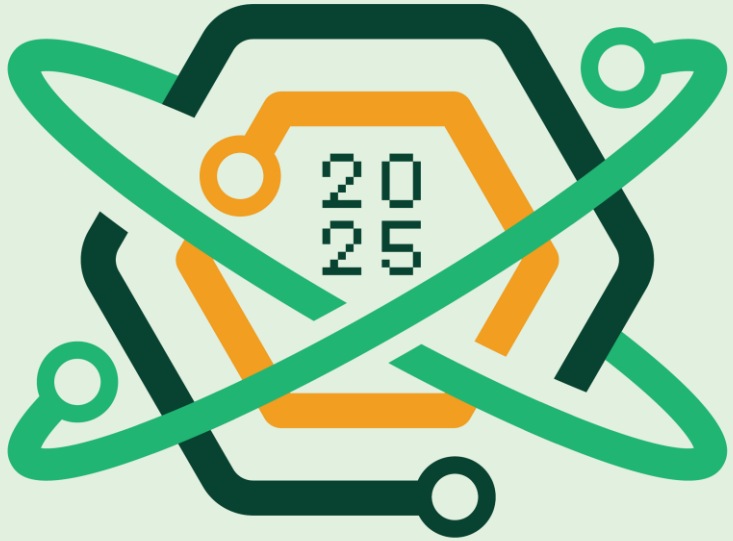


CYBER SYNC UP

COMBATTING CYBER CRIME

NSB Cyber
No Steps Backward

Triskele Labs

Hall&Wilcox
smarter law

McGrathNicol

WOTTON KEARNEY

HWL EBSWORTH
LAWYERS

Welcome

—

TROY FILIPCEVIC

CEO & Founder
Emergence Insurance

NSB Cyber
No Steps Backward

Triskele Labs

Hall&Wilcox
smarter law

McGrathNicol

WOTTON KEARNEY

HWL EBSWORTH
LAWYERS

Battlefield Cyber

Defence Strategies

CRIS WHITE

Head of Cyber Advisory
cyberSuite

NSB Cyber
No Steps Backward

Triskele Labs

Hall&Wilcox
smarter law

McGrathNicol

WOTTON KEARNEY

HWL EBSWORTH
LAWYERS

AGENDA

what we will cover

- How I got here?
- Modern battlefield
- Warfare strategies used to defend businesses
- Combat mindset

SHIELDS UP

modern battlefield

- The new front line is business and individuals
- Age of competition
- Requirement to build organisational resilience

warfare strategies and tactics

- Risk Management
- Cyber Threat Intelligence
- Kill Chain and MITRE ATT&CK
- Critical Factor Analysis
- Wargaming
- Training

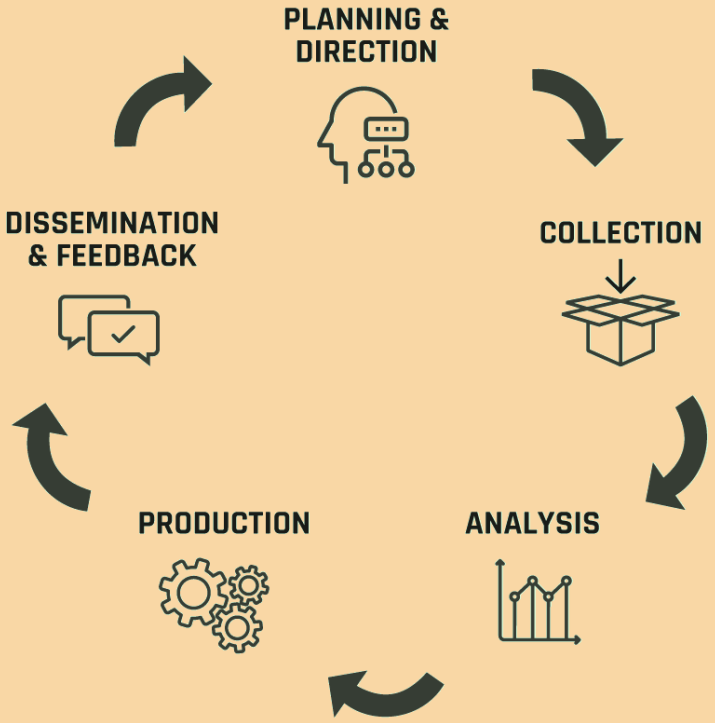
good guys vs bad guys

- What are you trying to protect?
  - Crown jewels, business continuity, sensitive information
- Who or what are you trying to protect it from?
- Who would target you?
  - Threat = Capability + Intent + Opportunity
- What are the likely or dangerous ways in which you would be targeted?
  - Risk scenarios
- What can we do to reduce the likelihood and/or impact?
  - Controls and response plans

MAKING BETTER DECISIONS

cyber threat intelligence

- Intelligence is all about enhancing decision making
- Understanding the threat and the tactics
- Intelligence sharing
- What questions need answering?

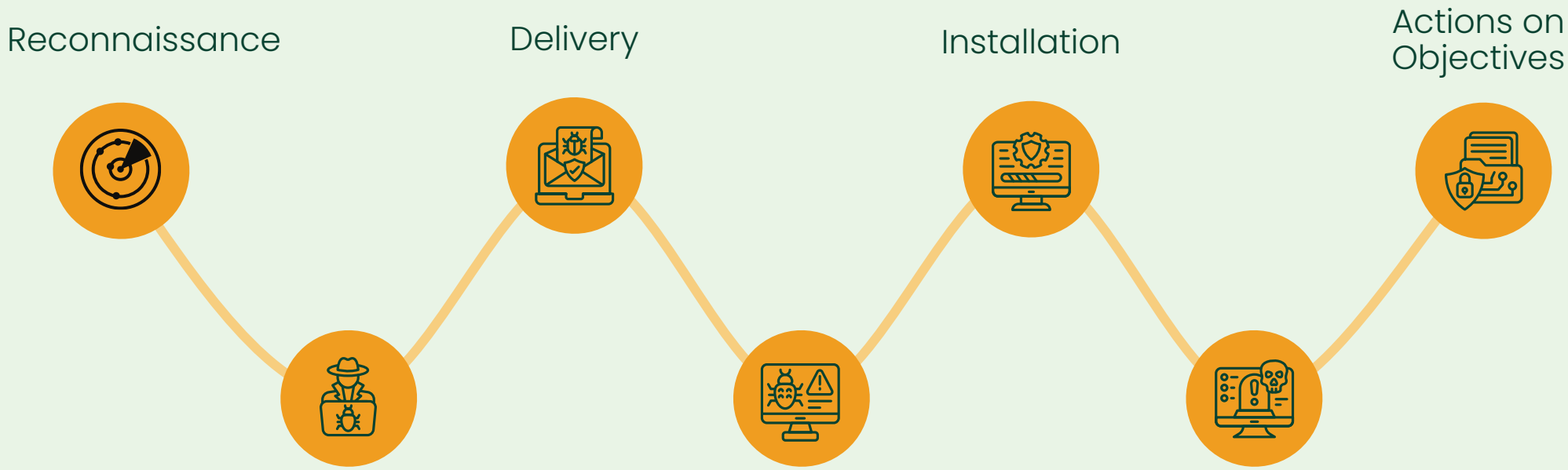


PRIORITY INFORMATION REQUIREMENTS

cyber threat intelligence

- What threat actors are currently targeting businesses in my industry or region?
- What are the most common tactics, techniques, and procedures (TTPs) used by these threat actors?
- Are there any recent cyber incidents or data breaches affecting companies like mine?
- What are the most critical vulnerabilities affecting my technology stack right now?
- Are any of my key vendors or third-party providers currently compromised or being targeted?

cyber kill chain



mitre att&ck

CYBER SYNC UP

cyberSuite

EXAMPLE SCENARIO

ransomware

- Awareness training
- Email philtering
- MFA
- Password managers

- MDR
- Network Segmentation
- Conditional Access
- Access Management

- MDR
- Offline backups
- Incident Response Plan
- Data Loss Prevention

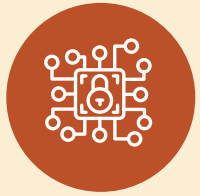
EXPLAINING WHAT CYBER RISKS LOOK LIKE

risk scenarios

MALWARE

- Ransomware
- Remote Access Trojans
- Keyloggers
- Botnet Agents

DENIAL OF SERVICE ATTACKS



- Overwhelm key services
- Physical and online

PHISHING

- Email compromise
- Browser in a browse

INSIDER THREATS

- Sensitive data loss
- Malicious or accidental

FINANCIAL THEFT

- Social engineering
- Push payments
- Online banking fraud
- PCI

THREAT INFORMED DEFENCE

what should I prioritise?

resources

money

time

ANALYSE RISK SCENARIOS

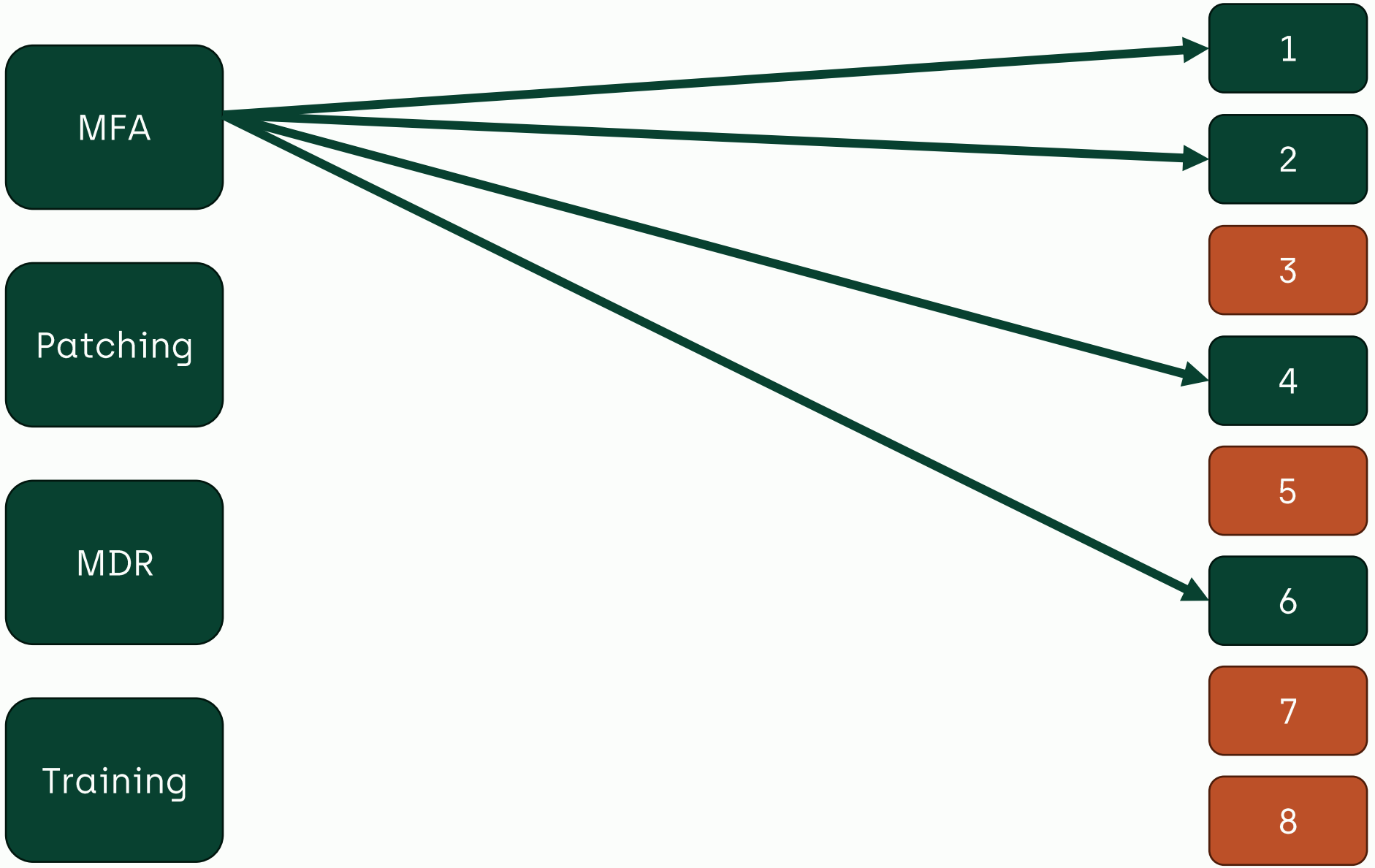
critical factor analysis

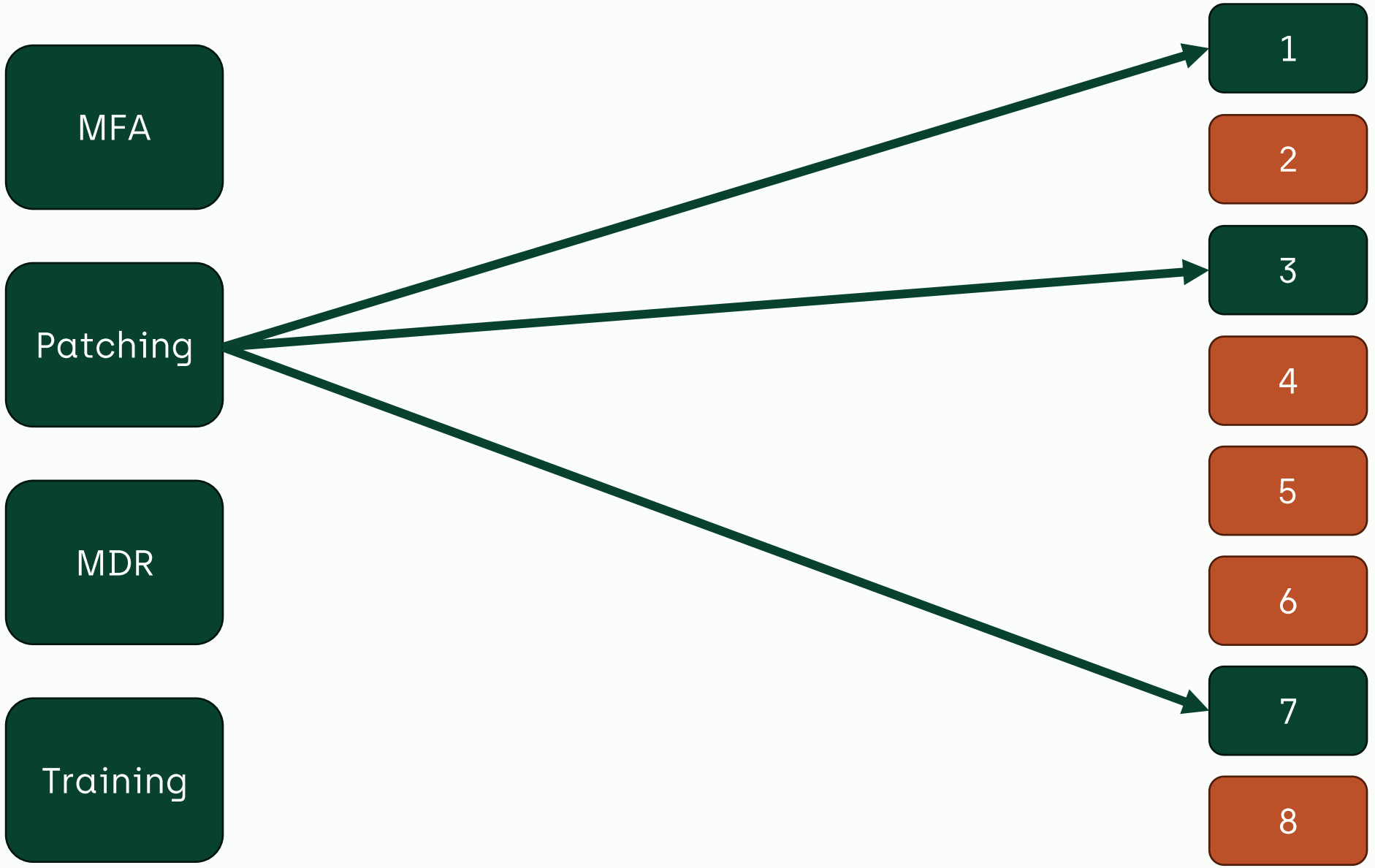
- Awareness training
- Email philtering
- MFA
- Password managers

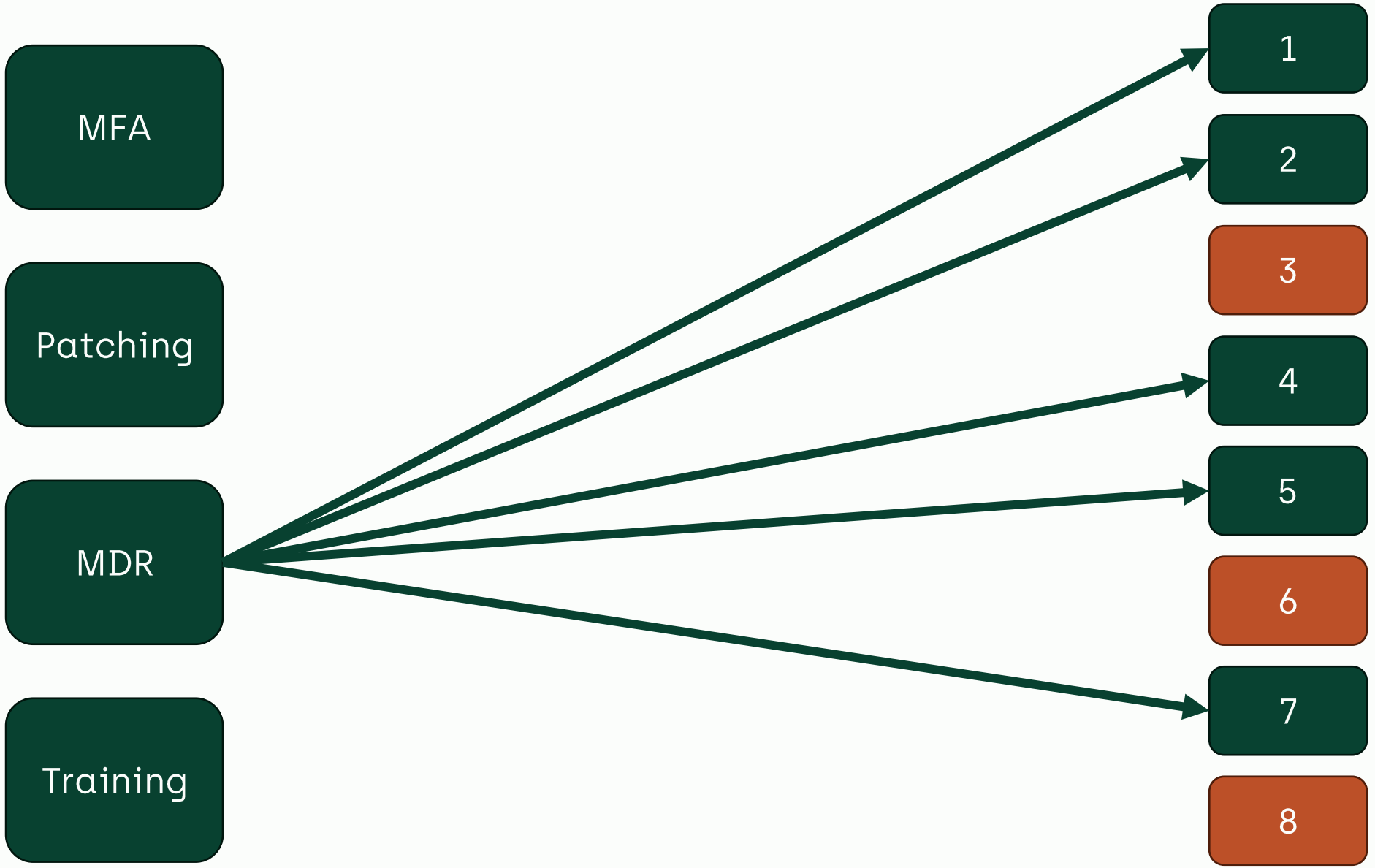
- MDR
- Network Segmentation
- Conditional Access
- Access Management

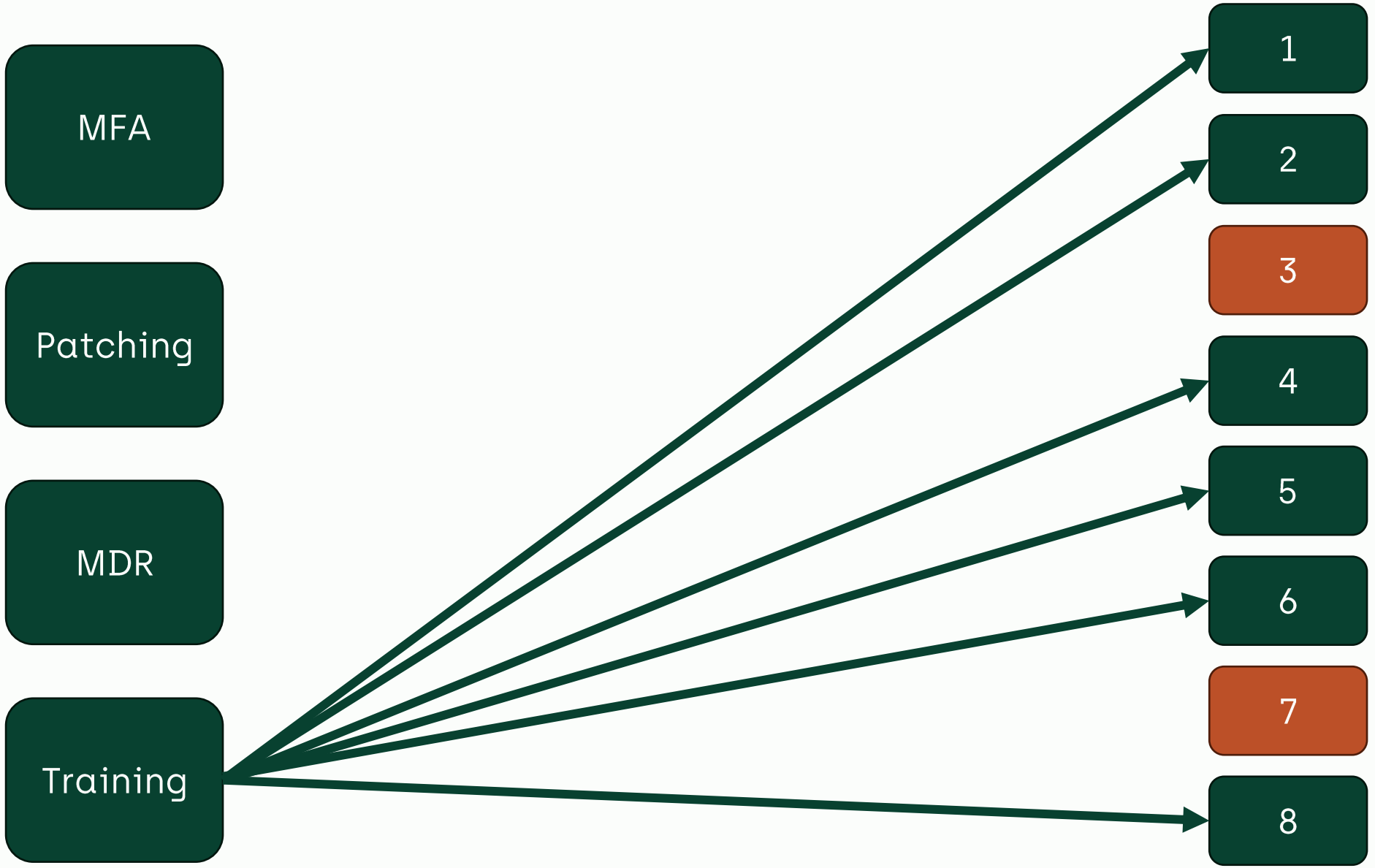
- MDR
- Offline backups
- Incident Response Plan
- Data Loss Prevention

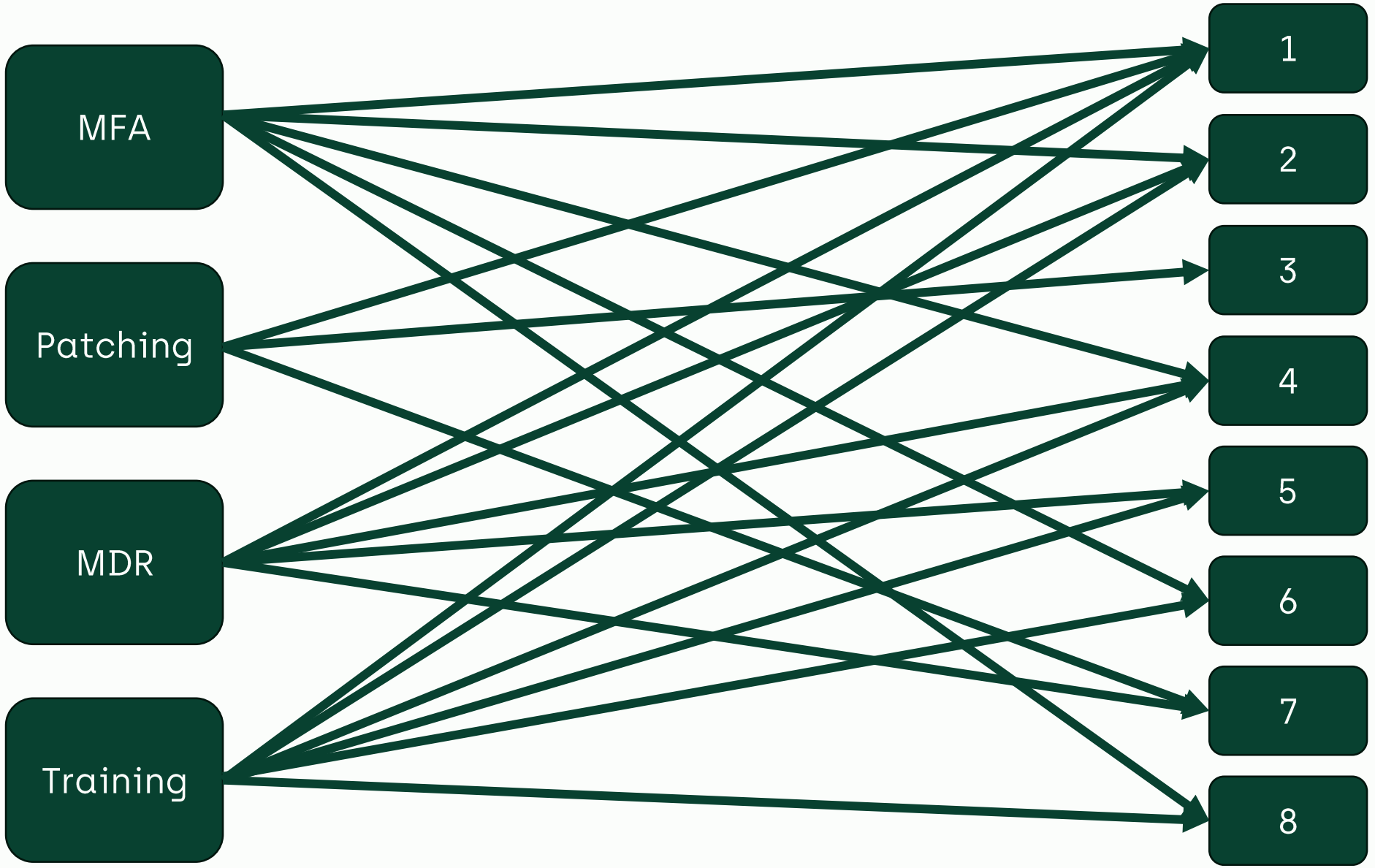

MFA
Patching
MDR
Training
1
2
3
4
5
6
7
8


MFA
Patching
MDR
Training
1
2
3
4
5
6
7
8


MFA
Patching
MDR
Training
1
2
3
4
5
6
7
8


MFA
Patching
MDR
Training
1
2
3
4
5
6
7
8


MFA
Patching
MDR
Training
1
2
3
4
5
6
7
8


MFA
Patching
MDR
Training
1
2
3
4
5
6
7
8

ARE YOU PREPARED?

training and response

- Train hard, fight easy
- Do you know what to do in the event of a cyber incident?
- Cyber Awareness Training
- Response Planning
- Wargaming = Tabletop exercises

In preparing for battle I have found that plans are useless, but planning is indispensable.

- Dwight D. Eisenhower

combat mindset

- Know what is valuable
- Know thy enemy
- Prioritise your resources
- Train hard, fight easy

Behind Enemy Lines

Demonstrating Real-World Cyber Threats

DARREN HOPKINS

Partner
McGrath Nicol

JESSE PEARCE

Senior Manager
McGrath Nicol

NSB Cyber
No Steps Backward

Triskele Labs

Hall&Wilcox
smarter law

McGrathNicol

WOTTON KEARNEY

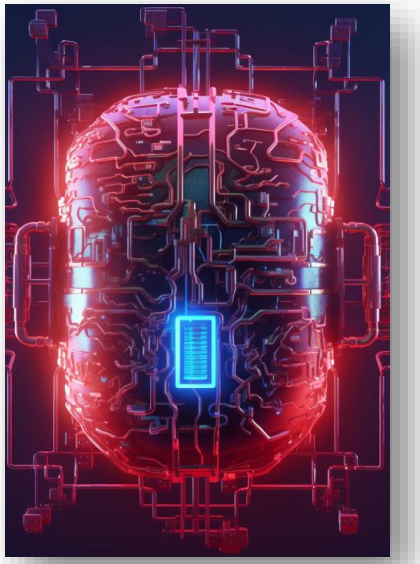
HWL EBSWORTH
LAWYERS

CYBER THREAT LANDSCAPE UPDATE

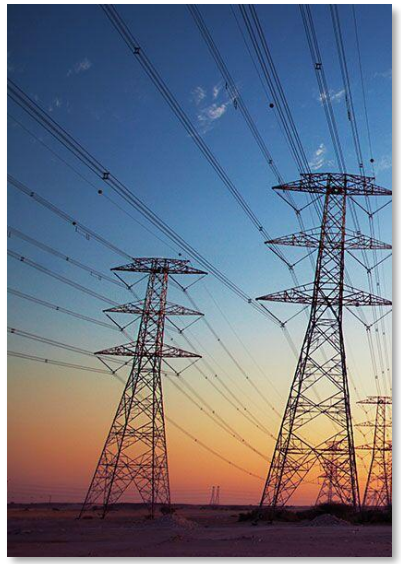
CYBER LANDSCAPE

2023-2030 Australian Cyber Security Strategy

ASD Annual Cyber Threat Report



The Impact of AI



Critical Infrastructure

Cyber Security Bill 2024

RECENT ATTACKS

FUNLAB

The Lynx ransomware group claimed responsibility for the attack on Funlab, owner of Strike Bowling, compromising of employee data.

2024
SEP

THE PLASTIC BAG CO.

The Plastic Bag Company was hit by the Sarcoma ransomware group, exposing sensitive data, including tax and insurance records.

2024
OCT

FOLLOWMONT TRANSPORT

Akira ransomware group claimed to have stolen 230GB of sensitive data from Queensland logistics company, Followmont Transport.

2024
NOV

NOTRE DAME UNIVERSITY

The Fog ransomware group breached systems including student enrolment, timetabling, payroll and email, exfiltrating approx. 62GB of data.

2025
JAN

GENEA

The Termite ransomware group claimed responsibility for the breach that affected patient management systems and PII including medical history.

2025
FEB

MCGRATHNICOL RANSOMWARE SURVEY

SUMMARY OF 2024 FINDINGS

69%
of surveyed businesses have experienced a ransomware attack in the past five years

42%
fell victim to a single attack, **26%** were targeted repeatedly

84%
of businesses that suffered a ransomware attack in the past five years paid a ransom

75%
paid the ransom within 48 hours

65%
negotiated prior to making a ransom payment

$1.35m vs **$1.42m**

estimated average cyber ransom that was paid

average ransom business leaders would be 'willing' to pay

79%
of business leaders say it should be mandatory to report ransomware attacks to the authorities
↑ from 60% in 2023

88%
say their view of a company would be negatively affected upon learning of a ransom payment
↑ from 83% in 2023

93%
of business leaders believe their organisation is 'prepared' for a ransomware attack
↑ from 88% in 2023

80%
of businesses have an incident response plan in place
↑ from 61% in 2023

44%
of businesses have experienced a malware attack or a Business Email Compromise attack (39%) in the past 12 months

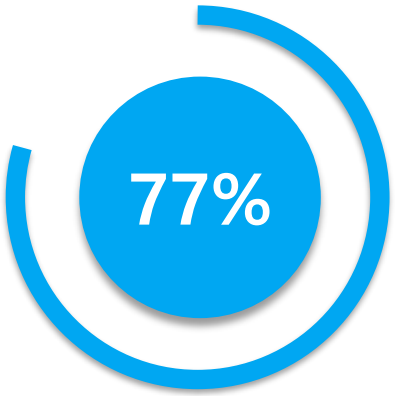
OTHER KEY FINDINGS

INSURED

91% of businesses are now insured against ransomware attacks, with an average coverage amount of **$1.47 million**.

IR PLAN

80% of businesses have an incident response plan in place.



BOARDS

77% of businesses now have a formal board notification protocol.

RANSOM PAYMENT

Only **one in ten** businesses say they would not pay under any circumstances.

RESULTS

Timeframe and Negotiation for Ransom Payment

- Two in three negotiated prior to making the ransom payment.

21%
made payment within 24 hours

53%
made payment between 24-48 hours

24%
made payment after 48 hours

- Businesses earning $50 million+ were approximately three times more likely to pay the ransom within 24 hours, without negotiation.

Willingness to Pay a Ransom

- Businesses aged over 10 years are more likely to not pay a ransom, under any circumstances.

83%
of businesses are willing to pay a ransom

34%
would be willing to pay $1 million or more

$1.42m
the average cyber ransom that businesses would be willing to pay

- Those in older businesses aged over 10 years are more likely than those in businesses aged up to 10 years to say their business wouldn't pay a ransom under any circumstance.
- In contrast, those in businesses aged up to 10 years are more likely than those in businesses aged 10 years or older to say their business would pay an amount.

RESULTS

Cyber insurance

Uptake

Nine in ten (91%) respondents say their business is currently insured against a ransomware attack (up from 79% in 2023).

Average Policy Coverage

The estimated insurance coverage average is $1.47m (up from $1.37m in 2023).

Policy Questions

One in ten (9%) who are insured are unsure of the cover amount (unchanged from 2023).

Approval

Nine in ten (89%) say their business was able to get insured or re-insured against future attacks after the attack (up from 81% in 2023).

Impact of Paying

Interestingly, those in businesses that decided to pay the ransom are more likely than peers in businesses that didn't to say the business was able to get insured or re-insured (92% compared to 74%).

Results

Mode of Entry

Email Fraud  24%

Malware  22%

MITM Attack  11%

Text Fraud  11%

Insider Threat  8%

Zero-Day  7%

Compromised Credentials  7%

CVE  7%

No 1 type of attack –

Business Email Compromise and Infostealers

INFOSTEALER OVERVIEW

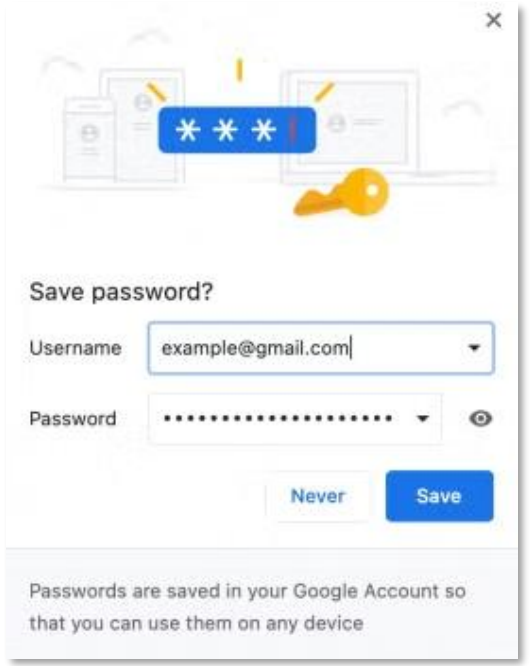
What is an Infostealer?

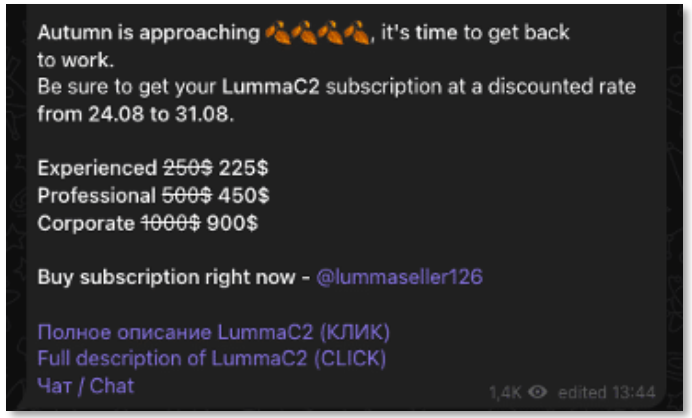
A type of malware designed to steal sensitive information that is often delivered via phishing emails and malicious web-based downloads.

Infostealers run as a background process, capturing sensitive data through the following techniques:

- Keylogging, to capture typed information
- Stored-credential theft
- Form grabbing, to intercept user inputs on websites
- Screenshot capture and clipboard monitoring

Some of the most common Infostealers include LummaC2, RedLine, Emotet, and Zeus.





LUMMA INFOSTEALER – INFORMATION CAPTURED

System information is captured from the victim's device...

```
LummaC2, Build 20231409
LID(Lumma ID): BhgGkI--IB2

- PC: [redacted]
- User: [redacted]
- Domain:
- Workgroup: [redacted]
- ComputerNameDnsHostname: [redacted]
- ComputerNameNetBIOS: [redacted]
- OS Version: Windows 10 (10.0.19045)
- HWID: [redacted]
- Screen Resoluton: 3840x2160
- Language: en-US
- CPU Name: Intel(R) Core(TM) i7-6700K CPU @ 4.00GHz
- GPU: NVIDIA GeForce RTX 3060
- Physical Installed Memory: 32768MB

- IP Address: [redacted]
- Country: AU

-------------------------------------
Брут и отработка крипты 70/30 > https://t.me/HUBHEAD

Депозит на форумах 5BTC. Берем балансы от 1000$. За время работы снято более 5.000.000$
Brute and withdraw cryptowallets 70/30
```

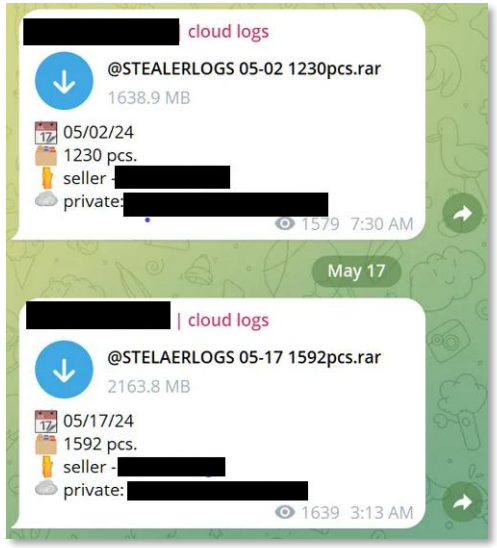
Login credentials that were previously saved in Google Chrome are captured...

```
SOFT: Chrome
URL: https://www.bcf.com.au/Member/Login
USER:
PASS: [redacted]

SOFT: Chrome
URL: http://www.entropialife.com/about/Signup.aspx
USER:
PASS: [redacted]

SOFT: Chrome
URL: https://www.seek.com.au/jobdetails/29883139/apply
USER:
PASS: [redacted]

SOFT: Chrome
URL: https://login.eveonline.com/Account/LogOn
USER:
PASS: [redacted]

SOFT: Chrome
URL: https://www.polarpersonaltrainer.com/
USER:
PASS: [redacted]

SOFT: Chrome
URL: https://careers.careersaustralia.edu.au/jobtools/jncustomlogin.
JobSeekerToolBoxAction
USER:
PASS: [redacted]
```

CYBER THREAT INTELLIGENCE – CREDENTIALS FOR SALE

- Privileged credentials for the victim's environment were listed for sale on an underground marketplace
- These credentials were sourced from the Infostealer infection on the employee's device
- The credentials were listed for sale for 5 Bitcoin (approximately $290K at the time of listing)
- Credentials were purchased by an affiliate of the ransomware group LockBit 3.0

Underground marketplace post…



"Brute and crypto mining 70/30 > https://t.me/HUBHEAD

Deposit on forums 5BTC. We take balances from $1000. Over $5,000,000 withdrawn during operation

Brute and withdraw cryptowallets 70/30"

THREAT ACTOR TACTICS INFOSTEALER AND MALWARE DEMO

How fast can we break Microsoft Office 365 MFA

How fast can we break Microsoft Office 365 MFA

Available exclusively to cybersecurity professionals

[redacted] is available exclusively to the owners or employees of legitimate red team or penetration testing companies.

We put the extra effort to ensure [redacted] Pro is used legitimately, by pre-screening potential buyers, before the purchase option is made available.

Focus on what you do best

- **For red teamers**

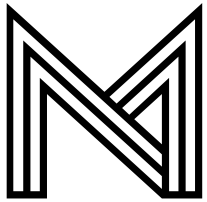
If you perform phishing as one of the initial vectors of gaining entry into the organization.

- **For penetration testers**

If you want to test and improve the company security by demonstrating a successful phishing attack from potential attackers.

- **For internal red teams**

If you perform security assessments in your company to test the security of employees and company resources.



McGrathNicol

The Shifting Legal Landscape

Recent cases and updates

EDEN WINOKUR

Partner
Hall & Wilcox

COLIN PAUSEY

Chief Operating Officer
Emergence Insurance

NSB Cyber
No Steps Backward

Triskele Labs

Hall&Wilcox
smarter law

McGrathNicol

WK WOTTON KEARNEY

HWL EBSWORTH
LAWYERS

Dispatches from the Frontline

BRIGITTE GASSON

Senior Associate
Hall & Wilcox

DARREN HOPKINS

Partner
McGrath Nicol

CRIS WHITE

Head of Cyber Advisory
cyberSuite

PETER FURST

Head of Incident Response
Emergence Insurance

NSB Cyber
No Steps Backward

Triskele Labs

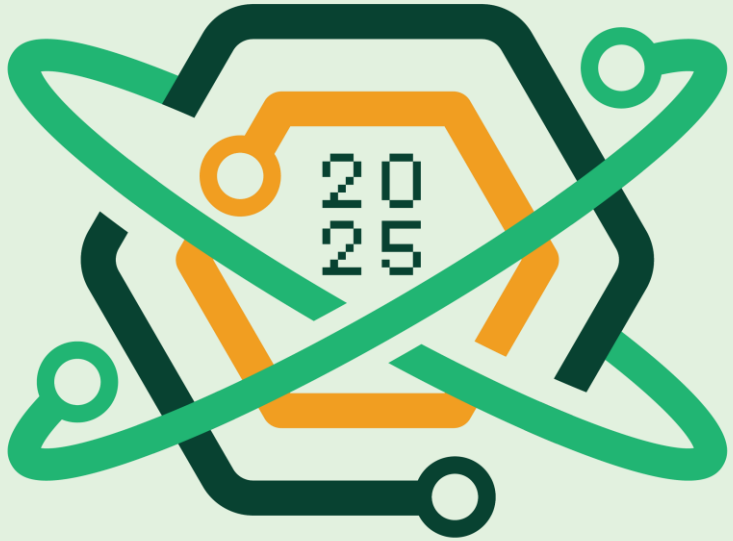
Hall&Wilcox
smarter law

McGrathNicol

WK WOTTON KEARNEY

HWL EBSWORTH
LAWYERS

THANK YOU



NSB Cyber
No Steps Backward

Triskele Labs

Hall&Wilcox
smarter law

McGrathNicol

WOTTON KEARNEY

HWL EBSWORTH
LAWYERS