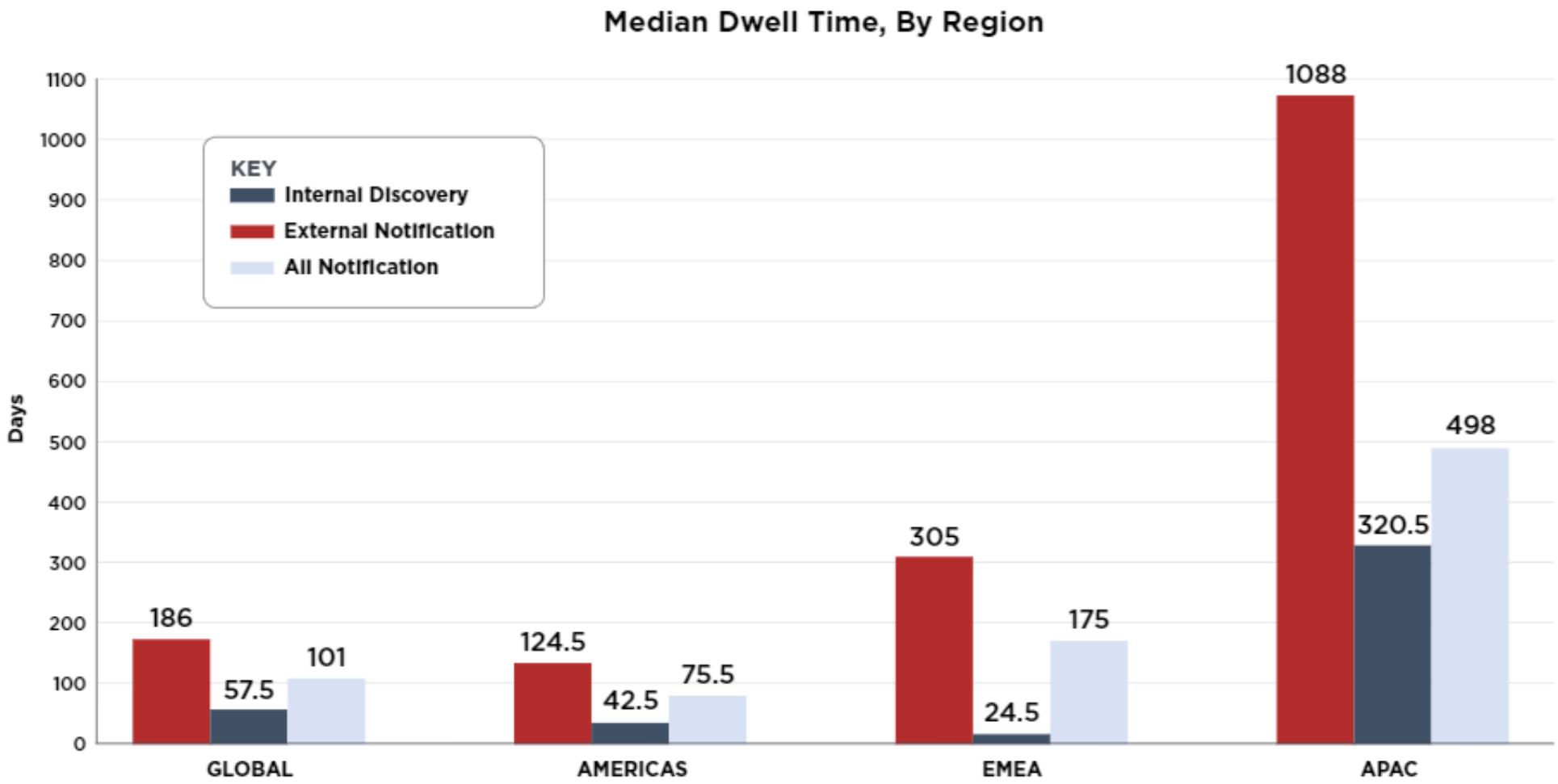
- Credit Cards
- Medical Records
- Intellectual Property
- Credentials
- Vulnerabilities
- Exploits

Source: HPE: the business of hacking

Advantage®
TAILORED TECHNOLOGY SOLUTIONS

MINISTRY OF SOCIAL DEVELOPMENT
TE MANATŪ WHAKAHIATO ORA

Dwell Time

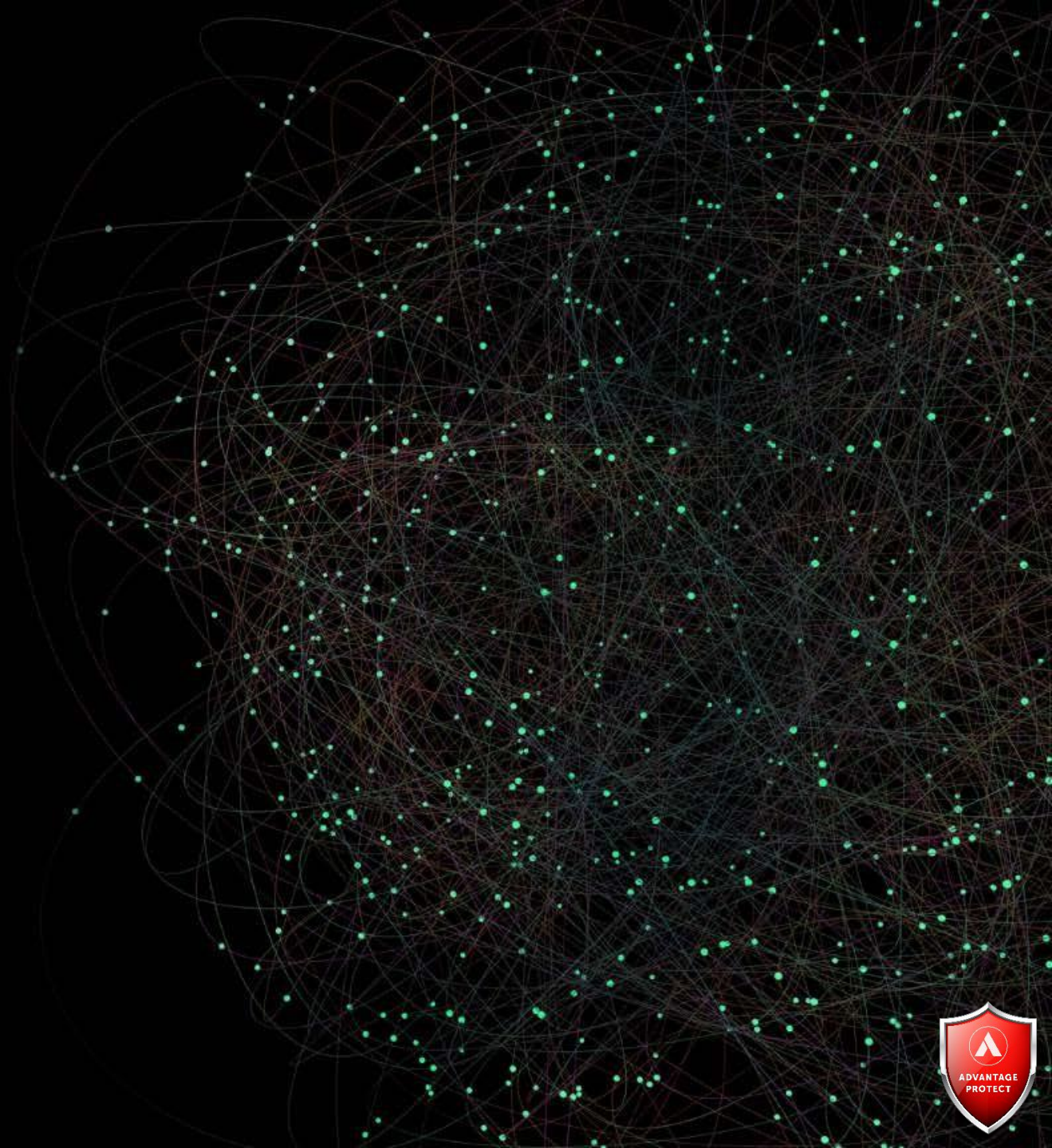


Median dwell time for externally notified breaches was 417 days in 2017 and 1,088 days in 2018 Fireeye Report

Advantage®
TAILORED TECHNOLOGY SOLUTIONS

Advantage®
TAILORED TECHNOLOGY SOLUTIONS

Blue Team



*“A **blue team** is a group who perform an analysis of information systems to ensure security, identify security flaws, verify the effectiveness of each security measure, and to make certain all security measures will continue to be effective after implementation.”*

Wikipedia

Advantage®
TAILORED TECHNOLOGY SOLUTIONS

- Security Operations Centre
  - Threat Intelligence

- Security Information Event Management (SIEM)

- Network protection
  - Authentication
  - Isolation
  - IDS/IPS

- Endpoint protection/EDR
  - Anti malware
  - Behavior analytics
  - Mobile Workforce

- Web protection
  - Web application firewalls/ DDOS filtering
  - Malware protection
  - Content filtering
  - Cloud Access Security Broker / CASB

- Vulnerability management
  - Patch Management
  - Configuration assurance

- Auditing and Compliance
  - Policy Review
  - Compliance assurance

- Incident Response and Forensics
  - Threat Hunting
  - Malware investigation/root analysis
  - Breach investigation
  - Legal/HR forensics

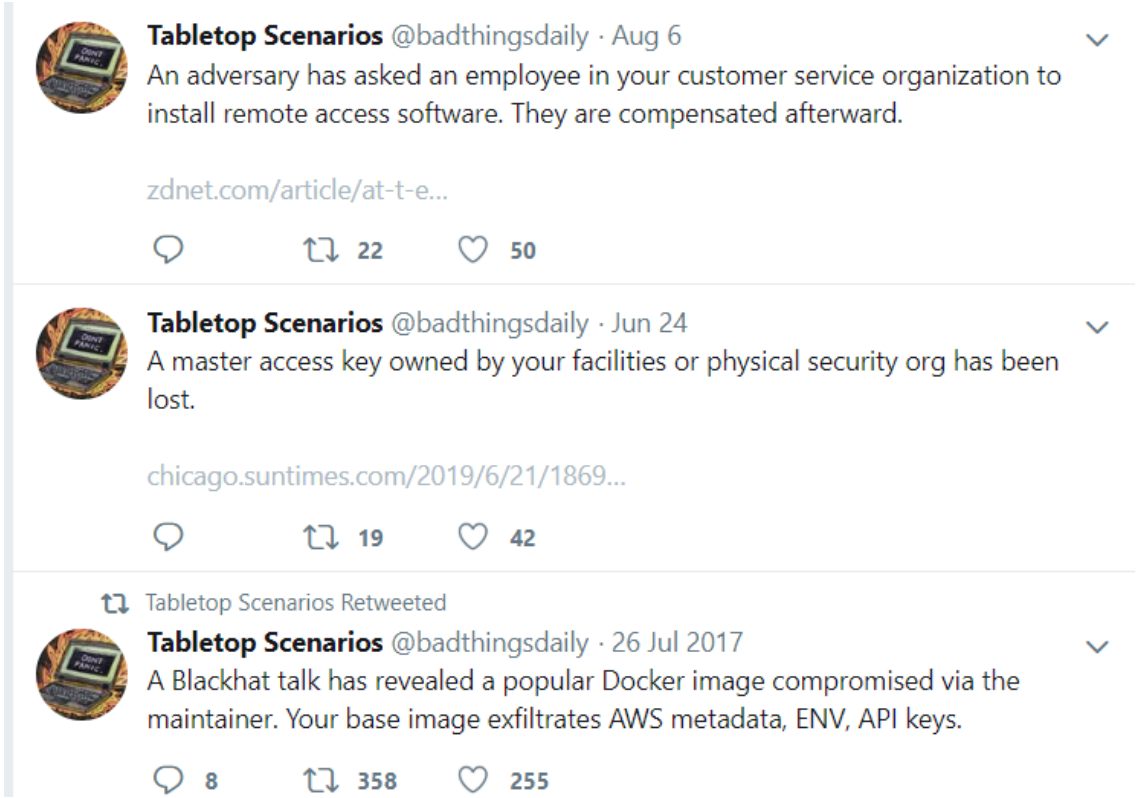
- Data Protection
  - DR and BCD
  - Data loss Prevention

- Mail protection
  - Spam
  - Malware
  - Archive

Advantage®
TAILORED TECHNOLOGY SOLUTIONS

Blue team evolved

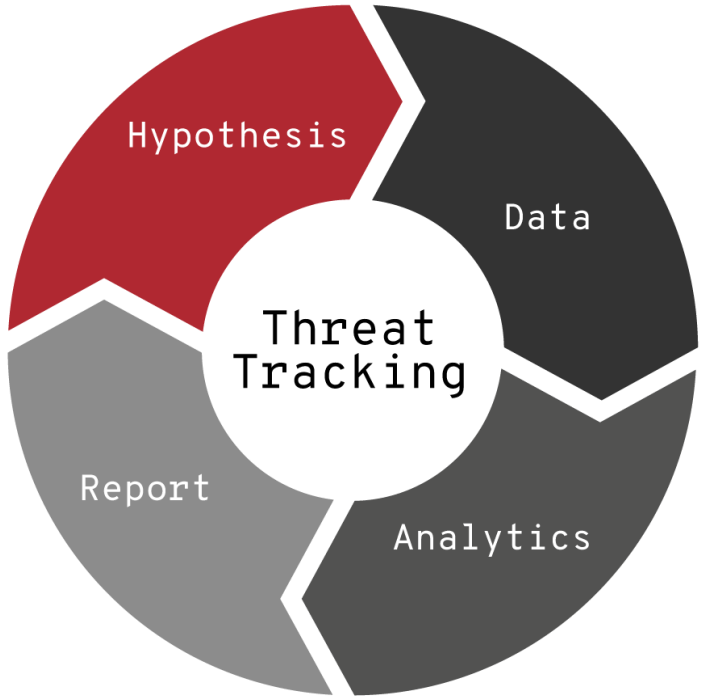
- Table top exercises
- Threat Hunting



Advantage
TAILORED TECHNOLOGY SOLUTIONS

Threat Hunting

- Known Bad
- Suspicious Behavior
- Unknown Bad



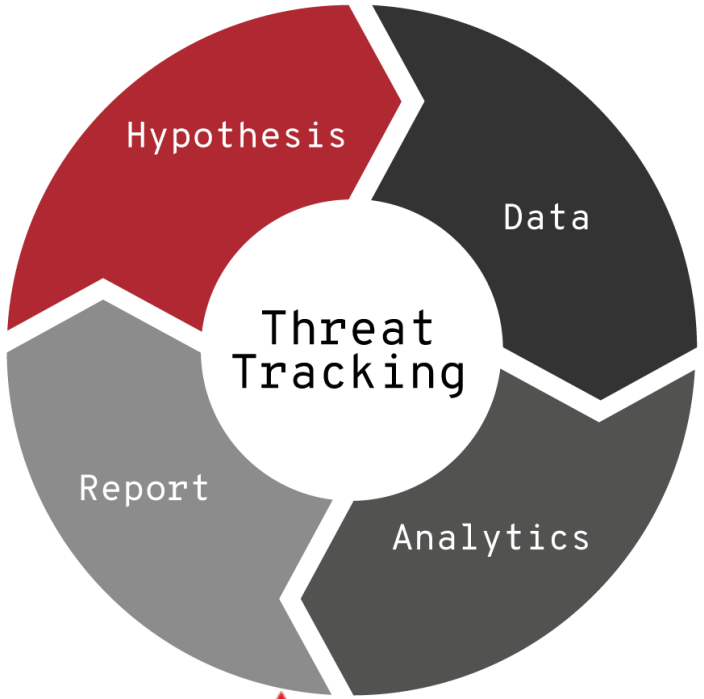
Advantage®
TAILORED TECHNOLOGY SOLUTIONS

Threat Hunting

Known Bad

- Indicators of Compromise
  - URLs
  - IPs
  - Domains
  - File (name, location, hash, signatures)
  - Country

- Threat feeds
  - Open source
  - Government
  - Industry specific
  - Commercial



Advantage®
TAILORED TECHNOLOGY SOLUTIONS

Threat Hunting

Suspicious Behavior

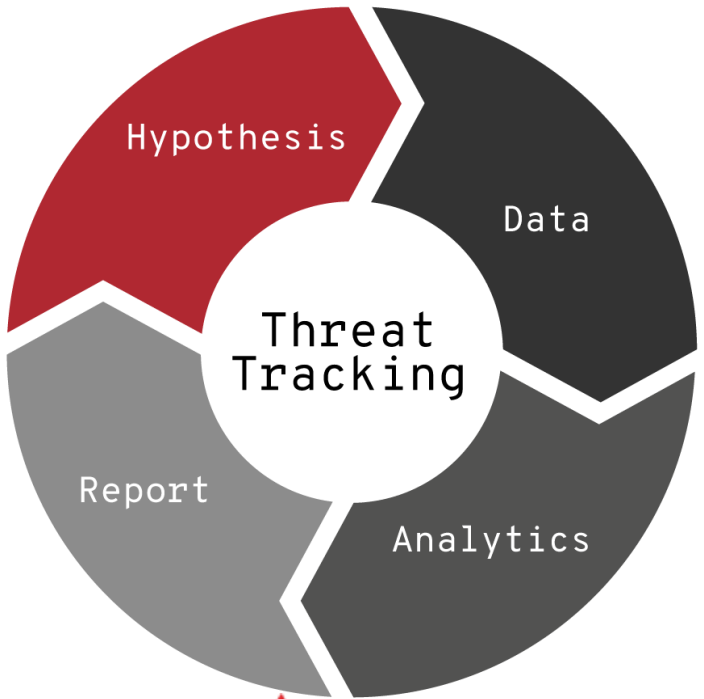
- Behavior analytics
  - Fast travel
  - Abnormal processes
  - Data use
- Employee/Customer reports
- Network traffic / application logs

Advantage®
TAILORED TECHNOLOGY SOLUTIONS

Threat Hunting

Unknown Bad

- Baseline
  - What is normal?
- Abnormal activity
  - Services
  - Files
  - Processes
  - Connections



Advantage®
TAILORED TECHNOLOGY SOLUTIONS

Advantage®

Questions

https://sli.do
Event ID: 6610

GAIN THE BUSINESS ADVANTAGE

Privacy and Data Breach Notification

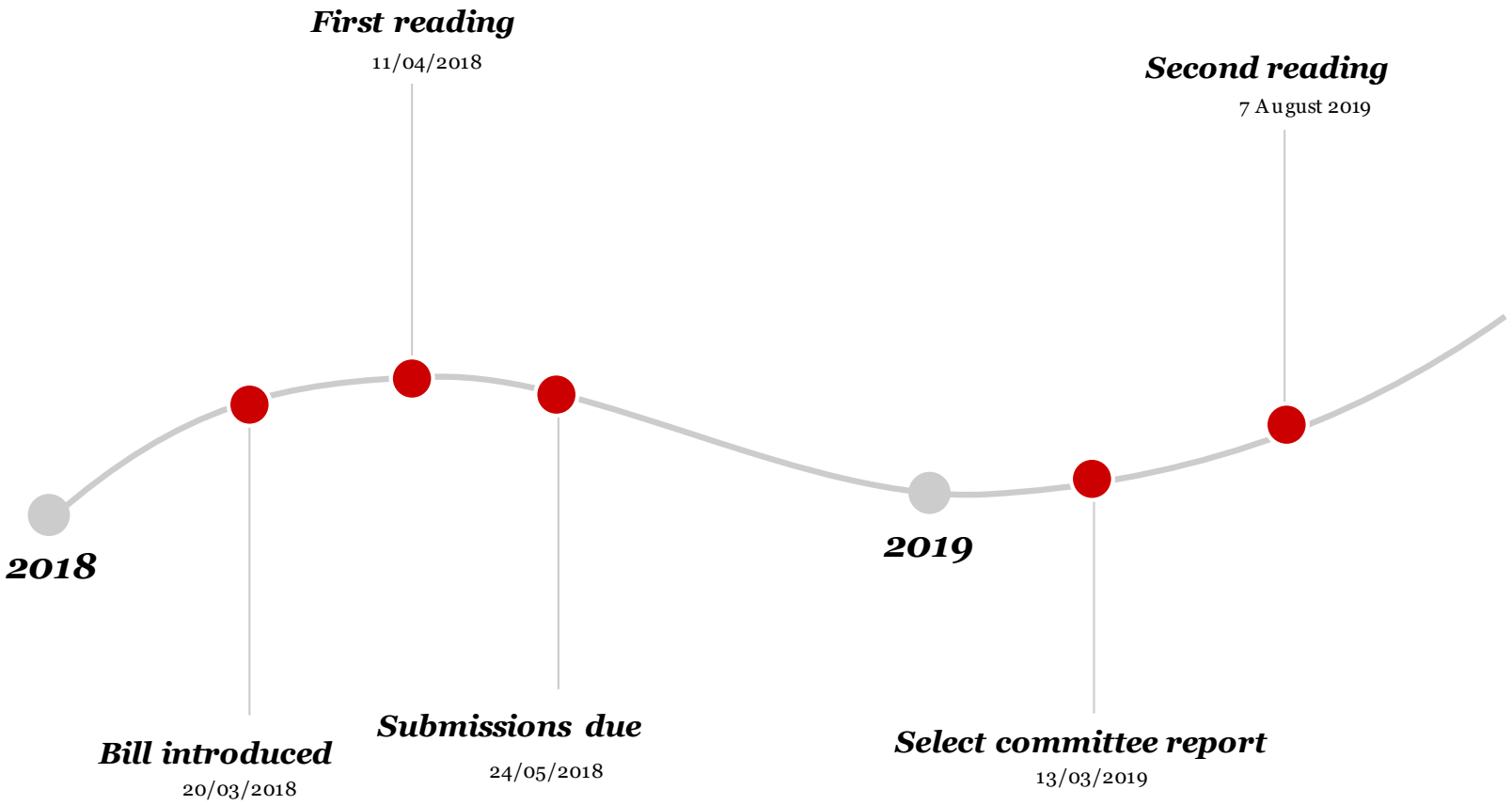
Richard Wells

3 October 2019

MinterEllisonRuddWatts

Privacy Bill – Current status

Where are we up to



Privacy Bill

- The Privacy Bill was introduced into Parliament in March 2018 and is set to replace the existing Privacy Act (expected to come into force March 2020).
- It is recommended that the Bill has a degree of extra-territorial effect.
- The Privacy Bill intends to provide for:
  - Stronger enforcement powers for the Privacy Commissioner
  - A mandatory data breach notification regime
  - Stricter rules around cross-border transfers
  - Tougher sanctions for non-compliance

Privacy Bill – Current status

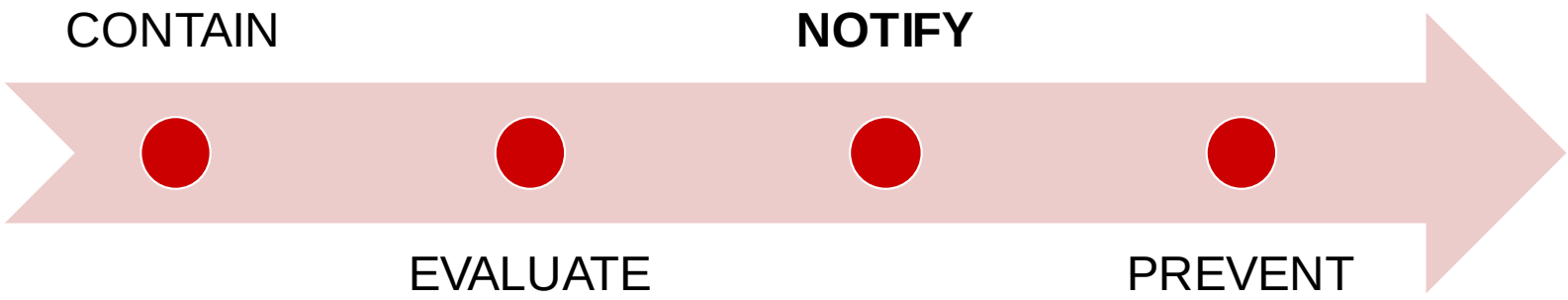
What is missing...

- From the Privacy Commissioner's wish list:
  - Increased financial sanctions
  - Right to data portability
- Compared to European data protection laws:
  - Right to data erasure
- From submissions:
  - Periodic review to keep up to date with tech
  - Practicality of Human Rights Review Tribunal's role
  - Privacy Commissioner accountability mechanism

Privacy Breach?

A '***privacy breach***' is unauthorised or accidental access to, or disclosure, alteration, loss or destruction of personal information OR an action which prevents access to personal information either temporarily or permanently

Privacy breach - notification



‘Serious Harm’ factors

- Action taken to reduce the risk of harm
- Does it involve sensitive data?
- The person or body that has obtained or may obtain personal information as a result of the breach
- Whether the personal information is protected by a security measure
- Nature of harm that may be caused to affected individuals
- Any other relevant factors

Example 1:

Scenario:

An attacker installs malicious software on a retailer's website which allows the attacker to intercept payment card details when customers make purchases. The attacker is also able to access basic account details for all customers who have an account on the website.

Does this constitute serious harm?

A privacy breach has occurred – But is **serious harm** being caused to all customers, not just the ones whose payment details have been taken?

Thoughts?

Example 2:

Scenario:

A data file, which includes the personal information of numerous individuals, is sent to an incorrect recipient outside the entity. The sender realises the error and contacts the recipient, who advises that the data file has not been accessed. The recipient has an ongoing contractual relationship with the sender, and regards the recipient as reliable and trustworthy. The sender then confirms that the recipient has not copied, and has permanently deleted the data file.

Does this constitute serious harm?

A privacy breach has occurred – But has any **serious harm** resulted from the breach?

Thoughts?

What information needs to be provided?

Privacy Commissioner

- Describe the incident
- Number of individuals affected
- Identity of entity or individual holding the information in an unauthorised manner
- The response plan
- The plan to notify affected individuals
- Provide contact details of someone within the agency to contact for inquiries

Affected Individuals

- Describe the incident and steps being taken to respond to it
- Any steps the individual needs to take to mitigate risk
- Describe in general terms who has the information
- Confirm that the Privacy Commissioner has been notified and advise of right to make a complaint
- Provide contact details of someone within the agency to contact for inquiries

The lead-up to 2020:

- Systems and processes to identify data breaches
- Clear written plan for data breach
- Privacy risk assessment and ‘dashboarding’

MinterEllisonRuddWatts

minterellison.co.nz

Advantage®

Questions

https://sli.do
Event ID: 6610

GAIN THE BUSINESS ADVANTAGE