COS30015 IT Security

Week 2

Presented by Dr Rory Coulter

7 August 2024

Acknowledgement of Country

We respectfully acknowledge the Wurundjeri People of the Kulin Nation, who are the Traditional Owners of the land on which Swinburne's Australian campuses are located in Melbourne's east and outer-east, and pay our respect to their Elders past, present and emerging.

We are honoured to recognise our connection to Wurundjeri Country, history, culture, and spirituality through these locations, and strive to ensure that we operate in a manner that respects and honours the Elders and Ancestors of these lands.

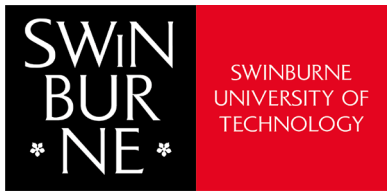
We also respectfully acknowledge Swinburne's Aboriginal and Torres Strait Islander staff, students, alumni, partners and visitors.

We also acknowledge and respect the Traditional Owners of lands across Australia, their Elders, Ancestors, cultures, and heritage, and recognise the continuing sovereignties of all Aboriginal and Torres Strait Islander Nations.

Offensive & Defensive Security
Cyber Roles
Red, Blue & Purple Teams
Threat Hunting
Security Tools and Commands
Cyber Security Exercises
Assessment

SWINBURNE UNIVERSITY OF TECHNOLOGY

Offensive & Defensive Security

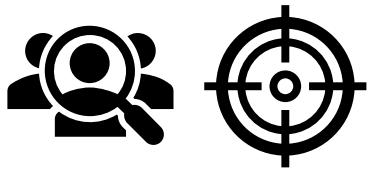


Offensive vs Defensive Security

Ultimately organisations favour defensive security over active probing production systems, but require a mixture

Understand the concepts

- Offensive
- Proactive approach to identify weakness, vulnerabilities
- Penetration tests***, mimic
- Active



- Defensive
- Preventative measures
- Detect incidents
- Passive

*** Very common for audit purposes

SWINBURNE UNIVERSITY OF TECHNOLOGY

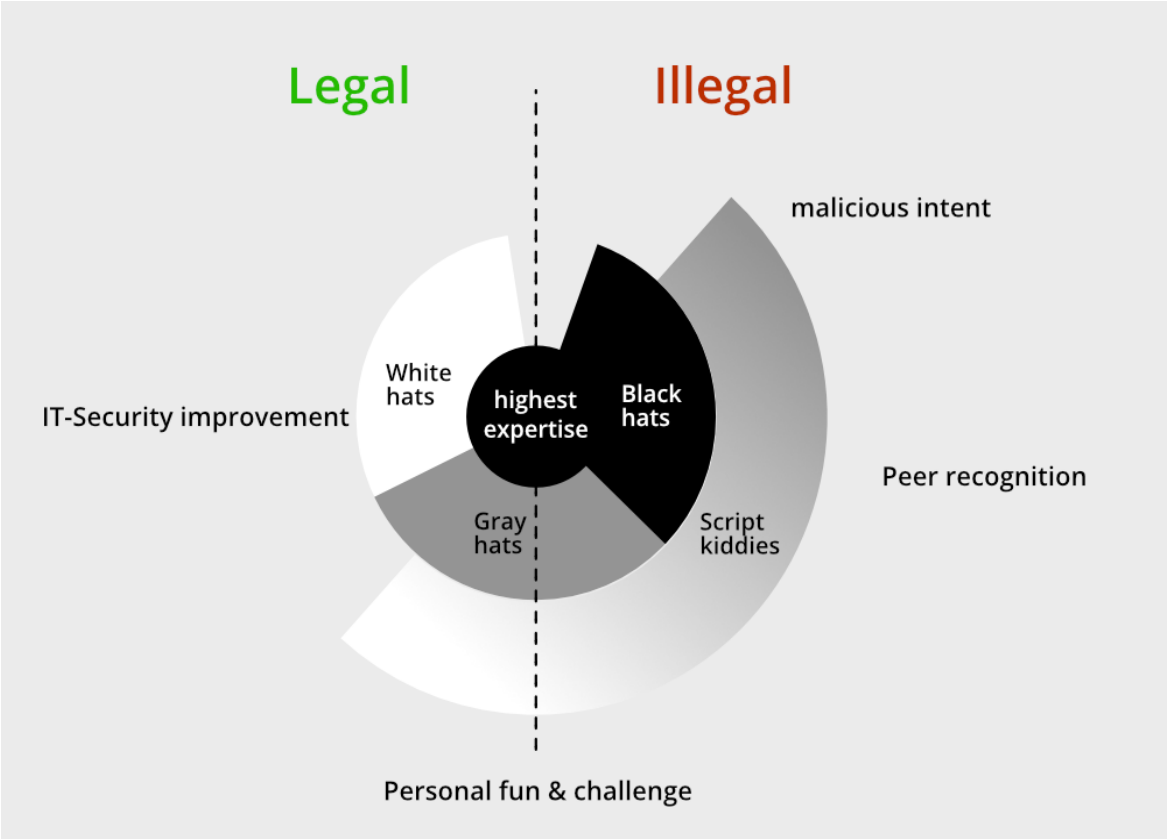
Player Recap

Broad Perspective(s)

Apposing sides defined by legality

Good intentions don't justify the action

Perspective 1	Perspective 2	Action
Patch	Exploit	Scan vulnerability
Report	Catalogue	Scan vulnerability
Automation/ administration	Persistence	Schedule task
Expose	Ransom	Website defacement
Expose	Ransom	Data leak



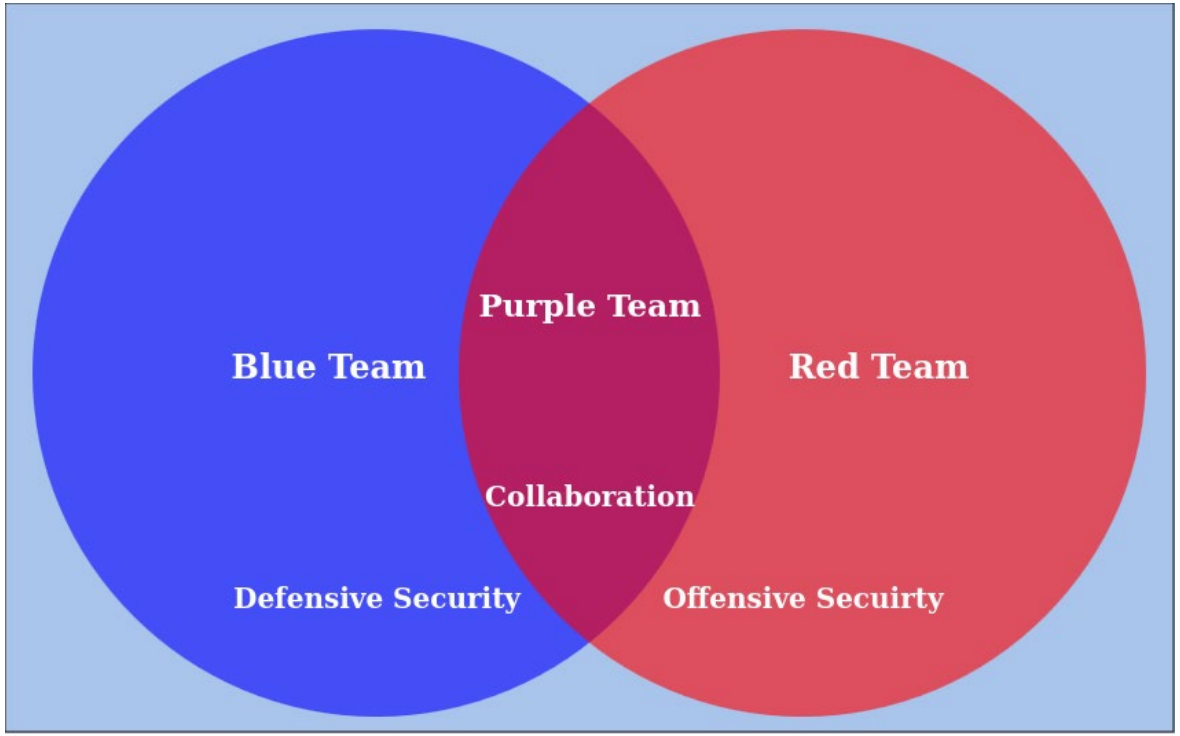
SOURCE: https://www.geeksforgeeks.org/what-are-white-hat-gray-hat-and-black-hat-hackers/

Roles

SWINBURNE UNIVERSITY OF TECHNOLOGY

Role Terms

Commonly used jargon to explain where your role aligns



Cyber Roles

Typical roles from graduate to principal

Mixture of offensive and defensive roles, and paper team

How to stand out? Blog or social posts investigating tools, use cases, pen test write ups, OSINT analysis, etc.

Role	Technical?
Incident Responder (forensic analysis)	Yes
Incident Handler	No
Threat Hunter	Yes
Malware Analyst	Yes
Governance, Risk & Compliance (GRC)	No
Vulnerability Management	Yes
Network***	Yes
Analyst (SOC, SIEM, Security Tool***)	Yes
Administrator	Yes
Penetration Tester	Yes
Consultant	Mixed
Technical Writer	Mixed
Infrastructure	Mixed
Intelligence	Mixed
Project manager, communications, legal	No

SWINBURNE UNIVERSITY OF TECHNOLOGY

Cyber Roles

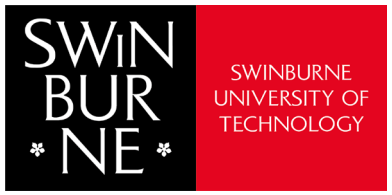
Typical roles from graduate to principal

Potential designation

Role	Technical?
Incident Responder (forensic analysis)	Yes
Incident Handler	No
Threat Hunter	Yes
Malware Analyst	Yes
Governance, Risk & Compliance (GRC)	No
Vulnerability Management	Yes
Network***	Yes
Analyst (SOC, SIEM, Security Tool***)	Yes
Administrator	Yes
Penetration Tester	Yes
Consultant	Mixed
Technical Writer	Mixed
Infrastructure	Mixed
Intelligence	Mixed
Project manager, communications, legal	No

SWINBURNE UNIVERSITY OF TECHNOLOGY

Red, Blue & Purple Teams



Red Teams

The role of the Red Team is to identify the gaps in the organisation in an authorized manner

- Have to think like a hacker
- Test the effectiveness of the organisation's security program
- Emulate the tactics, techniques, and procedures used by likely adversaries
- Runs tests over a prolonged period to find vulnerabilities and weakness
- Provide a complete audit of testing results
- Perform Regular Penetration Testing to determine how secure the systems are and what are the vulnerabilities or misconfigurations
    - White-box
    - Black-box
    - Grey-box

Tools

- C2 Frameworks: Metasploit
- Social Engineering frameworks: Social Engineering Toolkit (SET)
- Asset Discovery tools: Amass, Shodan

Red Teams - Penetration Testing

	Black-Box *aka close box penetration testing*	Grey-Box *combination of black box and white box testing*	White-Box *aka open box penetration testing*
Goal	Mimic a true cyber attack	Assess an organization's vulnerability to insider threats	Simulate an attack where an attacker gains access to a privileged account
Access Level	Zero access or internal information	Some internal access and internal information	Complete open access to applications and systems
Pros	Most realistic Testing is performed from point of view of attacker	More efficient than black-box andsaves on time and money Testing is performed from point of view of attacker	More comprehensive, less likely to miss a vulnerability and faster Testing is performed from point of view of attacker
Cons	Time consuming and more likely to miss a vulnerability	No real cons for this type of testing	More data (ex, source code) is required to be released to the tester and more expensive

SOURCE: https://www.packetlabs.net/posts/types-of-penetration-testing/

Blue Teams

The role of the Blue Team is to defend the organization against threats in the wild and improve the organisation's defences

- Defends against both real attackers and red teams
- Align security tooling and detection to TTPs, protect crown jewels
- Validate IRP and playbooks in case of an incident
- Adjust security posture based on insights from the red team and SOC
- Continuously improve detection and response
- Keep up with new threat intelligence
- Deploy and maintain security tooling
    - SOAR (Security Orchestration, Automation and Response)
    - SIEM (Security information and event management) tools

Purple Teaming

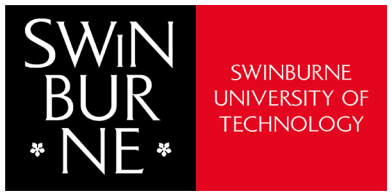
Red Team + Blue Team = Purple Teaming

- Members between the Red and Blue Teams
- To prepare red and blue teams and promote intel sharing
    - helps the Red Team understand the organisation's security policies and procedures
    - helps the Blue Team understand the vulnerabilities that the Red Team has identified
    - helps the Blue Team improve their incident response capabilities by providing feedback on their performance during simulated attacks
- Purple Teaming is a methodology and not a team inside the organisation

Offensive & Defensive Security
Cyber Roles
Red, Blue & Purple Teams
Threat Hunting
Security Tools and Commands
Cyber Security Exercises
Assessment

SWINBURNE UNIVERSITY OF TECHNOLOGY

Threat Hunting



Threat Hunting

Search for potential threats within a system or network

IoCs, TTPs, Living off the Land activity, Intelligence, Anomalies

- Security tooling alone is not a foolproof means to detect all threats
- Having an alert rule for every possible threat, action, technique is not applicable
- Threat hunting compliments security tooling as a way to proactively search for threats through different means
- Living off the Land based threats maximise this rule issue, as adversaries do not install and only make use of existing resources
- An adversary with a long dwell time is not raising any alerts, still worthwhile to hunt for threats

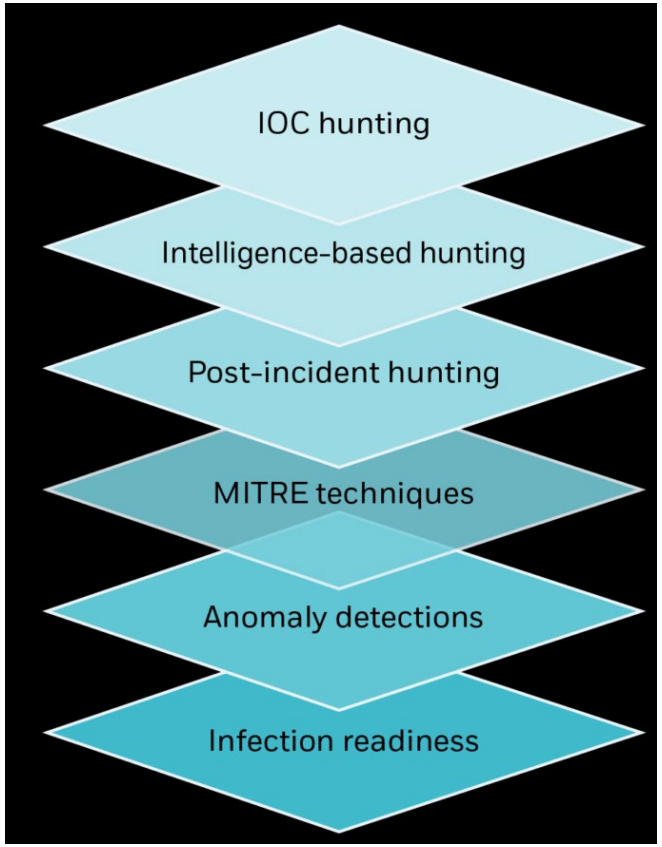


IMAGE SOURCE: https://www.cyberproof.com/cyber-101/threat-hunting/

Threat Hunting in Perspective

Threat Hunting is a compliment to other incident and security operations/activities

Top Tools:

- Dedicated threat hunter or part of a role
- SIEM
- Security Analytics
- Endpoint Detection and Response

Identify suspicious activity (possibly false positives)

Use intelligence to guide a starting point

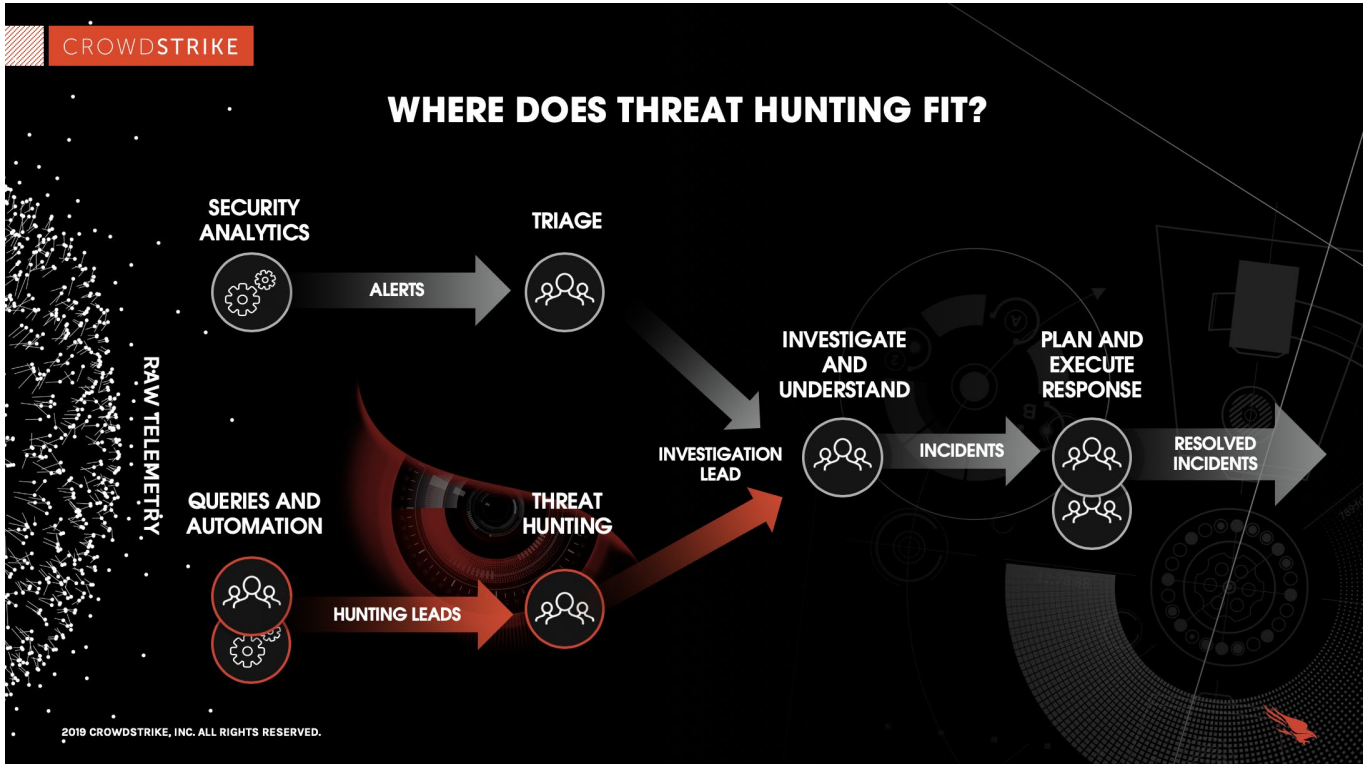


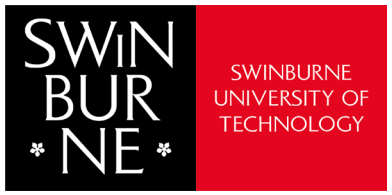
IMAGE SOURCE: https://www.crowdstrike.com/cybersecurity-101/threat-hunting/

SWINBURNE UNIVERSITY OF TECHNOLOGY

Offensive & Defensive Security
Cyber Roles
Red, Blue & Purple Teams
Threat Hunting
Security Tools and Commands
Cyber Security Exercises
Assessment

SWINBURNE UNIVERSITY OF TECHNOLOGY

Team Tools and Commands



Red Team Tools

A small selection of notable tools across various MITRE ATT&CK Tactics

- Reconnaissance
- Showdan[.]io (search engine)
- Initial Access
- Hydra (brute force)
- King Phisher
- Execution
- Rubeus (Active directory hack tool)
- Credential Access
- Mimikatz (Windows credential extractor)
- hashcat Password hash cracking
- John the Ripper Password hash cracking
- Collection
- BloodHound (Active directory visualisation)
- Impact
- SlowLoris (Simple denial of service)

SWINBURNE UNIVERSITY OF TECHNOLOGY

Red Team Commands

Educational Only – Do not perform

- Hiding the local admin account
- reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList" /t REG_DWORD /v hiddenaccountname /d 0 /f
- reg add: Adds or modifies registry keys and values
- "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList": Specifies the registry key path where the user account settings are stored
- /t REG_DWORD: Specifies the data type (DWORD) for the value
- /v hiddenaccountname : Sets the name of the value
- /d 0: Sets the value data to 0, which means the user account will be hidden
- /f: Forces the operation without prompting for confirmation

Red Team Commands

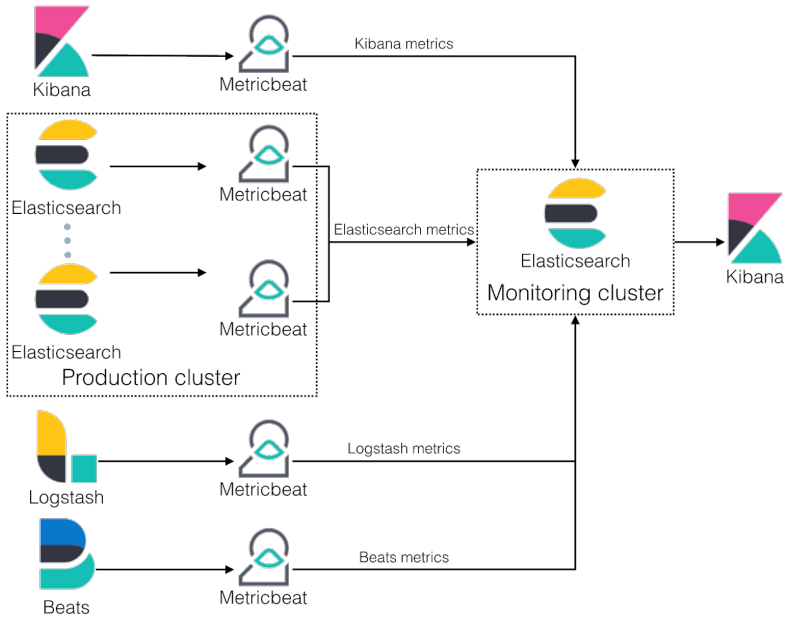
Educational Only – Do not perform

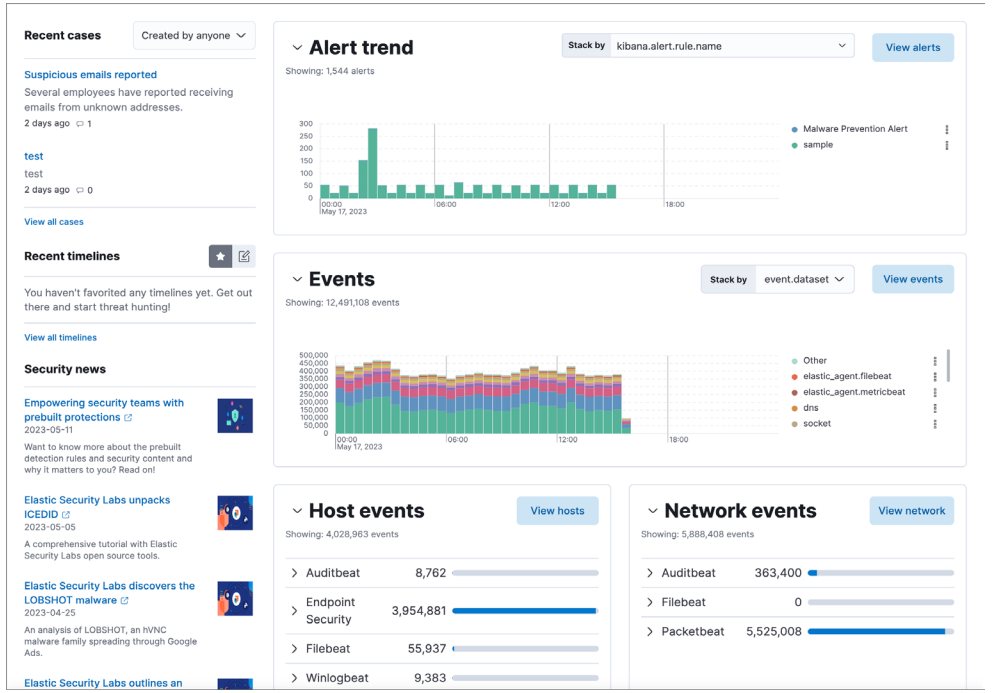
- Drop Defender signatures
- %Program Files%\Windows Defender\MpCmdRun.exe" -RemoveDefinitions –All
- -RemoveDefinitions -All: These parameters instruct Windows Defender to remove all virus and spyware definitions
- Determine is host is within a VM
- reg query HKLM\SYSTEM /s | findstr /S "VirtualBox VBOX VMWare"
- eg query command to search the HKLM\SYSTEM registry hive
- The | findstr /S "VirtualBox VBOX VMWare" part filters the results to include only lines containing the specified keywords
- If any references to VirtualBox, VBOX, or VMWare are found, they will be displayed

SWINBURNE UNIVERSITY OF TECHNOLOGY

ElasticSearch SIEM Demo

Linking adversary TTPs to security tooling





SOURCE: https://www.elastic.co/guide/en/elasticsearch/reference/current/monitoring-overview.html

https://www.elastic.co/guide/en/security/current/overview-dashboard.html

SWINBURNE UNIVERSITY OF TECHNOLOGY

Blue Team Tools

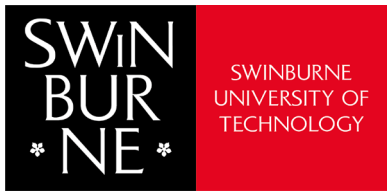
A collection of useful tools

- Threat Intelligence
- MISP
- Malware Detection and Analysis
- VirusTotal
- IDA (disassembler and debugger)
- Ghidra (reverse engineering tool)
- Data Recovery
- Recuva
- TestDisk
- Digital Forensics
- SANS SIFT
- The Sleuth Kit (disk analysis)
- Autopsy (forensic platform)

Offensive & Defensive Security
Cyber Roles
Red, Blue & Purple Teams
Threat Hunting
Security Tools and Commands
Cyber Security Exercises
Assessment

SWINBURNE UNIVERSITY OF TECHNOLOGY

Cyber Security Exercising



Cyber Exercises

Prepare before an incident occurs, a matter of when, not if

You've been part of exercises in other forms

- Ever been a part of a fire drill?
- It was testing plans and procedures to see if they were still relevant,
- Seek to identify if there were any fundings (building A was slower than building B)
- Meet regulatory and potentially legal requirements
- Provide testing opportunities for the responders
- Cyber is no different, we want to test incident response documentation
- Find gaps in the organisation (data not making it's way into a security tool)
- Provide training for security staff
- Prepare against a give adversary

Curious, explore more https://www.cyber.gov.au/resources-business-and-government/exercise-in-a-box

SWINBURNE UNIVERSITY OF TECHNOLOGY

Exercise Types & Teams

Exercises can be range from discussion to live play

Type	Characteristic	Team	Duration	Potential Aims
Tabletop (TTX)	Discussion based	Blue team SOC, Security Operations	2 -3 hours	Develop processes Educate Test response plans and processes
Hybrid	Discussion based Perform incident management tasks such as communication	Blue team	2 -3 hours	Develop processes Educate Test response plans and processes
Functional	Investigate technical artefacts forensically Offline artefacts	Blue team, some Red team input potentially in intelligence	3 – 4, 1 day	Develop processes Educate Test response plans and processes Test forensic tooling and know how
Functional Pre-Seeded	Artefacts are seeded in the environment Use own tooling and processes	Purple team	3 – 4, 1 day to week(s)	Develop processes Educate Test response plans and processes Test forensic tooling and know how Test system logging and tooling

Exercises can include technical teams to executives, boards and other business functions

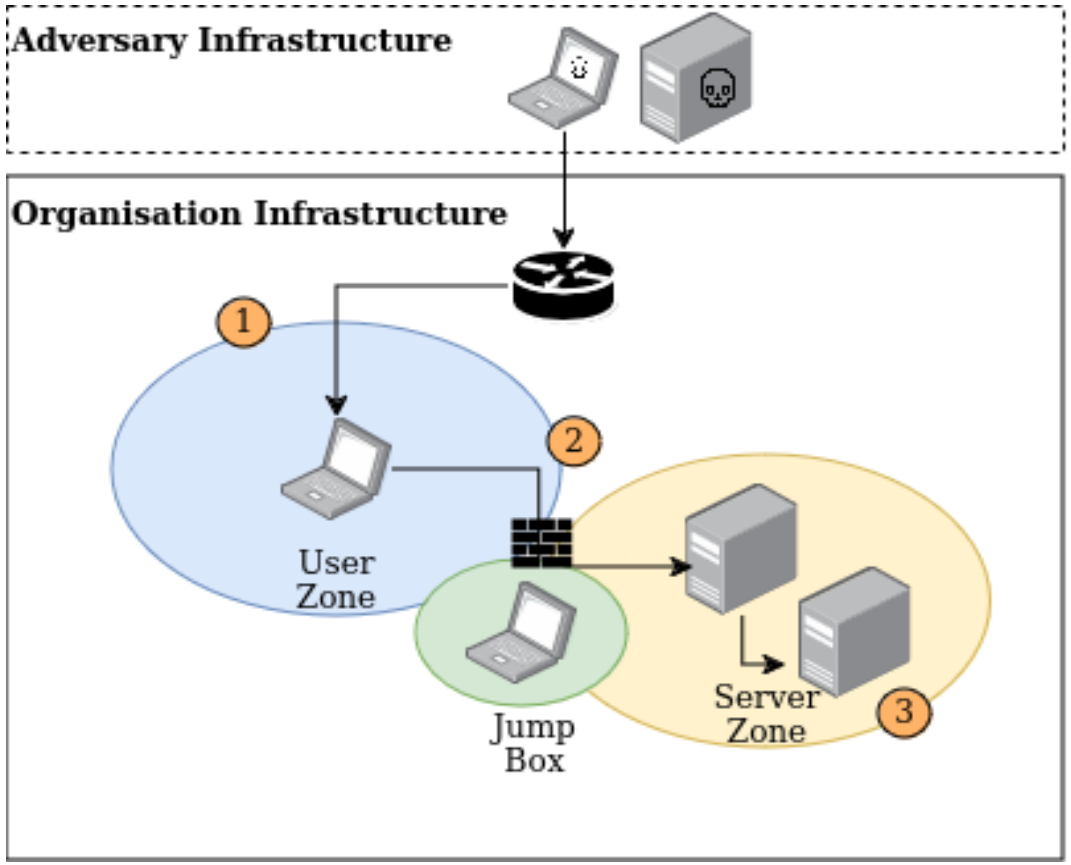
SWINBURNE UNIVERSITY OF TECHNOLOGY

Exercise Planning

Planning requires several elements to be identified

Consider

- Threat type
- Adversary backstory and steps
- TTPs to be tested
- Target audience
- Identification of tooling, systems, data sources to be analysed



Offensive & Defensive Security
Cyber Roles
Red, Blue & Purple Teams
Threat Hunting
Security Tools and Commands
Cyber Security Exercises
Assessment

SWINBURNE UNIVERSITY OF TECHNOLOGY

Assessment

SWINBURNE UNIVERSITY OF TECHNOLOGY

Current and Upcoming Assessment

Best to understand your responsibilities

- Assignment 1, due the XXX
  - Offensive and Defensive
- Quiz, week 7 lab
  - In class only and lab content, multiple choice, very easy
- Assignment 2, released after Assignment 1
- Assignment 2 is forensic-based, write a review of what has happened
- Assignment 1 walkthrough