



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

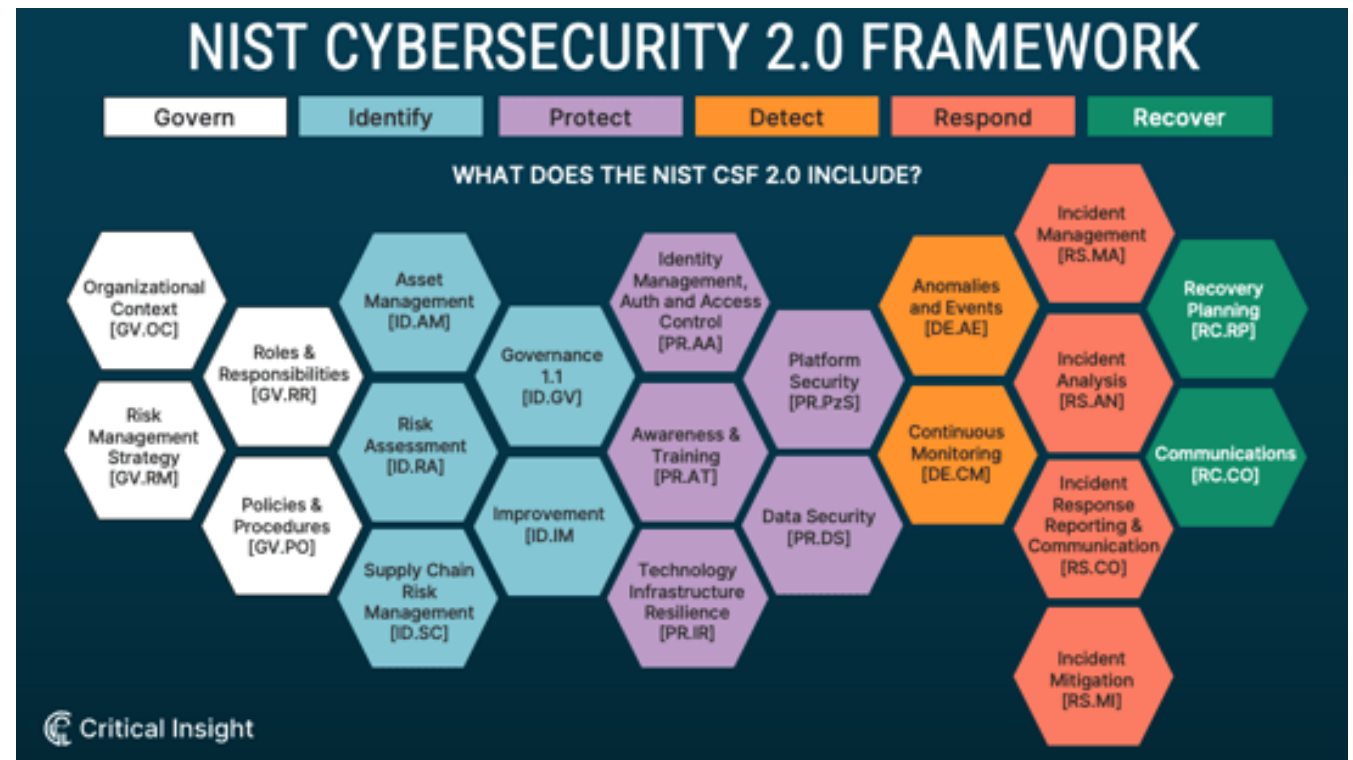
Technical

- ▶ 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

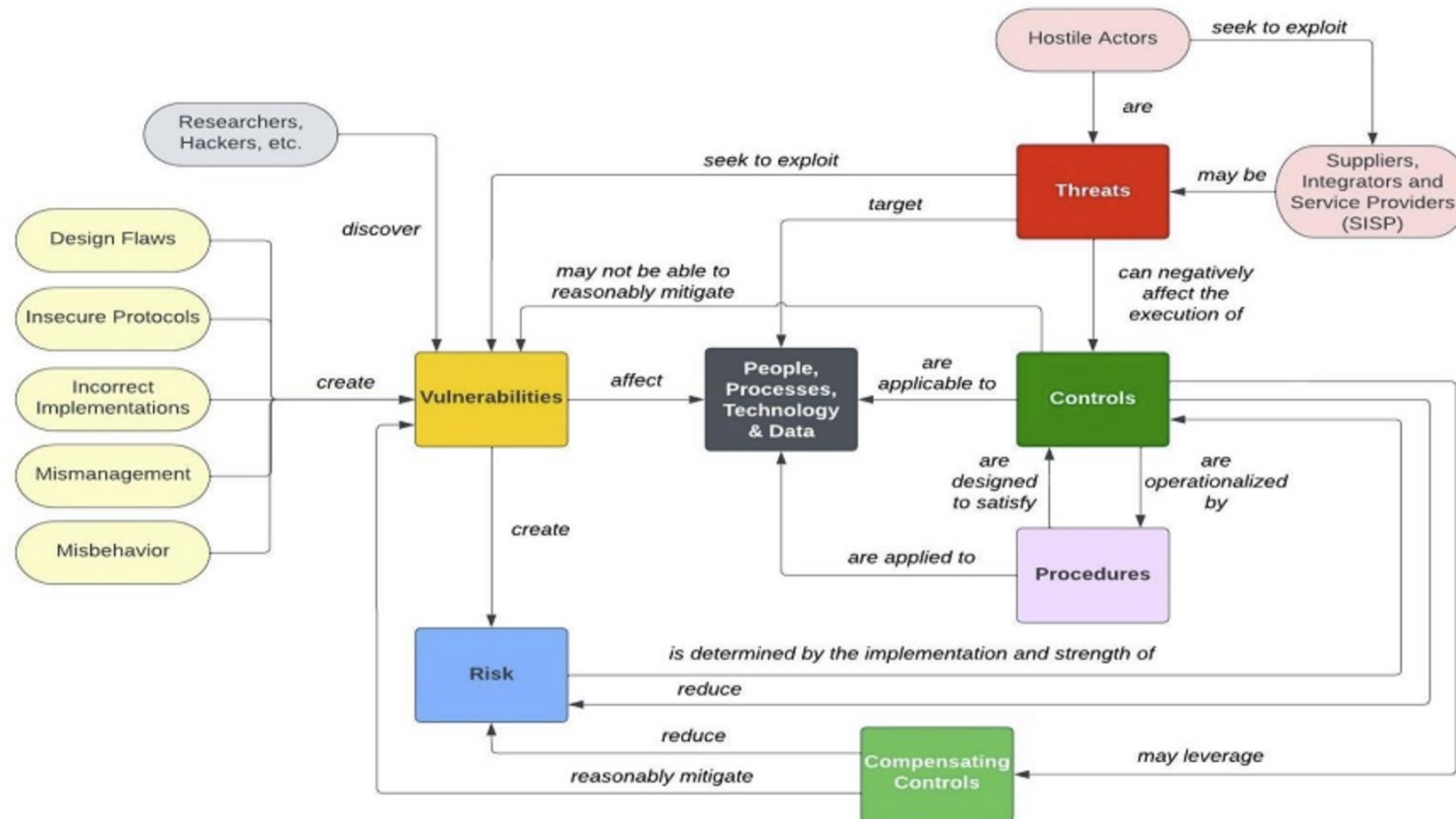
Best practice frameworks

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

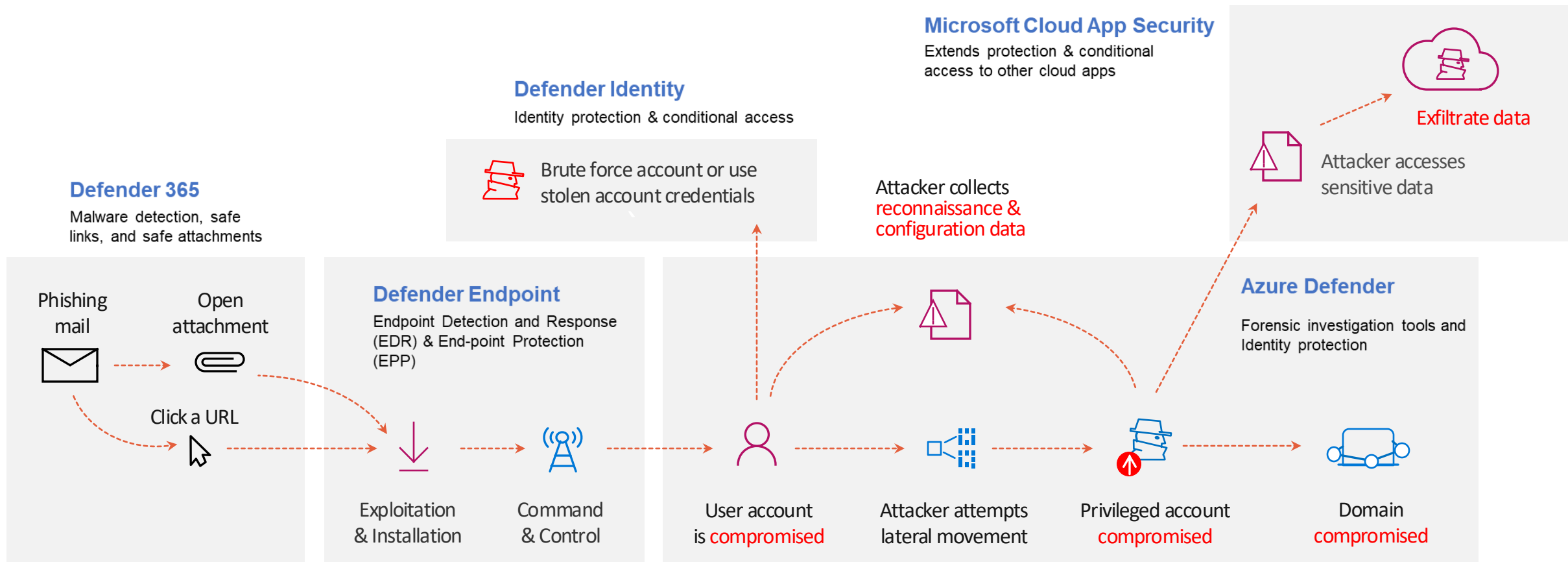


https://cybersecurity.criticalinsight.com/nist_csf_2.0

Risk, Threat, Controls Fundamentals



Kill Chain



MITRE ATT&CK

► Adversary tactics, techniques and procedures

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 16 techniques	Discovery 30 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (1,3)	Acquire Infrastructure (2,8)	Drive-by Compromise	Command and Scripting Interpreter (2,8)	Account Manipulation (2,5)	Abuse Elevation Control Mechanism (1,4)	Abuse Elevation Control Mechanism (1,4)	Adversary-in-the-Middle (2,3)	Account Discovery (2,4)	Exploitation of Remote Services	Adversary-in-the-Middle (2,3)	Application Layer Protocol (1,4)	Automated Exfiltration (2,7)	Account Access Removal
Gather Victim Host Information (2,4)	Compromise Accounts (1,2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (2,5)	Access Token Manipulation (2,5)	Brute Force (1,4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (1,3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (1,2)	Compromise Infrastructure (1,8)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (2,14)	Boot or Logon Autostart Execution (2,14)	Boot or Logon Autostart Execution (2,14)	Credentials from Password Stores (2,6)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding (2,3)	Exfiltration Over Alternative Protocol (1,3)	Data Encrypted for Impact
Gather Victim Network Information (2,8)	Develop Capabilities	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (2,5)	Boot or Logon Initialization Scripts (2,5)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2,2)	Automated Collection	Data Obfuscation (2,3)	Exfiltration Over C2 Channel	Data Manipulation (2,3)
Gather Victim Org Information (2,4)	Establish Accounts (2,12)	Phishing (2,3)	Inter-Process Communication (2,3)	Browser Extensions	Boot or Logon Initialization Scripts (2,5)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (2,4)	Browser Session Hijacking	Clipboard Data	Exfiltration Over Other Network Medium (2,3)	Defacement (2,3)
Phishing for Information (2,3)	Obtain Capabilities	Replication Through Removable Media	Native API	Compromise Client Software Binary	Create or Modify System Process (2,14)	Deobfuscate/Decode Files or Information	Input Capture (2,5)	Cloud Storage Discovery	Replication Through Removable Media	Clipboard Data	Data from Cloud Storage Object	Exfiltration Over Physical Medium (2,3)	End User (2,3)
Search Closed Sources (2,2)	Stage Capabilities (2,5)	Supply Chain Compromise (1,3)	Scheduled Task/Job (1,8)	Create Account (1,3)	Domain Policy Modification (1,2)	Deploy Container	Forge Web Credentials (2,2)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Configuration Repository (2,2)	Data from Configuration Repository (2,2)	Exfiltration Over Web Service (2,2)	Independent Denial of Service (2,4)
Search Open Technical Databases (2,3)		Trusted Relationship	Shared Modules	Create or Modify System Process (2,14)	Event Triggered Execution (2,14)	Direct Volume Access	Input Capture (2,5)	Container and Resource Discovery	Taint Shared Content	Data from Local System	Fallback Channels	Scheduled Transfer	Network Denial of Service (2,2)
Search Open Websites/Domains (2,3)		Valid Accounts (2,4)	Software Deployment Tools	Event Triggered Execution (2,14)	Exploitation for Privilege Escalation	Domain Policy Modification (1,2)	Multi-Factor Authentication Interception (2,5)	Debugger Evasion	Use Alternate Authentication Material (2,4)	Data from Network Shared Drive	Ingress Tool Transfer	Transfer Data to Cloud Account	Resource Hijacking
Search Victim-Owned Websites			System Services	External Remote Services	Hijack Execution Flow (2,12)	Execution Guardrails (2,1)	Multi-Factor Authentication Request Generation	Domain Trust Discovery		Data from Removable Media	Multi-Stage Channels		Service Stop
			User Execution (2,3)	Windows Management Instrumentation	Process Injection (2,12)	Exploitation for Defense Evasion	Network Sniffing	File and Directory Discovery		Proxy (2,4)	Non-Application Layer Protocol		System Shutdown/Reboot
					Scheduled Task/Job (1,8)	Hide Artifacts (2,12)	OS Credential Dumping (1,8)	Group Policy Discovery			Non-Standard Port		
					Valid Accounts (2,4)	Hijack Execution Flow (2,12)	Steal Application Access Token	Network Service Discovery			Protocol Tunneling		
						Impair Defenses (2,8)	Steal or Forge Kerberos Tickets (1,4)	Network Sniffing			Remote Access Software		
						Indicator Removal on Host (2,8)	Steal Web Session Cookie	Password Policy Discovery			Traffic Signaling (2,1)		
						Indirect Command Execution	Unsecured Credentials (1,7)	Peripheral Device Discovery			Web Service (1,3)		
						Massware (2,2)		Permission Groups Discovery (2,3)					
						Modify Authentication Process (2,5)		Process Discovery (2,3)					
						Modify Cloud Compute Infrastructure		Query Registry					
						Modify System Image (2,2)		Remote System Discovery (2,4)					
						Network Boundary Bridging (2,1)		System Information Discovery (2,3)					
						Obfuscated Files or Information (2,8)		System Location Discovery (2,1)					
						Plist File Modification		System Network Configuration Discovery (1,7)					
						Pre-OS Boot (2,3)		System Network Connections Discovery					
						Process Injection (2,12)		System Owner/User Discovery					

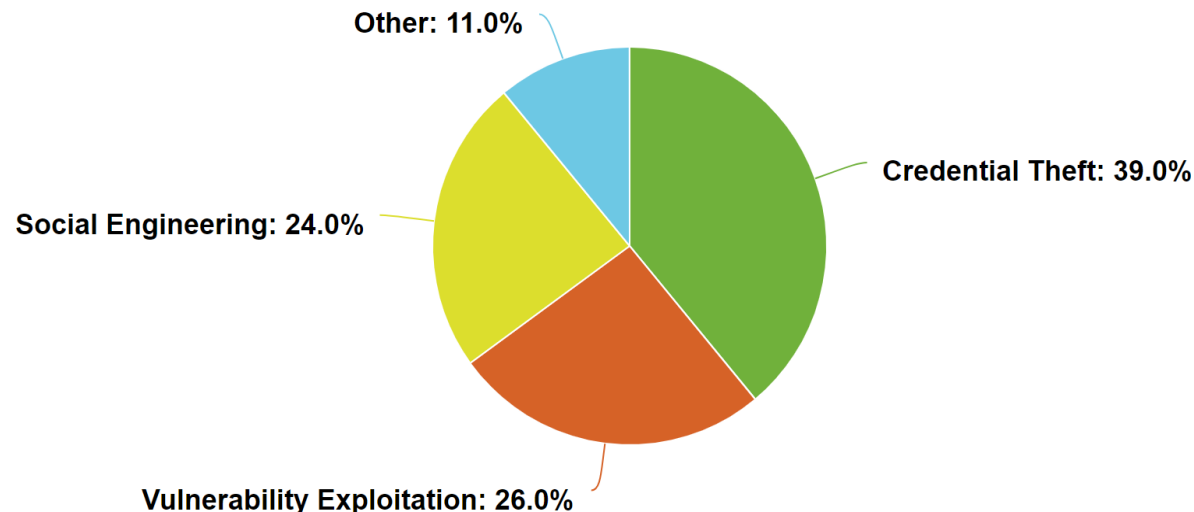
<https://mitre-attack.github.io/attack-navigator/>
APT29 overlay

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

THE TRUST EQUATION

$$\text{TRUST} = \frac{\text{CREDIBILITY} + \text{RELIABILITY} + \text{INTIMACY}}{\text{SELF-ORIENTATION}}$$

Credibility (Words) – *I can trust what he says about...*

Reliability (Actions) – *I can trust her to...*

Intimacy (Emotions) – *I feel comfortable discussing this...*

Self-orientation (Motives) – *Who does the advisor care about?*

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