



# An MSSP's Guide to ATT&CK

Scott McKean – Chief Security Officer – Interactive



Scott McKean

Chief Security Officer - Interactive

✉ smckean@interactive.com.au

🐦 @cyb3rsqu1ddy

🌐 <https://www.linkedin.com/in/scott-mckean-cyber/>

# Agenda

- The problem
- So what?
- Utilising ATT&CK
- What does the customer see?
- Kaizen (Continuous improvement)
- The result
- How do I start?

## The problem

- MSSP's have done a poor job helping customers understand:
  - Their current risk profile / business context
  - How they should start addressing these risks
  - How to measure the effectiveness of their security program

## So what?

- Customers see Cyber Security as a 'Black Box'
- Making it hard for MSSP's to demonstrate value
- Organisations believe "That won't happen to us!" so it lacks focus

## Utilising ATT&CK

- Focus our efforts on what 'matters most' to our customers
- Validating data – increasing confidence of detections
- Demystifying 24x7 Security Operations

**What does the customer see?**

Customers don't need it dumbed down – they need context.

Threats common in their industry

APT Groups and 'modus operandi'

TTP's used by APT's

Digitisation and automation have resulted in consumers moving away from traditional banking, finance and mortgage institutions in search of quicker, easier and more user-centric alternatives. This disruption of traditional processes has resulted in increased interconnectedness and sharing of borrower data. Ease of access and sharing has dramatically improved the process but brings with it significant threats and opportunities for exploitation; companies in the online mortgage industry are therefore a highly attractive target.

Potential security issues include identify theft, loss and leakage of private data and sensitive information; fraud; theft of funds; theft of intellectual property; sabotage; disruption of business; and damage to brand and reputation. Traditionally, cyber-attacks have been network-centric however the exponential increase in the aggregation of personal information digitally means organised cyber criminals – the number one threat to the industry – are now focused on customers, their credentials, the applications they access and the sensitive personal data stored within them. Popular attack methods include phishing-based account compromise leading to wire / bank transfer fraud, ransomware and vulnerability exploits to exfiltrate data. Recent examples include:

- Distributed-denial-of-service attack - Ellie Mae, 2018. Client information ultimately not breached but attack specifically targeted the mortgage industry. US credit monitoring firm Equifax - sensitive financial details of 150 million Americans stolen. Company reputation further damaged by response - a standalone website established for victims targeted by hackers, and company's official Twitter account shared a fake link four times before the mistake was identified.

- Equifax remains engaged in a determined effort to restore its reputation, but the community's trust – a crucial commodity for financial institutions – will take time to fully restored. In mid-2017, the US consumer credit reporting agency, Equifax, suffered a cyberattack that resulted in the leakage of personal information, including social security numbers, belonging to more than 145 million users.

- Wire transfer fraud - Californian escrow firm fell victim to a series of fraudulent wire transfers totalling \$1.1 million. Led to bankruptcy.

Insider threats are a significant security concern - insiders have access and ability to cause substantial harm and often go unnoticed for lengthy periods. Insider threats an increasing trend - disaffected individuals with access to confidential and sensitive data leaking information and/or assisting with the commission of cyber-attacks. Examples include:

- In 2018 a Westpac manager provided banking passwords of 80 customer accounts to a mortgage broker, allowing direct access to personal bank accounts in a serious breach of customer privacy.

- January 2013, a NAB employee entered a Facebook dispute with an individual regarding the shooting death of children in Sandy Hook in the US in December 2012. The employee then set up a fake Facebook persona and revealed the address of the owner of the online posts, according to the bank's correspondence with the privacy commissioner.

Hacktivists represent a lesser concern but they can still disrupt services by disrupting key government processes while simultaneously drawing attention to their issues. Targets often selected based on ease of hacking and/or the potential attention the hack or defacement will receive. Hacktivists often use known and relatively unsophisticated vulnerabilities and techniques including website defacement, organised Distributed Denial of Service (DDoS) attacks and, increasingly, the seizure and public disclosure of information from target systems. Examples include:

Advanced Persistent Threat (APT) represent the peak technical threat to the sector and aim to collect intelligence capable of providing their sponsoring government with insight into the target's operations, finances and sensitive personal information. APTs inherently difficult to detect and driven by geo-political situations and events. MITRE lists many sophisticated groups with a banking and finance target including: APT 19 & 38, RTM, Silence, Carbanate, Cobalt, GCMAN and Lazarus. Collectively these groups are known to use at least 90 different tactics under the ATT&CK model (listed on last sheet).

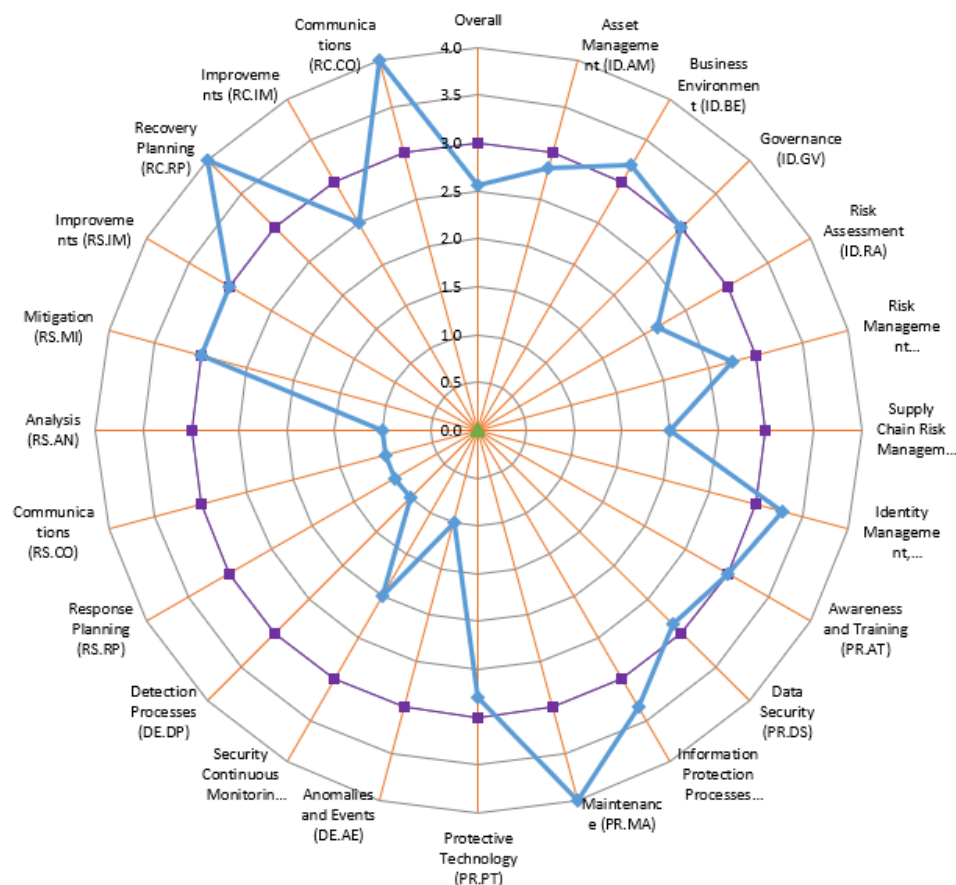


# NIST Cyber Security Framework Maturity

	NIST 2018 CSF Categories	Target Score	Policy Score	Practice Score
	<b>Overall</b>	<b>3.00</b>	<b>2.55</b>	<b>0.00</b>
IDENTITY (ID)	Asset Management (ID.AM)	3.00	2.83	0.00
	Business Environment (ID.BE)	3.00	3.20	0.00
	Governance (ID.GV)	3.00	3.00	0.00
	Risk Assessment (ID.RA)	3.00	2.17	0.00
	Risk Management Strategy (ID.RM)	3.00	2.75	0.00
	Supply Chain Risk Management (ID.SC)	3.00	2.00	0.00
PROTECT (PR)	Identity Management, Authentication and Access Control (PR.ID)	3.00	3.29	0.00
	Awareness and Training (PR.AT)	3.00	3.00	0.00
	Data Security (PR.DS)	3.00	2.88	0.00
	Information Protection Processes and Procedures (PR.IP)	3.00	3.33	0.00
	Maintenance (PR.MA)	3.00	4.00	0.00
	Protective Technology (PR.PT)	3.00	2.80	0.00
DETECT (DE)	Anomalies and Events (DE.AE)	3.00	1.00	0.00
	Security Continuous Monitoring (DE.CM)	3.00	2.00	0.00
	Detection Processes (DE.DP)	3.00	1.00	0.00
RESPOND (RS)	Response Planning (RS.RP)	3.00	1.00	0.00
	Communications (RS.CO)	3.00	1.00	0.00
	Analysis (RS.AN)	3.00	1.00	0.00
	Mitigation (RS.MI)	3.00	3.00	0.00
	Improvements (RS.IM)	3.00	3.00	0.00
RECOVER (RC)	Recovery Planning (RC.RP)	3.00	4.00	0.00
	Improvements (RC.IM)	3.00	2.50	0.00
	Communications (RC.CO)	3.00	4.00	0.00


## NIST Cyber Security Framework Maturity Levels

- 5 - Optimal
- 4 - Managed
- 3 - Defined
- 2 - Acknowledged
- 1 - Initial
- 0 - Non-existent



— Target Score  
— Policy Score

# Develop a Risk Register

 Risk Register											Risk Appetite	
Risk ID	Risk Name	Category	Description	Pre Control Rating			Controls	Post Control Rating			Risk Tolerance (Board or Client Decision)	Alignment
				Likelihood	Consequences	Risk Rating		Likelihood	Consequences	Risk Rating		
R1	A lack of user security awareness	Security	No formal security awareness trg could lead to staff failing to identify threats, and fails to keep security a part of decision making.	Likely	Serious	High	C1. Security awareness program (online and live realistic training) C2. Learning Management Solution C3. Security reporting mechanism C4. Testing C5. Security bulletins C6. Mimecast	Unlikely	Serious	Medium	Medium	Aligned
R2	Weak cipher used to secure environment leads to breach	Security	TLS cypher relatively easy to break	Possible	Severe	High	C7. Pen Testing of site and LB C8. Audits C9. Encryption Policy / Standards C10. Vulnerability scanning C11. Netflow (unencrypted traffic alerts)	Remote	Severe	Medium	Medium	Aligned
R3	Data leakage via email, USB, local storage	Security	Sensitive leaks via USB, email, cloud or local storage	Likely	Severe	High	C1. Security awareness program (online and live realistic training) C9. Encryption policy C12. DLP C13. Device level encryption C14. USB whitelisting C15. CASB C16. Acceptable Use Policy C17. Information classification policy	Possible	Catastrophic	High	Medium	Not Aligned

**Now for ATT&CK**

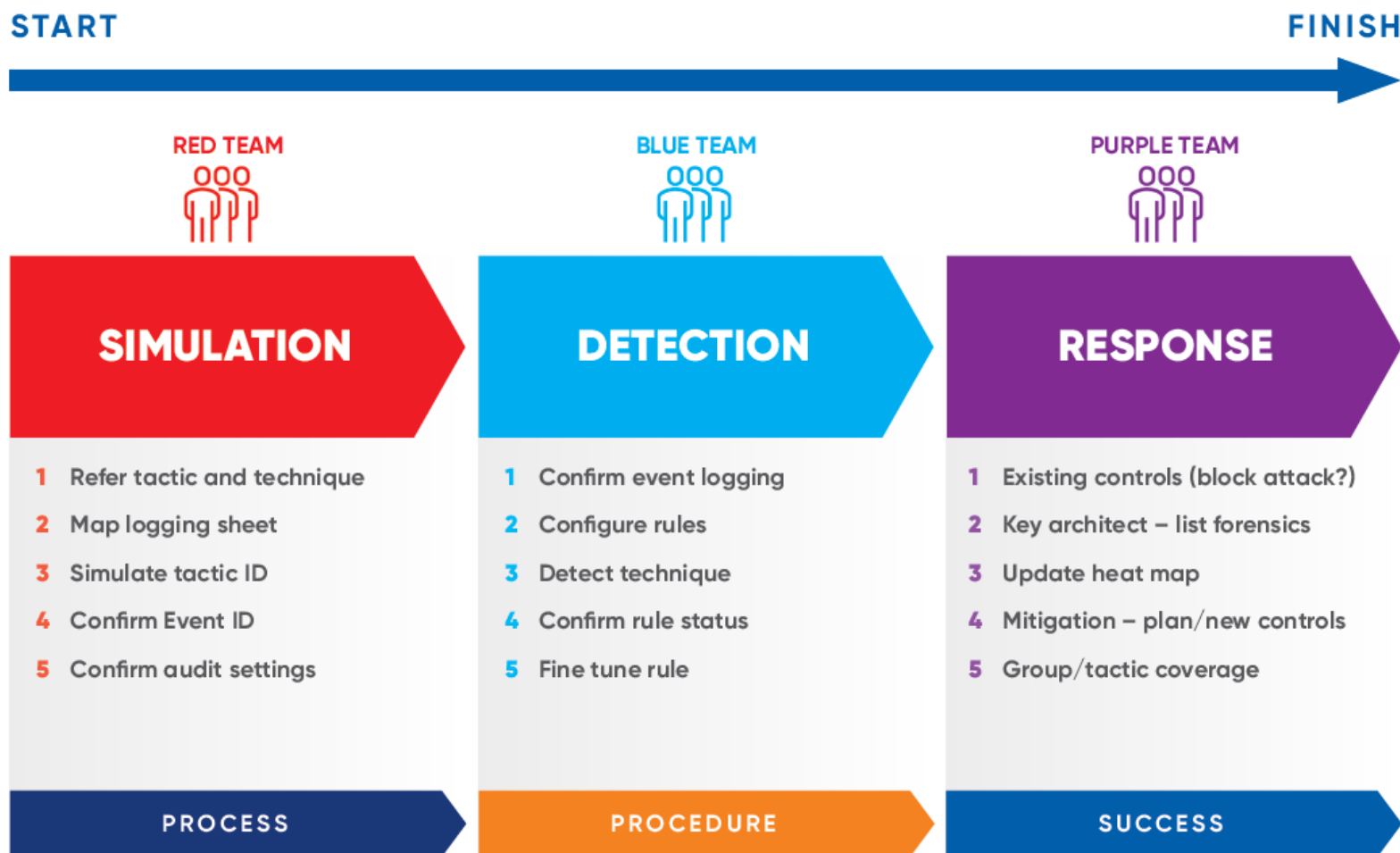
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 Items	34 Items	62 Items	32 Items	69 Items	21 Items	23 Items	18 Items	13 Items	22 Items	9 Items	16 Items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	Appinit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	Appinit DLLs	Application Shimming	Clear Command History	Credentials from Web Browsers	File and Directory Discovery	Internal Spearphishing	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	Code Signing	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Spearphishing via Service	Execution through API	BITS Jobs	Dylib Hijacking	Compile After Delivery	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Supply Chain Compromise	Execution through Module Load	Bootkit	Elevated Execution with Prompt	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery
Trusted Relationship	Exploitation for Client Execution	Browser Extensions	Emond	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Input Capture	Fallback Channels		Network Denial of Service
Valid Accounts	Graphical User Interface	Change Default File Association	Exploitation for Privilege Escalation	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services	Man in the Browser	Multi-hop Proxy		Resource Hijacking
	InstallUtil	Component Firmware	Extra Window Memory Injection	Connection Proxy	Input Prompt	Process Discovery	Replication Through Removable Media	Screen Capture	Multi-Stage Channels		Runtime Data Manipulation
	Launchctl	Component Object Model Hijacking	File System Permissions Weakness	Control Panel Items	Kerberoasting	Query Registry	Shared Webroot	Video Capture	Multiband Communication		Service Stop
	Local Job Scheduling	Create Account	Hooking	DCShadow	Keychain	Remote System Discovery	SSH Hijacking		Multilayer Encryption		Stored Data Manipulation
	LSASS Driver	DLL Search Order Hijacking	Image File Execution Options Injection	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Security Software Discovery	Taint Shared Content		Port Knocking		System Shutdown/Reboot
	Mshst	Dylib Hijacking	Launch Daemon	Disabling Security Tools	Network Sniffing	Software Discovery	Third-party Software		Remote Access Tools		Transmitted Data Manipulation
	PowerShell	Emond	New Service	DLL Search Order Hijacking	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote File Copy		
	Regsvcs/Regasm	External Remote Services	Parent PID Spoofing	DLL Side-Loading	Private Keys	System Network Configuration Discovery	Windows Remote Management		Standard Application Layer Protocol		
	File System Permissions Weakness	Path Interception	Execution Guardrails	Securid Memory	SecurityID Memory	System Network Connections Discovery			Standard Cryptographic Protocol		
	Regsvr32	Hidden Files and Directories	Plist Modification	Exploitation for Defense Evasion	Steal Web Session Cookie	System Owner/User Discovery			Standard Non-Application Layer Protocol		
	Rundll32	Hooking	Port Monitors	Extra Window Memory Injection	Two-Factor Authentication Interception	System Service Discovery			Uncommonly Used Port		
	Scheduled Task	Hypervisor	PowerShell Profile	File and Directory Permissions Modification		System Time Discovery			Web Service		
	Scripting	Image File Execution Options Injection	Process Injection	File Deletion		Virtualization/Sandbox Evasion					
	Service Execution	Kernel Modules and Extensions	Scheduled Task	File System Logical Offsets							
	Signed Binary Proxy Execution	Launch Agent	Service Registry Permissions Weakness	Gatekeeper Bypass							
	Signed Script Proxy Execution	Launch Daemon	Setuid and Setgid	Group Policy Modification							
	Source	Launchctl	SID-History Injection	Hidden Files and Directories							
	Space after Filename	LC_LOAD_DYLIB Addition	Startup Items	Hidden Users							
	Third-party Software	Local Job Scheduling	Sudo	Hidden Window							
	Trap	Login Item	Sudo Caching	HISTCONTROL							
	Trusted Developer Utilities	Logon Scripts	Valid Accounts	Image File Execution Options Injection							
	User Execution	LSASS Driver	Web Shell	Indicator Blocking							
	Windows Management Instrumentation	Modify Existing Service	Indicator Removal from Tools	Indicator Removal on Host							
	Windows Remote Management	Netsh Helper DLL	Indirect Command Execution	Install Root Certificate							
	XSL Script Processing	New Service	Install Root Certificate	InstallUtil							
		Office Application Startup	InstallUtil	Launchctl							
		Path Interception	Launchctl	LC_MAIN Hijacking							
		Plist Modification	Port Knocking	Masquerading							
		Port Knocking	PowerShell Profile	Modify Registry							
		Port Monitors	Rccommon	Mshst							
		PowerShell Profile	Re-opened Applications	Network Share Connection Removal							
		Rccommon	Redundant Access	NTFS File Attributes							
		Registry Run Keys / Startup Folder	Obfuscated Files or Information	Parent PID Spoofing							
		Scheduled Task	Plist Modification	Port Knocking							
		Screensaver	Process Doppelganging	Process Hollowing							
		Security Support Provider	Process Injection	Redundant Access							
		Server Software Component	Regsvcs/Regasm	Rundll32							
		Service Registry Permissions Weakness	Rootkit	Scripting							
		Setuid and Setgid	Rootkit								
		Shortcut Modification	Rundll32								
		SIP and Trust Provider Hijacking	Scripting								
		Startup Items									
		System Firmware									
		Systemd Service									
		Time Providers									

Techniques common for this customer's context

APT19

This is the beginning of our Heatmap

# Kaizen - Improving detection capability utilising ATT&CK

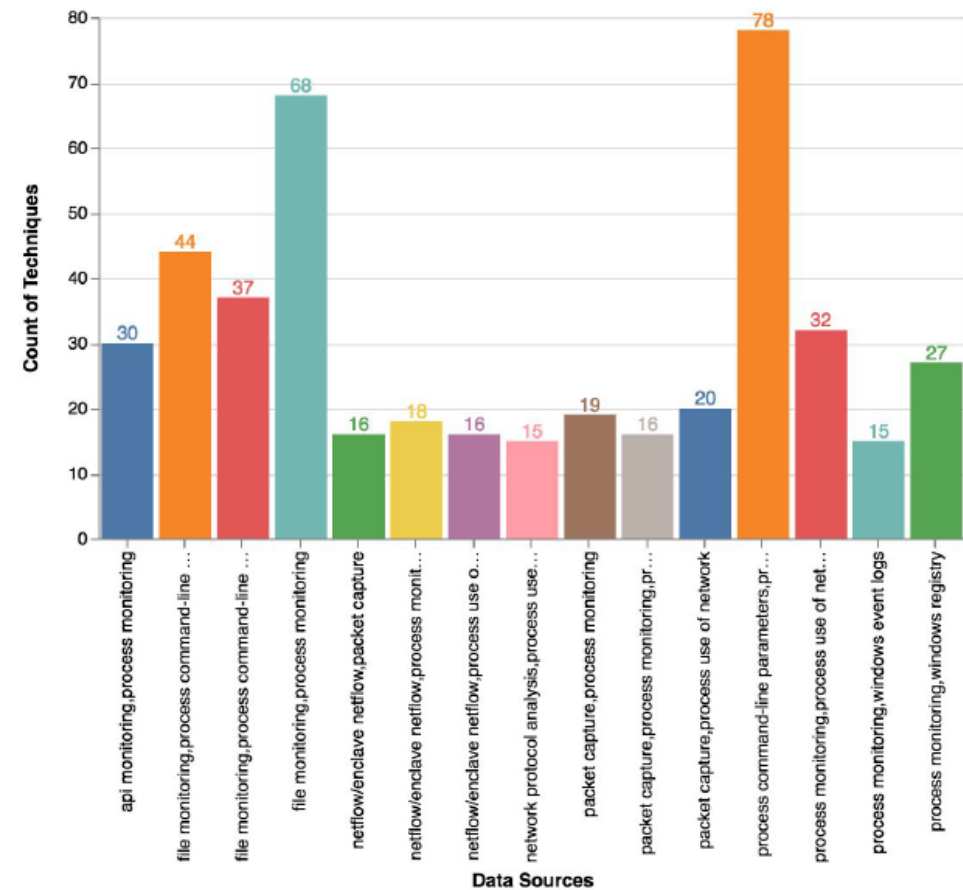


# Mapping data sources to Event Logs

Data Source ▼	Sub - Data Source ⇅	Data Object ⇅	Relationship ⇅	Data Object ⇅	Event ID ⇅
File monitoring	file access request	user	requested_a_handle	file	4656
File monitoring	file deletion request	user	requested_a_handle	file	4656
File monitoring	file access	user	accessed	file	4663
File monitoring	file deletion	user	deleted	file	4663
File monitoring	file permissions change	user	changed_permissions	file	4670
Process monitoring	process creation	process	created	process	4688
Process monitoring	process creation	process	created	process	1
Process monitoring	process termination	process	terminated	process	4689
Process monitoring	process termination	process	terminated		5
Process monitoring	process write to process	process	wrote_to	process	8
Process monitoring	process access	process	opened	process	10
Windows event logs	kerberos TGT request	user	requested	ticket granting ticket	4768
Windows event logs	kerberos service ticket request	user	requested	service ticket	4769
Windows event logs	kerberos service ticket renewal	user	renewed	service ticket	4770
Windows event logs	kerberos service ticket failure	user	requested	service ticket	4773
Windows event logs	user rdp session	user	disconnected_from	host	4779

# Prioritise based on Top15 + Customers context

subsets_name	subsets_count
process command-line parameters,process monitoring	78
file monitoring,process monitoring	68
file monitoring,process command-line parameters	44
file monitoring,process command-line parameters,process monitoring	37
process monitoring,process use of network	32
api monitoring,process monitoring	30
process monitoring,windows registry	27
packet capture,process use of network	20
packet capture,process monitoring	19
netflow/enclave netflow,process monitoring	18
packet capture,process monitoring,process use of network	16
netflow/enclave netflow,packet capture	16
netflow/enclave netflow,process use of network	16
process monitoring,windows event logs	15
network protocol analysis,process use of network	15





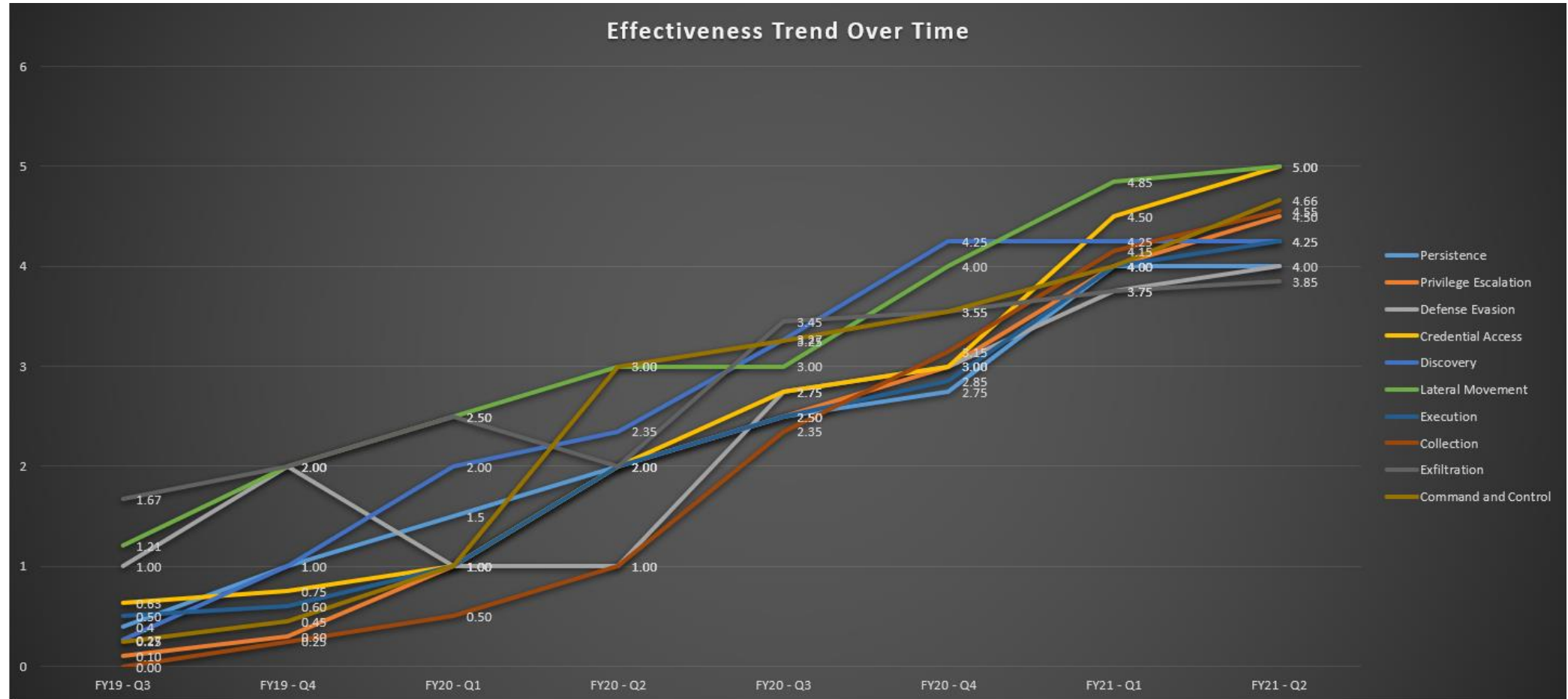
# Focus on what is important

## Customer specific Heatmap

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Application Shimming	Automated Collection	Data Compressed	Communication Through Removable Media
Applint DLLs	Applint DLLs	Bypass User Account Control	Brute Force	File and Directory Discovery	Exploitation of Vulnerability	Command-Line Interface	Clipboard Data	Data Encrypted	Connection Proxy
Application Shimming	Application Shimming	Clear Command History	Create Account	Network Service Scanning	Logon Scripts	Execution through API	Data from Local System	Data Transfer Size Limits	Custom Command and Control Protocol
Authentication Package	Bypass User Account Control	Code Signing	Credential Dumping	Network Share Discovery	Pass the Hash	Execution through Module Load	Data from Network Shared Drive	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Bootkit	DLL Injection	Component Firmware	Credentials in Files	Peripheral Device Discovery	Pass the Ticket	Graphical User Interface	Data from Removable Media	Exfiltration Over Command and Control Channel	Data Encoding
Change Default File Association	DLL Search Order Hijacking	Component Object Model Hijacking	Exploitation of Vulnerability	Permission Groups Discovery	Remote Desktop Protocol	InstallUtil	Data Staged	Exfiltration Over Other Network Medium	Data Obfuscation
Component Firmware	Dylib Hijacking	Deobfuscate/Decode Files or Information	Input Capture	Process Discovery	Remote File Copy	Launchctl	Email Collection	Exfiltration Over Physical Medium	Fallback Channels
Component Object Model Hijacking	Exploitation of Vulnerability	Disabling Security Tools	Input Prompt	Query Registry	Remote Services	PowerShell	Input Capture	Scheduled Transfer	Multiband Communication
Cron Job	File System Permissions Weakness	DLL Injection	Keychain	Remote System Discovery	Replication Through Removable Media	Process Hollowing	Screen Capture		Multilayer Encryption
DLL Search Order Hijacking	Launch Daemon	DLL Search Order Hijacking	Network Sniffing	Security Software Discovery	Shared Webroot	Regsvcs/Regasm	Video Capture		Multi-Stage Channels
Dylib Hijacking	Local Port Monitor	DLL Side-Loading	Private Keys	System Information Discovery	Taint Shared Content	Regsvr32			Remote File Copy
External Remote Services	New Service	Exploitation of Vulnerability	Securityd Memory	System Network Configuration Discovery	Third-party Software	Rundll32			Standard Application Layer Protocol
File System Permissions Weakness	Path Interception	File Deletion	Two-Factor Authentication Interception	System Network Connections Discovery	Windows Admin Shares	Scheduled Task			Standard Cryptographic Protocol
Hidden Files and Directories	Plist Modification	File System Logical Offsets		System Owner/User Discovery	Windows Remote Management	Scripting			Standard Non-Application Layer Protocol
Hypervisor	Scheduled Task	Gatekeeper Bypass		System Service Discovery		Service Execution			Uncommonly Used Port
Launch Agent	Service Registry Permissions Weakness	Hidden Files and Directories		System Time Discovery		Source			Web Service
Launch Daemon	Setuid and Setgid	Hidden Users				Space after Filename			
Launchctl	Startup Items	Hidden Window				Third-party Software			
LC_LOAD_DYLIB Addition	Sudo	HISTCONTROL				Trap			
Local Port Monitor	Valid Accounts	Indicator Blocking				Trusted Developer Utilities			
Login Item	Web Shell	Indicator Removal from Tools				Windows Management Instrumentation			
Logon Scripts		Indicator Removal on Host				Windows Remote Management			
Modify Existing Service		Install Root Certificate							
Netsh Helper DLL		InstallUtil							
New Service		Launchctl							
Office Application Startup		LC_MAIN Hijacking							
Path Interception		Masquerading							
Plist Modification		Modify Registry							
Re.common		Network Share Connection Removal							
Redundant Access		NTFS Extended Attributes							
Registry Run Keys / Start Folder		Obfuscated Files or Information							
Re-opened Applications		Plist Modification							
Scheduled Task		Process Hollowing							
Security Support Provider		Redundant Access							
Service Registry Permissions Weakness		Regsvcs/Regasm							
Shortcut Modification		Regsvr32							
Startup Items		Rootkit							
System Firmware		Rundll32							
Trap		Scripting							
Valid Accounts		Software Packing							
Web Shell		Space after Filename							
Windows Management Instrumentation Event Subscription		Timestamp							
Winlogon Helper DLL		Trusted Developer Utilities							
		Valid Accounts							



# Track progress over time



## The result

- We can prove we will deliver exactly what we say we will deliver  
'No smoke and mirrors'
- Our customers can understand how we prioritise effort
- Our customers can hold us to account
- Our customers are engaged and invested in the process

## How do you start?

- Have a process to understand the quality of your customers data
- Help your customer understand how to increase the effectiveness with ATT&CK
- Help your analyst's understand the value that you are delivering
- Develop a process to engage your customer on what is important to THEM!

# The future

- No longer a 'Black Box'
- Demonstrable value
- Build confidence and trust

Thank you – The shoulders of the giants we've stood on.

- @Cyb3rWard0g
- @olafhartong
- @Neo23x0
- @darkoperator
- And many more....



Scott McKean

Chief Security Officer - Interactive

✉ smckean@interactive.com.au

🐦 @cyb3rsqu1ddy

🌐 <https://www.linkedin.com/in/scott-mckean-cyber/>