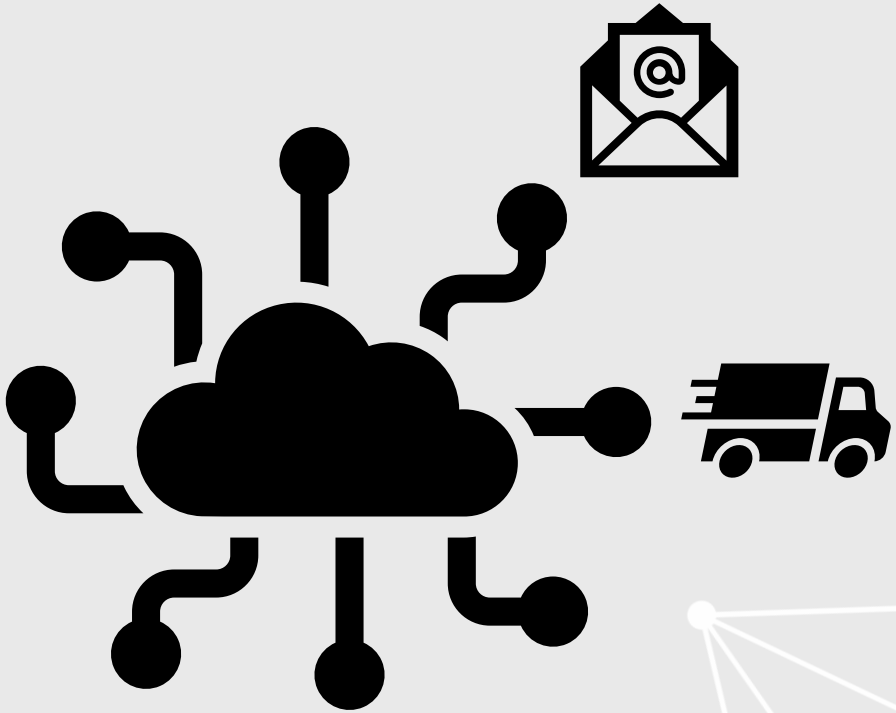
CyberPro

“Bringing World class Managed I.T. and Cyber Security to Australian Businesses” - Ian Ward, Founder & CEO

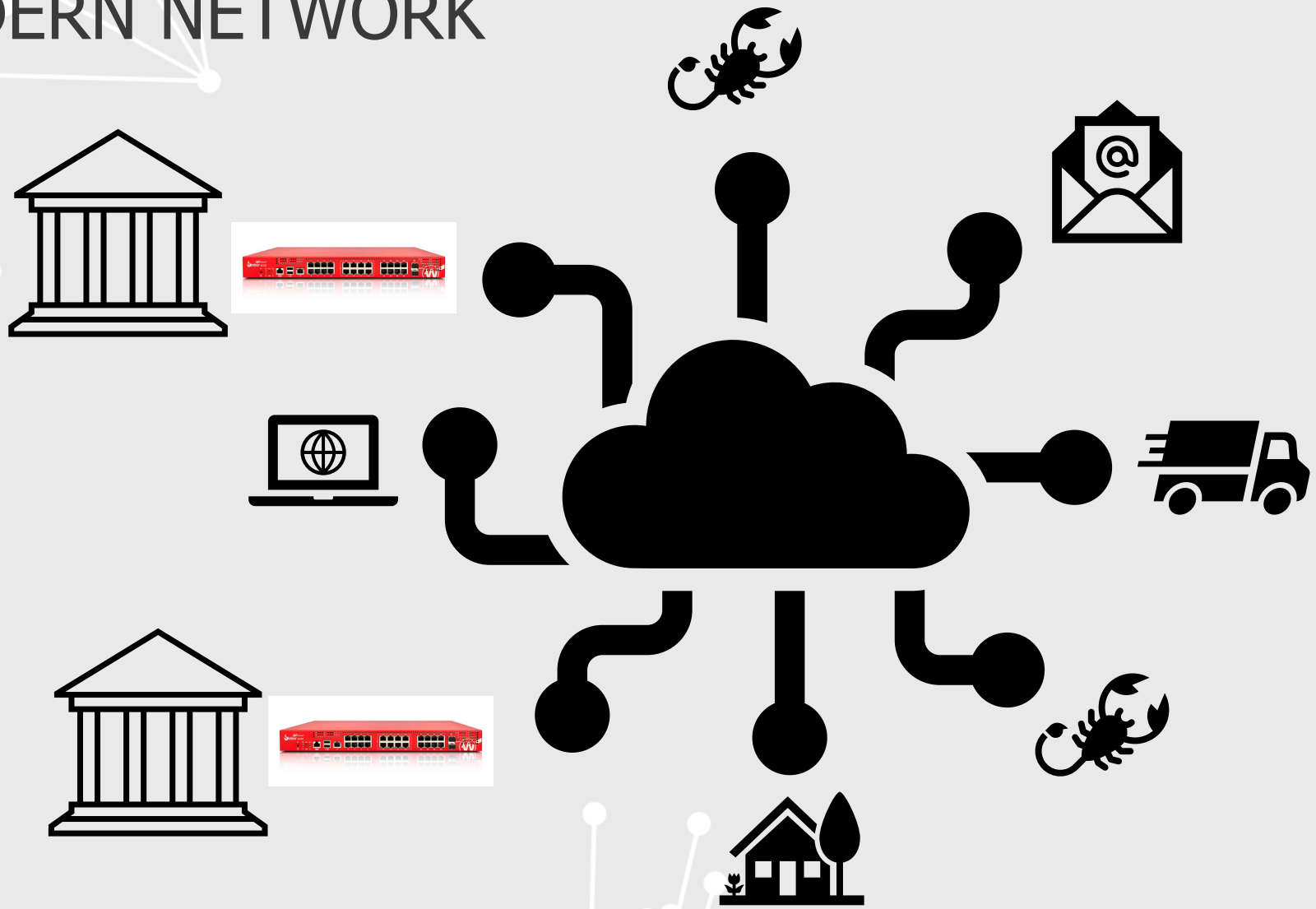
AGENDA

- How Corporate Networks have changed – The Attack Surface
- Sophistication Level of todays Hackers
- The always evolving “Security Stack”
- A typical hack timeline
- Mitigation Strategies
- Evolution of advanced techniques such as “XDR”

TRADITIONAL NETWORK



MODERN NETWORK



HACKER TYPES - COMMON

Maturity Level 1

- Opportunistically using a publicly available exploit
- Any victim rather than a specific victim
- Seeking common weaknesses in many Targets
- Concentrates on the User rather than the entire Enterprise

Maturity Level 2

- Uses social engineering, phishing, weak passwords
- Conservative with Time, Money and Effort to get a result

Mitigation Strategies to Prevent Malware Delivery and Execution:

Essential	**Application control** to prevent execution of unapproved/malicious programs including .exe, DLL, scripts (e.g. W
Essential	**Patch applications** (e.g. Flash, web browsers, Microsoft Office, Java and PDF viewers). Patch/mitigate computer
Essential	**Configure Microsoft Office macro settings** to block macros from the internet, and only allow vetted macros eith
Essential	**User application hardening**. Configure web browsers to block Flash (ideally uninstall it), ads and Java on the int
Excellent	**Automated dynamic analysis of email and web content run in a sandbox**, blocked if suspicious behaviour is ide
Excellent	**Email content filtering**. Allow only approved attachment types (including in archives and nested archives). Anal
Excellent	**Web content filtering**. Allow only approved types of web content and websites with good reputation ratings. Bl
Excellent	**Deny corporate computers direct internet connectivity**. Use a gateway firewall to require use of a split DNS ser
Excellent	**Operating system generic exploit mitigation** e.g. Data Execution Prevention (DEP), Address Space Layout Rando
Very Good	**Server application hardening** especially internet-accessible web applications (sanitise input and use TLS not SSL
Very Good	**Operating system hardening** (including for network devices) based on a Standard Operating Environment, disab
Very Good	**Antivirus software using heuristics and reputation ratings** to check a file's prevalence and digital signature pric
Very Good	**Control removable storage media and connected devices**. Block unapproved CD/DVD/USB storage media. Bloc
Very Good	**Block spoofed emails**. Use Sender Policy Framework (SPF) or Sender ID to check incoming emails. Use 'hard fail'
Good	**User education**. Avoid phishing emails (e.g. with links to login to fake websites), weak passphrases, passphrase
Limited	**Antivirus software with up-to-date signatures** to identify malware, from a vendor that rapidly adds signatures
Limited	**TLS encryption between email servers** to help prevent legitimate emails being intercepted and subsequently le

Mitigation Strategies to Prevent Malware Delivery and Execution:

Essential	**Application control** to prevent execution of unapproved/malicious programs including .exe, DLL, scripts (e.g. W
Essential	**Patch applications** (e.g. Flash, web browsers, Microsoft Office, Java and PDF viewers). Patch/mitigate computer
Essential	**Configure Microsoft Office macro settings** to block macros from the internet, and only allow vetted macros eith
Essential	**User application hardening**. Configure web browsers to block Flash (ideally uninstall it), ads and Java on the int
Excellent	**Automated dynamic analysis of email and web content run in a sandbox**, blocked if suspicious behaviour is ide
Excellent	**Email content filtering**. g in archives and nested archives). Anal
Excellent	**Web content filtering**. ebsites with good reputation ratings. Bl
	firewall to require use of a split DNS ser
	tion (DEP), Address Space Layout Rando
Very Good	**Server application hardening** especially internet-accessible web applications (sanitise input and use TLS not SSL
Very Good	**Operating system hardening** (including for network devices) based on a Standard Operating Environment, disab
Very Good	**Antivirus software using heuristics and reputation ratings** to check a file's prevalence and digital signature pric
Very Good	**Control removable storage media and connected devices**. Block unapproved CD/DVD/USB storage media. Bloc
Very Good	**Block spoofed emails**. Use Sender Policy Framework (SPF) or Sender ID to check incoming emails. Use 'hard fail'
Limited	**Antivirus software with up-to-date signatures**
Limited	**TLS encryption between email servers** to help prevent legitimate emails being intercepted and subsequently le

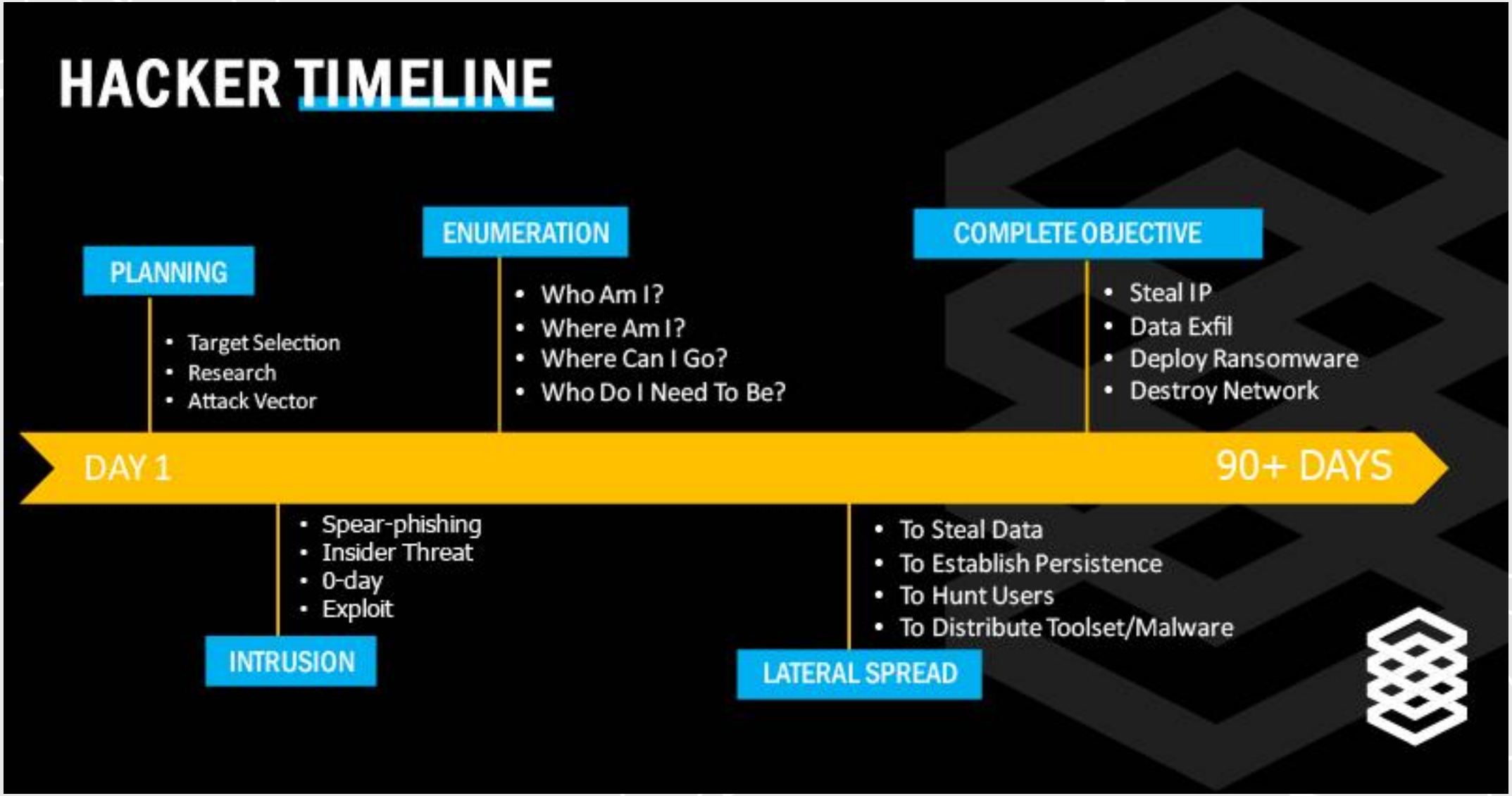
HACKER TYPES - SOPHISTICATED

Maturation Level 3

- Less reliant on public tools
- Adjust and adapt to the weaknesses presented
- Focused on particular targets
- Willing and able to invest some effort into circumvention

Objective:

- Pivot to other parts of a network
- Extend and Elevate Network Privileges
- Create Persistency, Cover their tracks


HACKER TIMELINE
PLANNING
Target Selection
Research
Attack Vector
ENUMERATION
Who Am I?
Where Am I?
Where Can I Go?
Who Do I Need To Be?
COMPLETE OBJECTIVE
Steal IP
Data Exfil
Deploy Ransomware
Destroy Network
DAY 1
90+ DAYS
INTRUSION
Spear-phishing
Insider Threat
0-day
Exploit
LATERAL SPREAD
To Steal Data
To Establish Persistence
To Hunt Users
To Distribute Toolset/Malware

MITIGATION STRATEGIES

- Restrict Administrative privileges.
- Different Administrator / Sub-Administrator accounts.
- Patch operating systems.
- Multi-factor Authentication.
- Network segmentation.
- Block network traffic of known malicious command and control protocols.

LIMITING THE DAMAGE

- Sensitive or Archive data – kept offline
- Immutable Storage for Backups and Original Data
- Data at rest should be Encrypted
- Time is of the essence to prevent lateral movement
- Extended Detection and Response “XDR”
  - Detecting footprints and door knocking as the perpetrator attempts to move laterally around the network.
  - Setup “Honey Pots” to trap malicious users
  - Time is of the essence – detection and apprehend before the damage

XDR "EXTENDED DETECTION AND RESPONSE"

- Infrastructure, Devices, Users, Privileges monitored
- Thousands of daily events aggregated and correlated
- Machine Learning (AI) sifts through the noise
- HIPAA, Essential Eight and CMMC Triggers
- Regular Penetration Testing
- Active Threat Hunting
- Honey Pots
- Daily Cyber Security Health check and audit

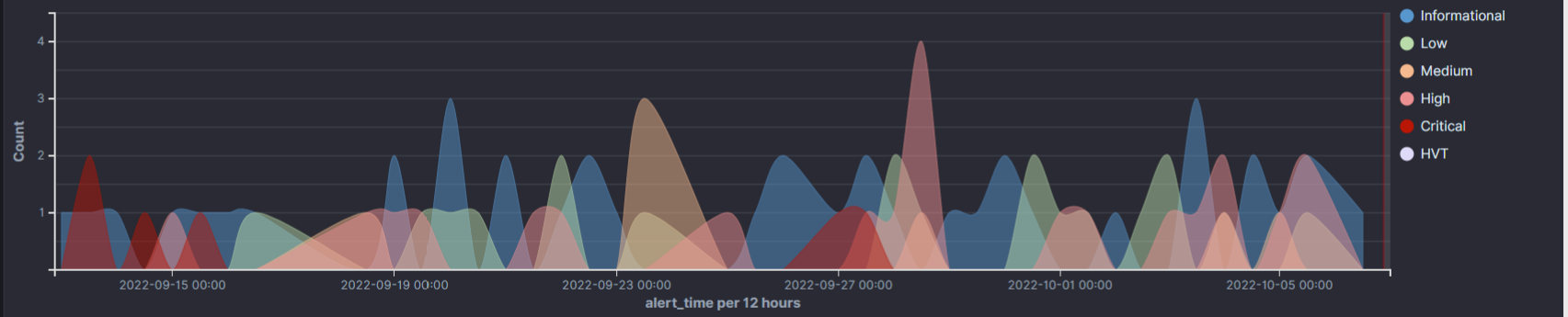
All Alerts	High Severity	HVT
94	23	0

Alert Name: Select...
Severity: Select...
Tenant: Select...
Technique: Select...

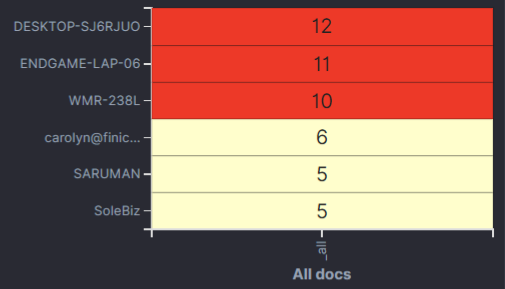
Alerts By Severity

Alert Category	Severity	Total
Windows Defender Actions	15	6
Host With External Vulnerability	12	3
TDAgent uninstalled	10	1
Logon attempts from multiple IP addresses for the user	10	7
Local Accounts Discovery (Quser or qwinsta)	10	1
Application with admin consent granted	10	5
Multiple common web attacks from same source ip	9	3
Multiple Credentials Reset Attempts	9	2
Attacks Or Recon Behaviour	7	3
RDP Login from Localhost	6	2
O365 Exchange Anti-Phish Rule Modification	6	1
O365 Exchange Anti-Phish Policy Deletion	6	1
Suspicious Autorun Application	5	4
Potentially Unwanted Open Port	5	4
		94

1 2 »



Most Alerts

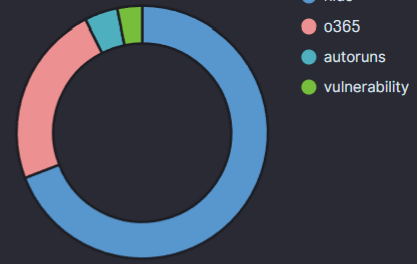


Techniques

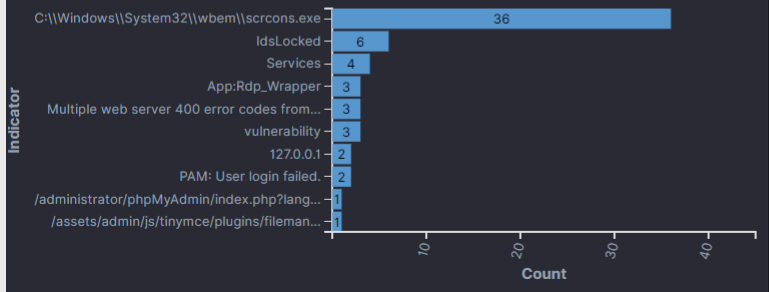
Technique	Alerts
Event Triggered Execution	36
Brute Force	14
Valid Accounts	12
Impair Defenses	9

1 2 3 4 »

Data Sources



Top Indicators

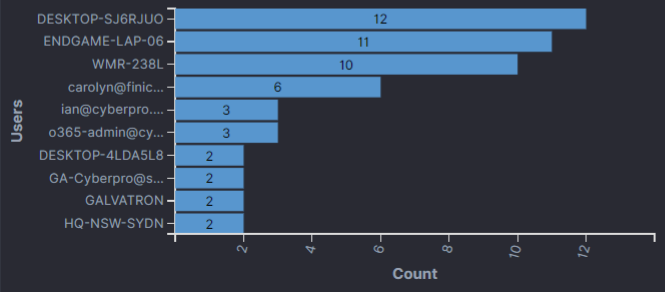


Sub Techniques

Sub Technique	Alerts
Windows Management Instrumentation Event Subscription	36
Cloud Accounts	12
Password Guessing	9
Password Spraying	7

1 2 3 »

Users With Most Alerts



Tenant

Tenant	Alerts
[redacted]	43
[redacted]	6
[redacted]	1
[redacted]	22

1 2 »

CyberPro

“Bringing World class Managed I.T. and Cyber Security to Australian Businesses” - Ian Ward, Founder & CEO