Uncover, Analyze, Protect

The Allure of Incident Response
and Digital Forensics

CyberCX

DFIR NZ

Rhys Jenkins

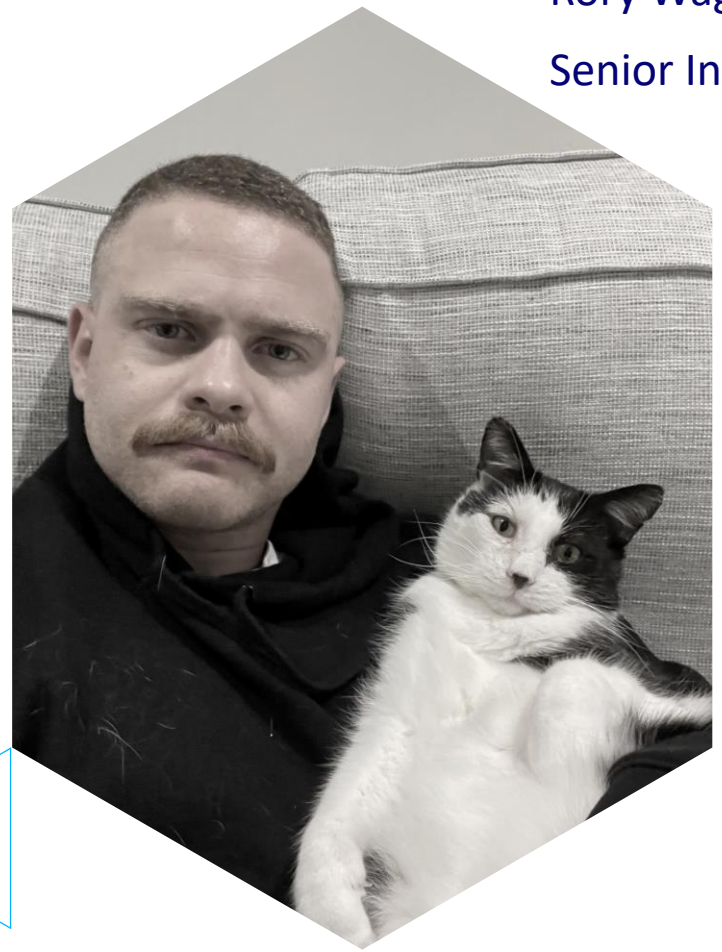
Senior Investigator

Rune

Executive Support

Rory Wagner

Senior Investigator



Fred

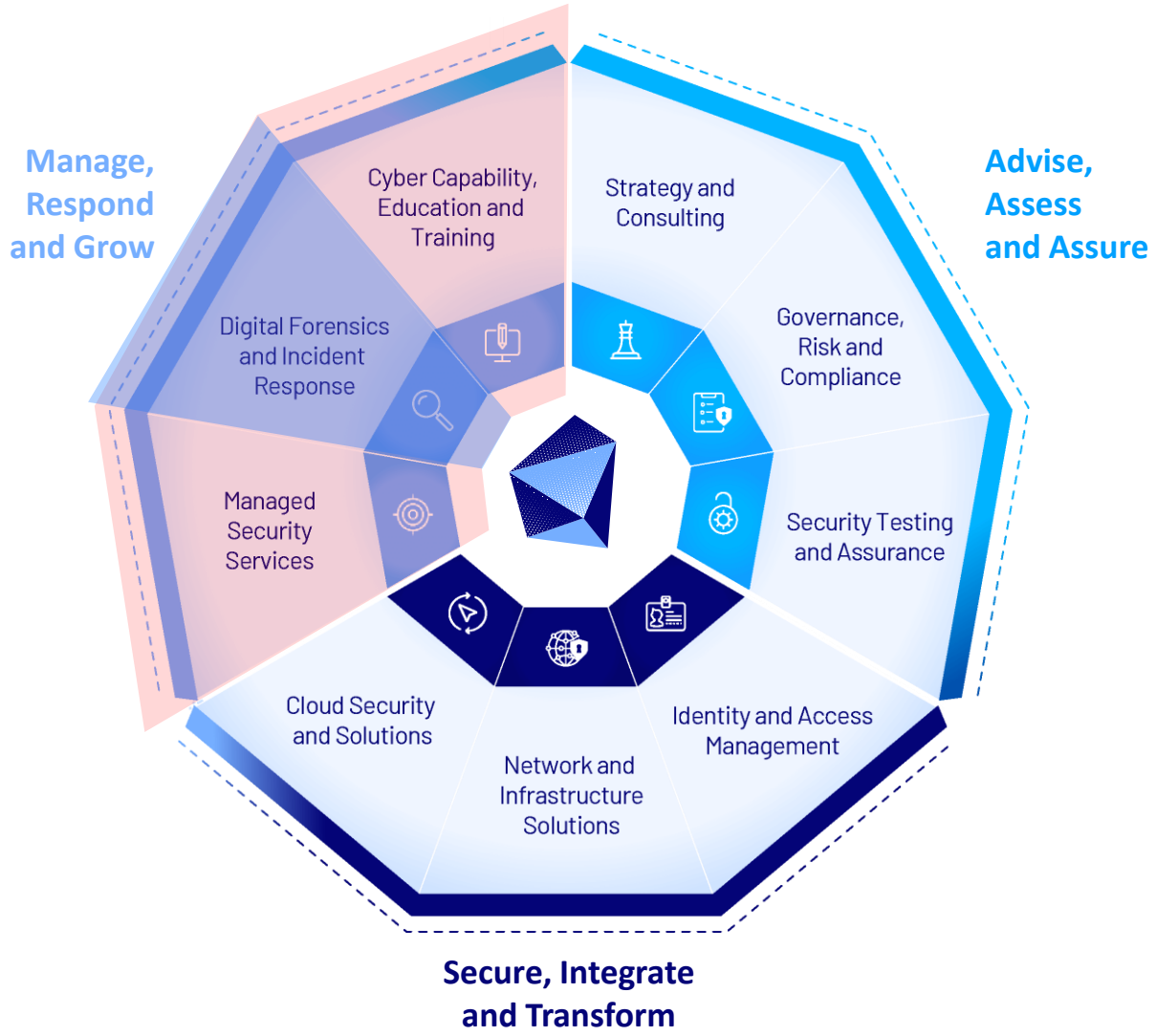
Executive Support

Who We Are

CyberCX is a global cyber security company comprising highly-skilled consultants, capabilities and offices in Australia, New Zealand, the United Kingdom and the United States.

What We Do

With a workforce of over 1,200 professionals, we are a trusted partner to private and public sector organisations helping our customers confidently manage cyber risk, respond to incidents and build resilience in an increasingly complex and challenging threat environment.

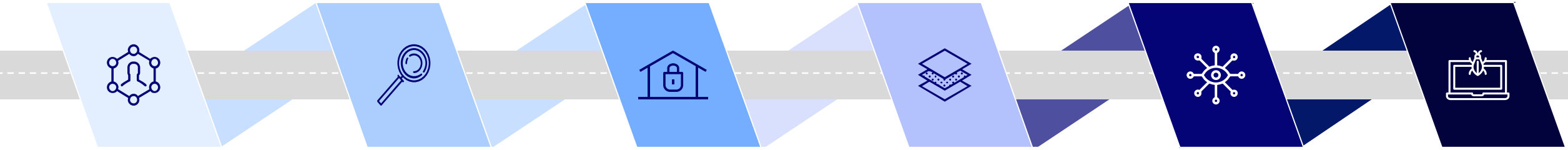


The Stats

250+
Security incidents responded to per year

500+
Cyber security baseline assessments per year

2500+
Penetration test per year



1200+
Cyber Security Professionals

20+
Offices across Australia & New Zealand

7
Active SOCs

Overview

- What we do?
- What software we use
- Threat Actor initial access
  - A few examples relating to each type
- What software Threat Actors use
- A closer look at two examples of Threat Actor software
  - MimiKatz
  - CobaltStrike
- Methods of exfiltration of data

What we do?

- Calls at all hours of the day and night to assist businesses
- An understanding of technology across the spectrum
  - Architecture
  - Implementation
  - Software
  - Hardware
- Engaging with clients using soft skills to understand:
  - What has happened?
  - How it’s happened?
  - Why it’s happened?
- Work to ensure it doesn’t happen again

Software we use

Paid

X-Ways

MAGNET FORENSICS

Cellebrite

Free

VIRUSTOTAL

CyberChef

Velociraptor

Initial Access

01
Phishing

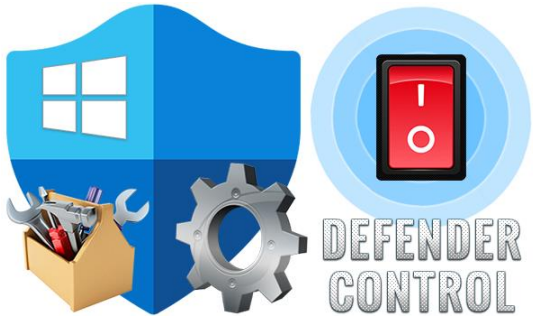
02
Exploit vulnerability

03
Password guessing/ spraying/ brute forcing

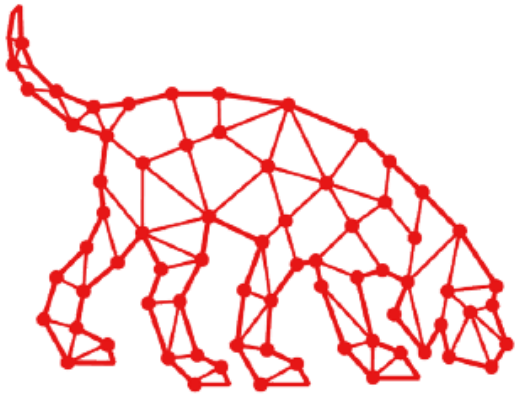
04
Malicious documents

“How do we pop this bad boy” – Threat Actor

Threat Actor Tooling



COBALTSTRIKE
ADVANCED THREAT TACTICS FOR PENETRATION TESTERS



BLOODHOUND

ADVANCED
IP SCANNER

Mimikatz


```
  .#####.   mimikatz 2.2.0 (x64) #17763 Apr  10 2019 00:55
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY gentilkiwi ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # privilege::debug
privilege '20' OK

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 234764 (00000000:0002deb6)
Session           : Interactive from 2
User Name         : user
Domain            : test-PC-x64
SID               : S-1-5-21-1982681256-1210654043-1600862990-1000
        msv :
         [00000003] Primary
         * Username : test
         * Domain   : test-PC-x64
         * LM       : d0e9aee149655a6075e4540af1f22d3b
         * NTLM     : cc36cf7a8514893efccd332446158b1a
         * SHA1     : a299912f3dc7cf0023aef8e4361abfc03e9a8c30
        tspkg :
         * Username : user
         * Domain   : test-PC-x64
         * Password : t3stus3r
...
```

Post compromise tool to extract sensitive information, such as passwords, from compromised systems

Usually executed on shared systems that will have many concurrent users

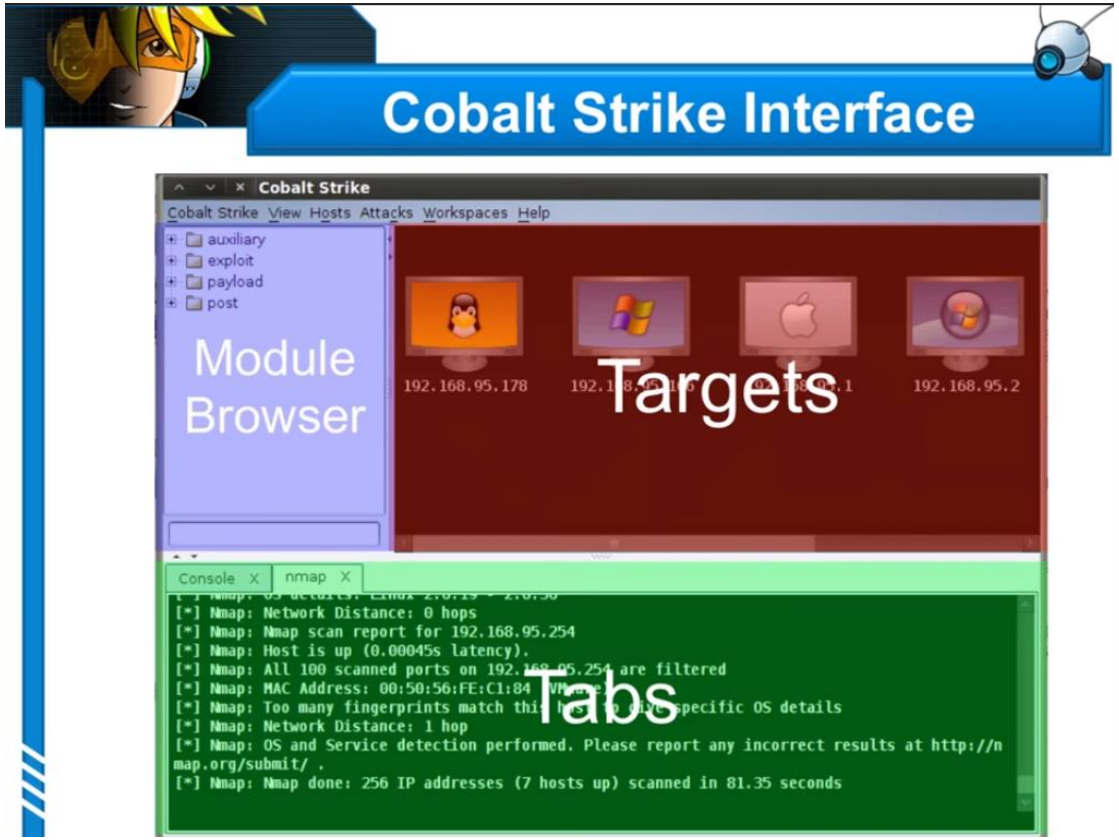
- RDP servers
- file servers
- jump boxes
- print servers

Accesses multiple resources to access this information

Outputs can vary depending on the module used

- plain-text passwords
- password hashes and tickets
- extract sensitive databases

CobaltStrike



Post-exploitation tool originally created for penetration testers but has gained infamy for it's use by Threat Actors.

An all-in-one tool with capabilities such as:

- Deliver weaponized documents or exploits to gain access among other methods
- Command and Control
- Lateral movement
- Process injection and further control over systems

Enables covert access to an environment and organizes it all into a nice graphical interface

When used correctly, can bypass many security products

Exfiltration

Questions?

CyberCX