Cyber:

HOW TO LAND YOUR FIRST CYBER ROLE IN INDUSTRY AND HOW TO SUCCEED

MATT SIOMOS – OCTOBER 2024

Agenda

- Cyber role OSINT: searching for your first role
- Cyber interview TTPs: tactics, techniques and procedures
- Corporate cyber life: how to succeed
- Discussion

About Me

- 20+ years in IT / Cyber Security
- Managed dozens of cyber incidents including ransomware, data theft and business email compromise for well known Australian businesses
- SOC, incident response, GRC, ISO27001 specialties
- Junior basketball coach

CYBER ROLE OSINT

SEARCHING FOR YOUR FIRST ROLE

Typical Organisations

- Large corporates – financial services, energy, telecommunications etc.
- Managed security service providers (MSSP) – CyberCX, Telstra, NCC, Data3, Tesserant, TrustWave, NTT, Macquarie etc.
- Consulting firms – Deloitte, KPMG, EY, PwC/ Scyne advisory, AON, BDO etc.
- Medium size businesses

Typical Entry Level Roles

- General (cyber analyst)
- Blue teamer (SOC Analyst, vulnerability analyst)
- Red teamer (junior pen tester)
- GRC (supply chain analyst, cyber risk analyst, threat analyst)
- NICE framework

Which Companies To Target?

- Research the company
  - What threats / incidents have impacted the same industry?
    - Google, ACSC, MITRE ATT&CK groups, FireEye Mandiant
  - Know their values
    - Do they align to your own values? Have examples

Searching For Roles

- Job boards – Uni, SEEK, graduate programs
- Clubs – AISA, LTOTM, ISACA, MeetUp, 2600
- Conferences and events – BSides, uni open days
- LinkedIn connections
- Direct

A CV That Gets Shortlisted

- Demonstrate experience and passion outside of your uni course
  - Volunteer, cyber clubs, webinars, home lab, TryHackMe
- What is unique about you?
  - Write a blog or LinkedIn post or post a YouTube video about something security related you've done
- Cover letter
  - Don't CV spray - tailor it to each organisation you're applying to
- Focus on what you achieved, what value you added
- Check your grammar and spelling, use dot points and cyber key words

Cyber Interview TTPs

TACTICS, TECHNIQUES AND PROCEDURES FOR THE INTERVIEW

What the Interviewer is Looking For

Cultural

- Alignment to company values
- Passion for cyber
- Eager to learn
- Not a brilliant jerk

What the Interviewer is Looking For

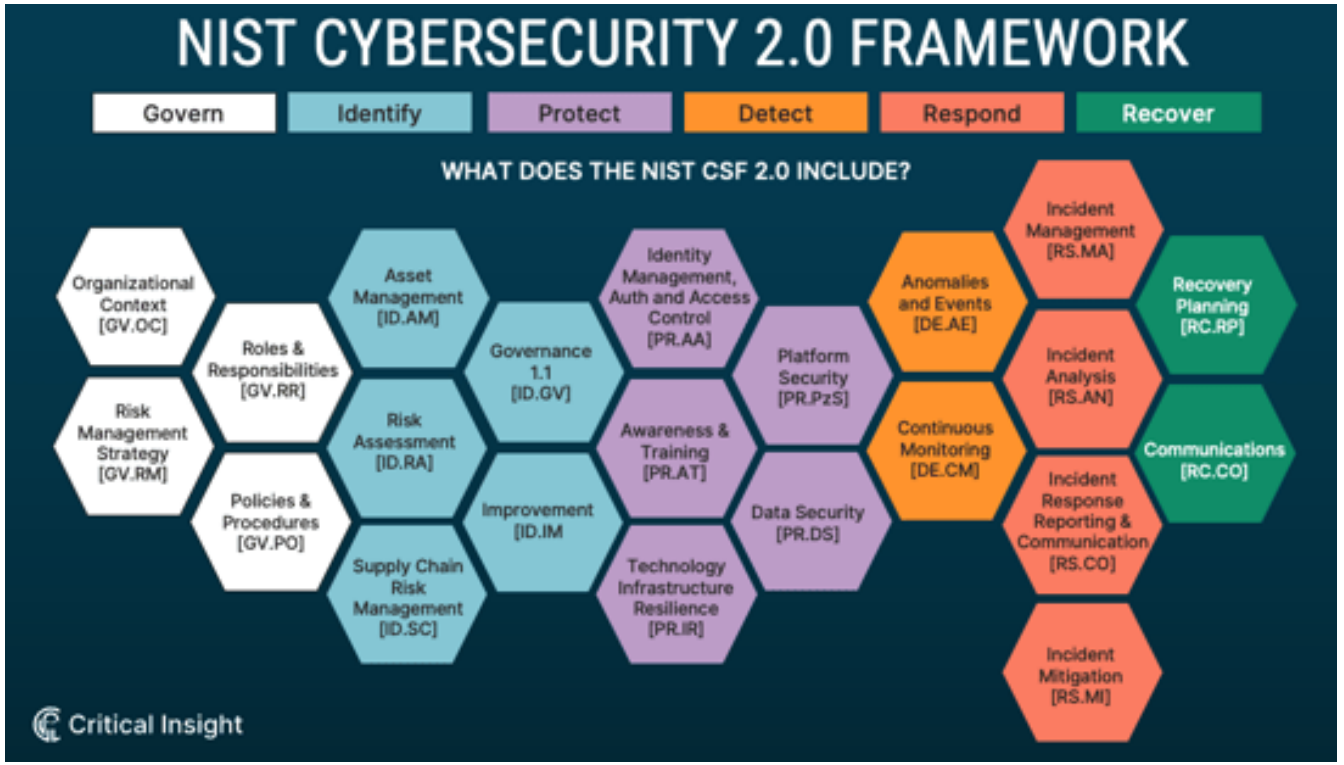
Technical

- General Cyber
  - Kill chain, MITRE ATT&CK, frameworks: NIST, ASD Essential 8, OWASP
- Technology Platforms
  - Linux, Windows, Cloud: AWS, Azure
- Security Tools
  - Kali, vulnerability scanning, EDR, open source
- Industry Context
  - Threat intelligence and real world attacks: Optus, Medibank, Lattitude Financial

Security Frameworks

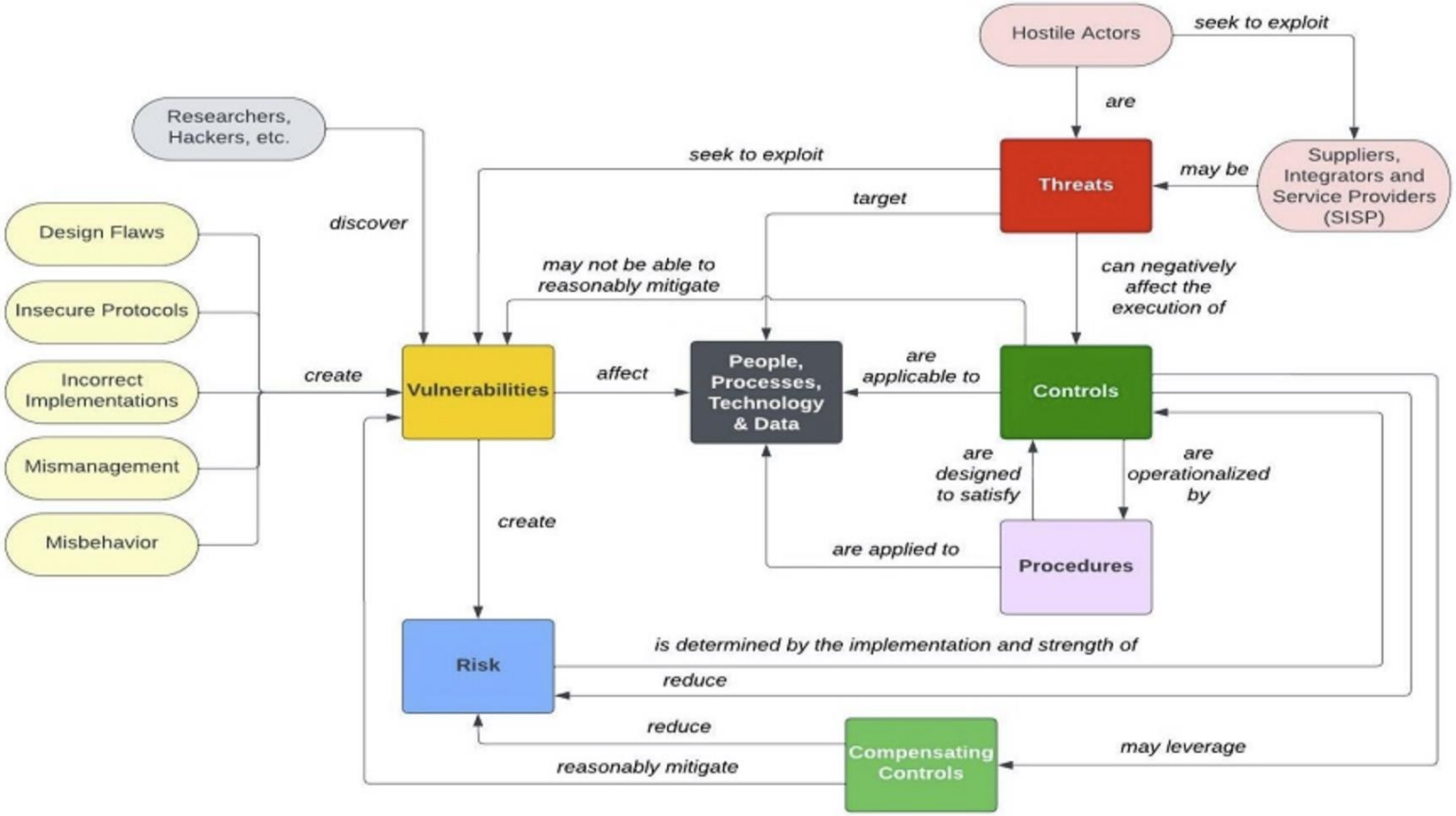
Best practice frameworks

- General
  - NIST, ISO27001, ASD Essential 8
- Industry specific
  - SOCI, APRA CPS234, PSPF, PCI



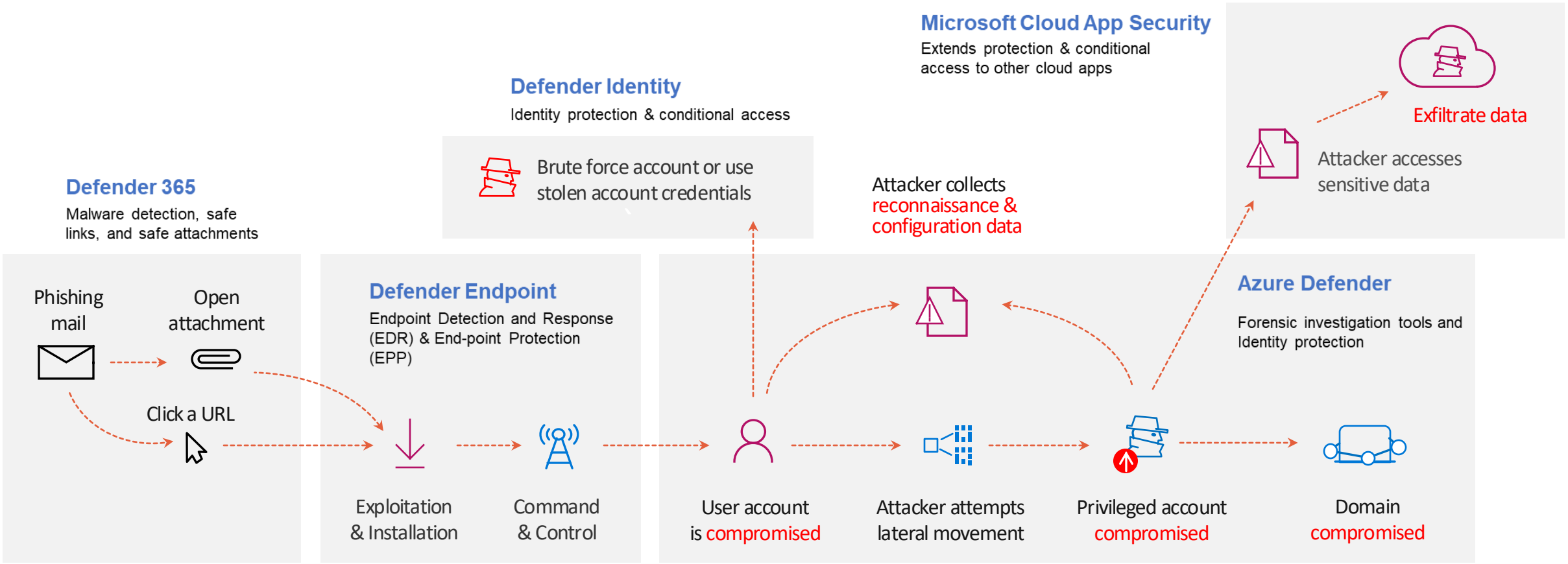
https://cybersecurity.criticalinsight.com/nist_csf_2.0

Risk, Threat, Controls Fundamentals



https://securecontrolsframework.com/risk-management-model/

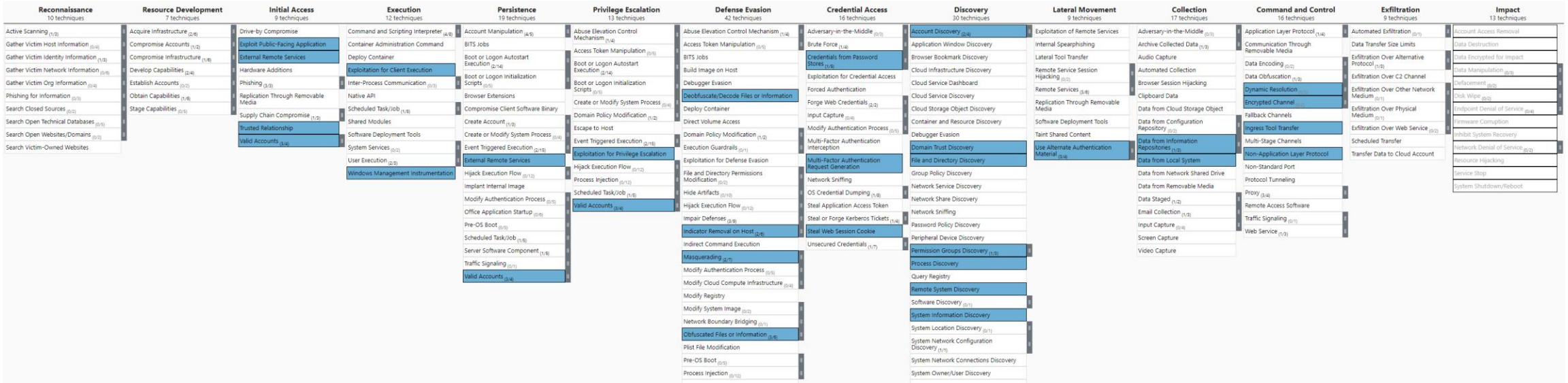
Kill Chain



https://docs.microsoft.com/en-gb/security/cybersecurity-reference-architecture/mcra

MITRE ATT&CK

- Adversary tactics, techniques and procedures



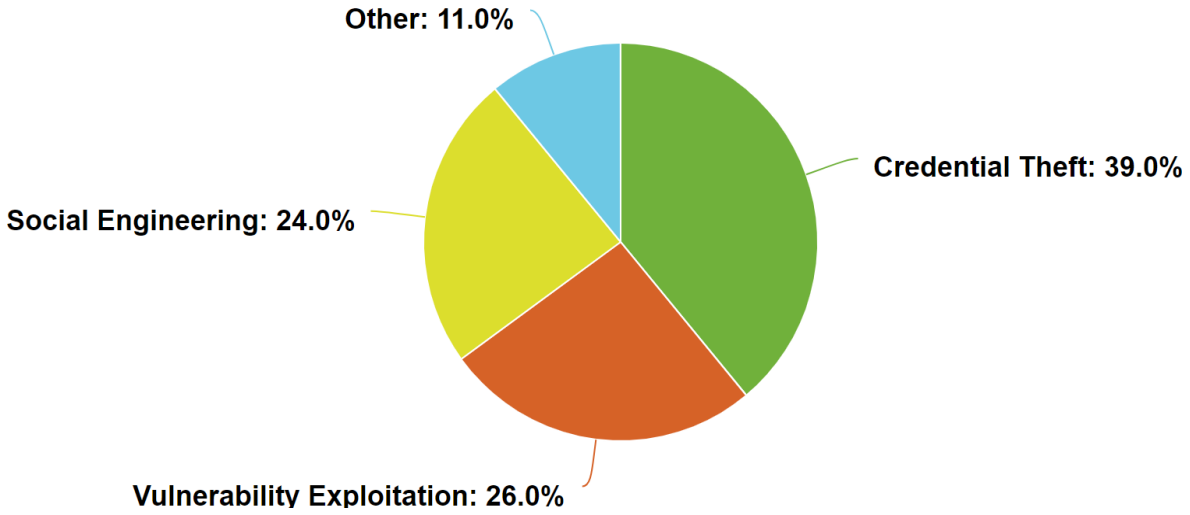
https://mitre-attack.github.io/attack-navigator/
APT29 overlay

Top Attack Techniques

- Top 10 lists – Red Canary (and others)
  - T1059: PowerShell / Command and Scripting Interpreter
  - T1059: Windows Command Shell
  - T1047: Windows Management Instrumentation
  - T1078: Cloud Accounts
  - T1027: Obfuscated Files or Information
  - T1053: Email Forwarding Rule
  - T1003: OS Credential Dumping
  - T1218: Rundll32
  - T1105: Ingress Tool Transfer
  - T1036: Rename System Utilities

Top Cyber Intrusions

Top intrusions



Arctic Wolf State of Cybersecurity 2024 Trends Report

How to protect

- Credential theft
  - MFA, O365 conditional access, Geofencing, dark web monitoring, privileged access management, password policy, SOC/SIEM
- Phishing
  - Email threat protection, SPF/DKIM, phishing campaigns, security awareness training, supply chain security
- Exploit vulnerabilities
  - vulnerability scanning, pen tests, WAF, patching, post exploitation (EDR, app. whitelisting)
- ASD Essential 8

Technical Scenario

You get a security alert – ransomware or c2 traffic, what do you do?

- Analyse
  - Form a hypothesis
  - Look for data to either prove or disprove the hypothesis
  - Correlate data in security tools and event logs (SIEM)
  - Pivot
  - Blast radius
  - Take an image
  - Attribution
- Contain
  - Isolate: quarantine endpoint, disable account, isolate network, block traffic on firewall
  - DON'T shutdown device if you can avoid it
- Eradicate
  - Remove malicious program / re-image device
- Recover
  - Restore from backup

Interview Summary

- Bring your best, authentic self
- Be prepared, don't wing it
  - Arrive early, wear formal attire, bring examples of your work
  - Research the company and their values
- Prepare responses to questions, use STAR
  - https://hbr.org/2021/11/10-common-job-interview-questions-and-how-to-answer-them
- Follow up after your interview

Starting Salaries

- Most importantly, gain experience. Hard work and learning today means money tomorrow
- If you get the chance to do unpaid volunteer work, take the opportunity
- For entry level roles you may expect to start on 65k to 80k p.a + super

Corporate Cyber Life: How To Succeed

Trust

- Most companies will have this as a core value

- How to build trust
  - Be reliable
  - Take ownership
  - Be humble and vulnerable
  - Manage your workload and other's expectations

John Cutler ar (Twitter)

First Month – What to Expect

- Lots of reading and training – company policies, tool specific training
- Work examples
  - Reviewing phishing Email that gets blocked
  - Cyber hygiene – following up other teams on vulnerabilities, finding unprotected assets
  - Issuing security questionnaires to third parties
  - Triaging security alerts
    - SIEM alerts
    - Data loss prevention alerts
- Build trust by doing well in the boring tasks and you're better placed to get more interesting work

Corporate Challenges

- 1000s of known problems (let alone novel attack techniques and unknown threats)
- Resource constrained (skills, time, budget)
- Lots of opinions and different priorities among teams
- Lots of things ‘in progress’
- Most procedures wont be documented

References

- Podcasts
  - RiskyBiz, SANS StormCenter, SANS Blue Team
- Newsletters / websites
  - ACSC, KrebsOnSecurity, CISA, SANS
- Industry Reports
  - ACSC, OAIC, Red Canary Threat Detection Report 2024

Conclusion

- Learn as much as you can
- You will make mistakes, learn and move on
- Build trust with your team
- If you're not growing, it's time to move on

Discussion