

GROUP-IB



MANAGING RISK & RESPONDING TO THREATS

11TH MAY 2022

INTRODUCTION

Many security professionals believe it is no longer a question of “if” an organization will be compromised, but “when”. The damage caused by a successful has also grown in recent years, with ransomware gangs increasingly demanding multi-million dollar ransoms.

The increased probability and impact of an attack has led to many organizations categorizing cybersecurity as a key business risk.



About me



Alexandra Wells

Threat Intelligence & Attribution
Group-IB

GROUP-IB



PART 1: EVOLVING IMPORTANCE OF CYBERSECURITY

CONTI & CONTI LEAKS



Conti is currently one of the most active ransomware gangs, and is believed by CISA to have hit over 1,000 organizations across the world.

Conti's share of DLS victims in 2020



Conti's share of DLS victims in 2021



Conti Leaks appears to be a dissatisfied member of the gang that has leaked over 160,000 internal communications.

Conti's stats

Estimated earnings in 2021

\$180 million

Average ransom extracted

\$750 thousand

Average victim revenue

+\$100 million

CONTI'S TOOLS



How Conti uses OSINT during attacks

Conti has a dedicated team that uses OSINT to research their victim, their goals include:

- Identifying which of the thousands of devices infected by Conti belong to large corporations.
- Discovering the revenue of victims to determine the amount demanded.
- Finding information about board members and investors was used to harass them directly.

The legitimate services Conti uses

The gang utilizes legitimate services as part of their operations, such as:

- Testing their malware approximately every four hours against Windows Defender to ensure it works as intended.
- Investing \$60,000 in acquiring a license to Cobalt Strike, with half going to the company purchasing it on their behalf.
- Budgeting thousands of dollars each month for subscriptions to job-hunting websites to find new developers.

EXAMPLE: LOCALISED INFORMATION



Ransomware

Europe suffered the **second most** ransomware attacks in 2021 of any region

Ransomware attacks on European organizations grew **84%** last year

The Netherlands is **ranked 11th globally**, for the number of ransomware attacks

Phishing

Europe is the most targeted region by phishing, receiving **36.2%** of all attacks

The Netherlands has **3,836 phishing** resources hosted in the country

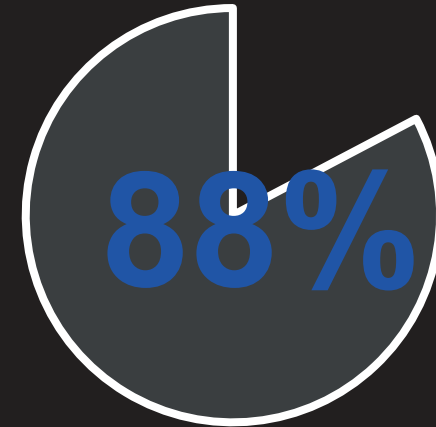
Phishing-as-a-Service programs are being developed in the Netherlands

LEADERSHIP IS MORE AWARE OF THE RISK



Over three quarters of CISOs say their organization experienced an increase in the number of cyber attacks in the past 12 months

VMware Global Security Insights Report 2021



88% of board directors now view cybersecurity as a business risk

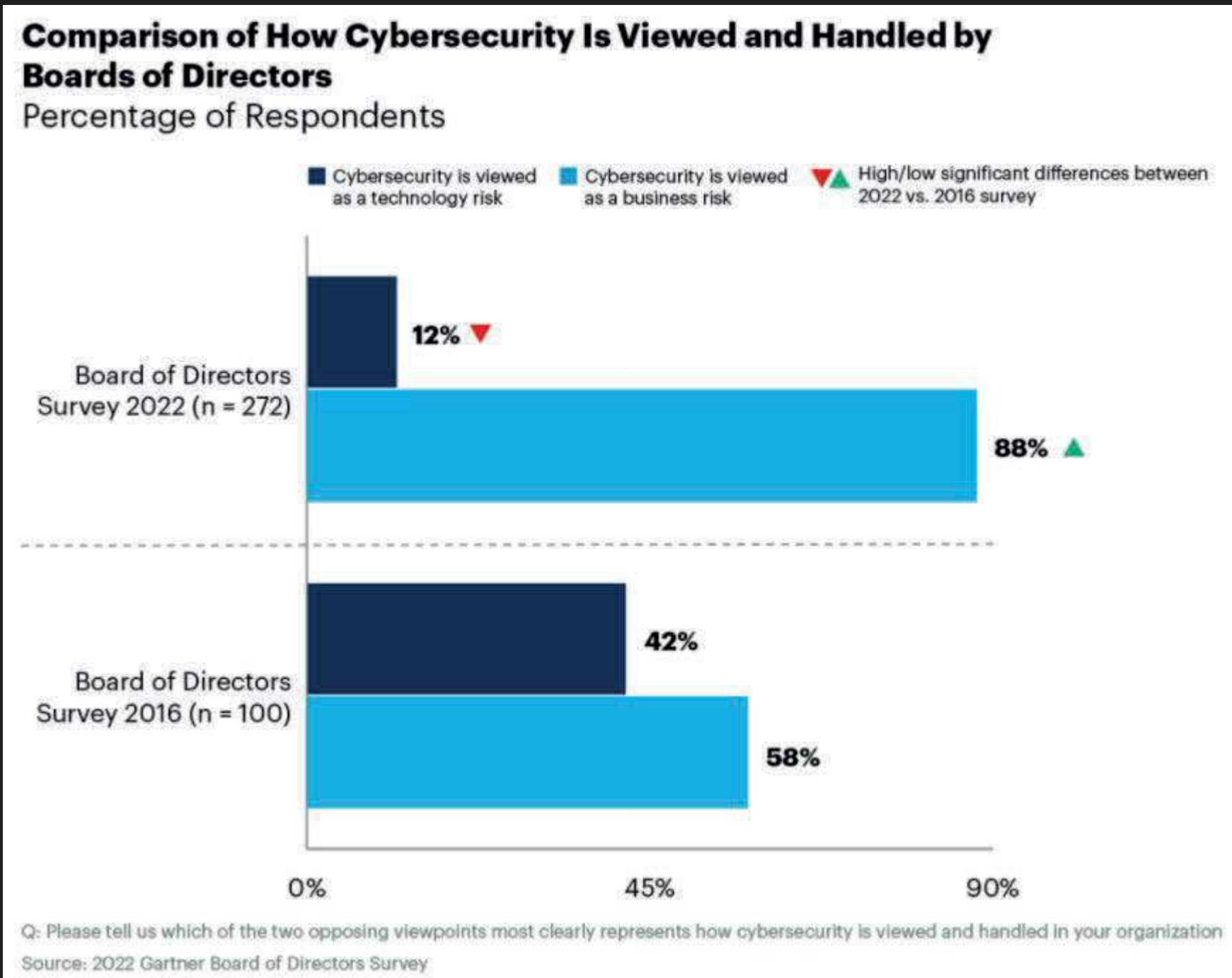
Gartner: CIOs Need to Rebalance Accountability for Cybersecurity With Business Leaders (2021)



Cyberattacks 2nd most concerning risk for doing business globally over the next 10 years

World Economic Forum - Global Risk Report (2020)

CYBERSECURITY WILL BECOME A PRIORITY



By 2025, 40 percent of boards of directors will have a dedicated cybersecurity committee overseen by a qualified board member, up from 10% today

- Gartner

WHAT DOES THIS MEAN FOR US?



We need to be able to assess the cyber risk of our organization and develop effective strategies to mitigate it

GROUP-IB



PART 2: UNDERSTANDING THE CYBER RESPONSE CHAIN

COMPLIANCE STANDARDS



Common standards:

ISO, NIST, GDPR, SWIFT CSCF, PCI DSS

Pros

- Easily auditable
- Simple to understand

Cons

- Are not updated regularly
- Define minimum requirements

THE CYBER RESPONSE CHAIN



3 Stages and 11 Steps of Response

Pre-compromise Response

Intra-compromise Response

Post-compromise Response

Prepare

Simulate

Detect

Redirect

Forensics

Neutralize

Harden

Block

Contain

Recover

Attribution

PRE-COMPROMISE



Prepare - understand threats and develop policies

Harden - reduce overall attack surface

Simulate - test the organization's capabilities

Pre-compromise Response

Intra-compromise Response

Post-compromise Response

Prepare

Simulate

Detect

Redirect

Forensics

Neutralize



Harden

Block

Contain

Recover

Attribution

INTRA-COMPROMISE

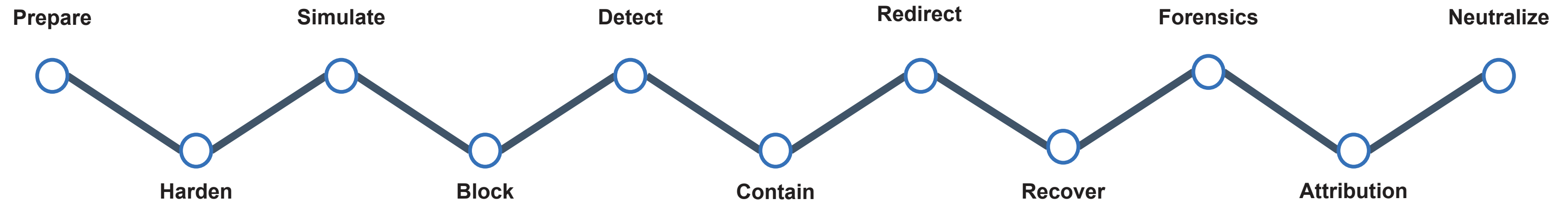


Block - identify and prevent attacks
Detect - hunt for signs of compromise
Contain - stop ongoing attacks
Redirect - analyse the tools used by attackers

Pre-compromise Response

Intra-compromise Response

Post-compromise Response



POST-COMPROMISE



Recover - remove attacker and restore systems

Investigate - review attack and identify area of improvement

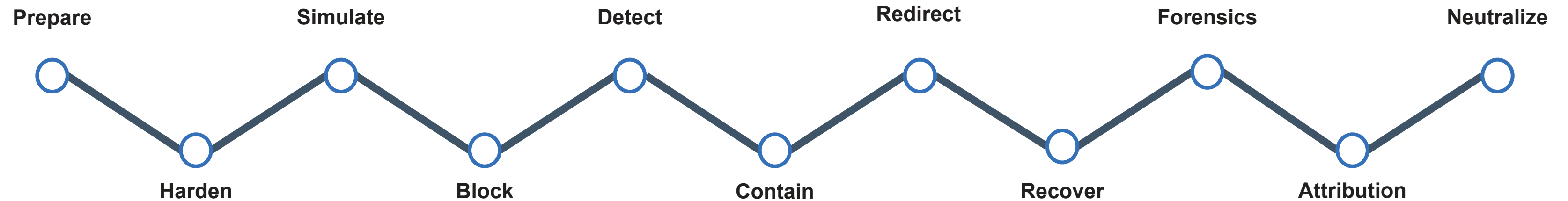
Attribute - correlate the tools and methods with ATPs

Neutralize - Restrict and disable the attacker

Pre-compromise Response

Intra-compromise Response

Post-compromise Response



HOW IT WAS DEVELOPED



Most cybersecurity attention and spending is conducted at the Block and Detect stages

Group-IB began by helping organizations in the post-compromise stage



Pre-compromise Response

Intra-compromise Response

Post-compromise Response

Prepare

Simulate

Detect

Redirect

Forensics

Neutralize

Harden

Block

Contain

Recover

Attribution

COMPARISON WITH OTHER FRAMEWORKS



Cyber Response chain	Prepare	Harden	Simulate	Block	Detect	Contain	Redirect	Recover	Forensics	Attribution	Neutralize
MITRE DEF3ND	X	Harden	X	Isolate	Detect	Evict	Deceive	X	X	X	X
MITRE Engage	Prepare	X	X	X	Expose	Affect	Elicit	X	X	Understand	X
NIST Cyber Security Framework	Identify	Protect	X	X	Detect	Respond	X	Recover	X	X	X
SANS PICERL	Prepare	X	X	X	Identification	Containment & Eradification	X	Recovery	Lessons learned	X	X
PCI DSS	R10 Auditable R12 Policy	R2 No Defaults R6 Secure systems R11 Test	R11 Test	R1 FW R5 AV R6 WAF R11 IPS	R11 IDS	R7 Restrict Access R3 Encrypt Mask	X	X	X	X	X

CYBER RESPONSE CHAIN MATRIX



Pre-compromise Response			Intra-compromise Response				Post-compromise Response			
Prepare	Harden	Simulate	Block	Detect	Contain	Redirect	Recover	Forensics	Attribution	Neutralize
IR Preparation	Automatic patching	BAS	Firewall NGFW	EDR	SOAR XSOAR	Honeypots Honeynets	Roll-back Restore	Evidence Collection	Investigation	Take-down services
Enable audit tracking, logging	Software life cycle management	CART	Spam & Phishing Filter Download filter	NDR NTA IDS	Tar-pits	Sandbox Detonation	Fail-over	DFIR	De-anonymize	Local Police FBI
Audits	Configuration Management	Pentest	WAF	SIEM	Self-defending networks	Execution in forensics environment	Buildscripts	Imaging	Malware attribution	INTERPOL Europol
Security Policies	Static and Dynamic Code analysis	Red-team	WIFI Encryption	XDR MDR	network Segmentation DMZ	Decoy Objects Deception	Infrastructure as Code	Lessons learned		Recover assets/ Money
Response planning, phone trees	Encrypt	Table top exercises	Antivirus Application whitelist	Threat Hunting	Zero Trust Network Access		Data recovery services	Prioritize improvements to chain		Disrupt Money Laundering networks
Attack Surface Management		Vulnerability Assessment	IPS	Compromise Assessment	Account Locking Process termination		Retrieval of Off-site backup	Malware Code Analysis		
Secure Design			Bot prevention	User Anomaly Detection	Access Restrictions					

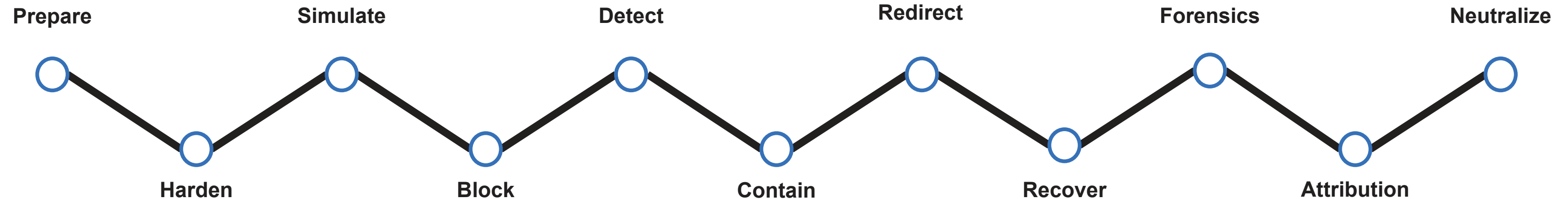
USING THE CYBER RESPONSE CHAIN



Pre-compromise Response

Intra-compromise Response

Post-compromise Response



Understand capabilities and how effectively the organization can respond

GROUP-IB



PART 3: USE CASES FOR THE CYBER RESPONSE CHAIN

THREE USE CASES WITH IMMEDIATE VALUE



1. Explaining a cyber attack

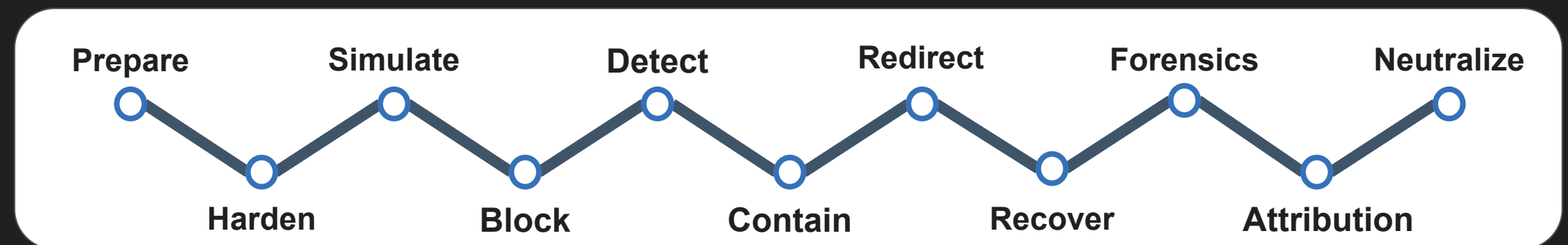
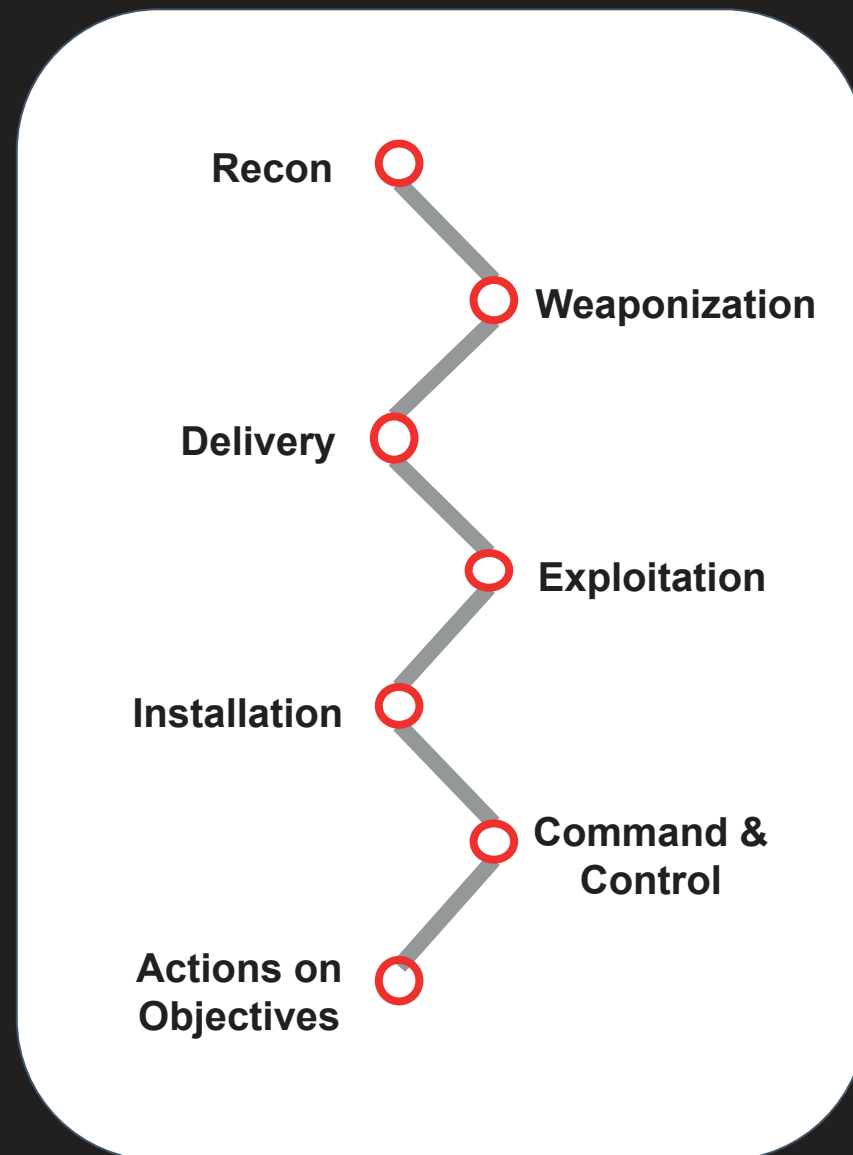
2. Performing table top exercises

3. Optimising annual budgeting

EXPLAINING A CYBER ATTACK



What about the Cyber Kill Chain?



The Response Chain

Describes the organization's responses
Full scope of activity
Greater value for explanation and review

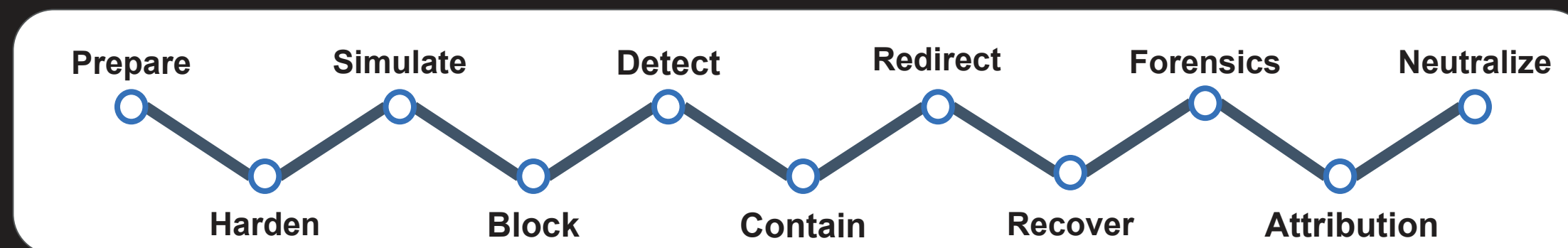


PERFORMING TABLE TOP EXERCISES

A security incident preparedness activity, taking participants through the process of dealing with a simulated incident scenario and providing hands-on training for participants that can then highlight flaws in incident response planning.

The exercise begins with the Incident Response Plan and gauges team performance against the following questions:

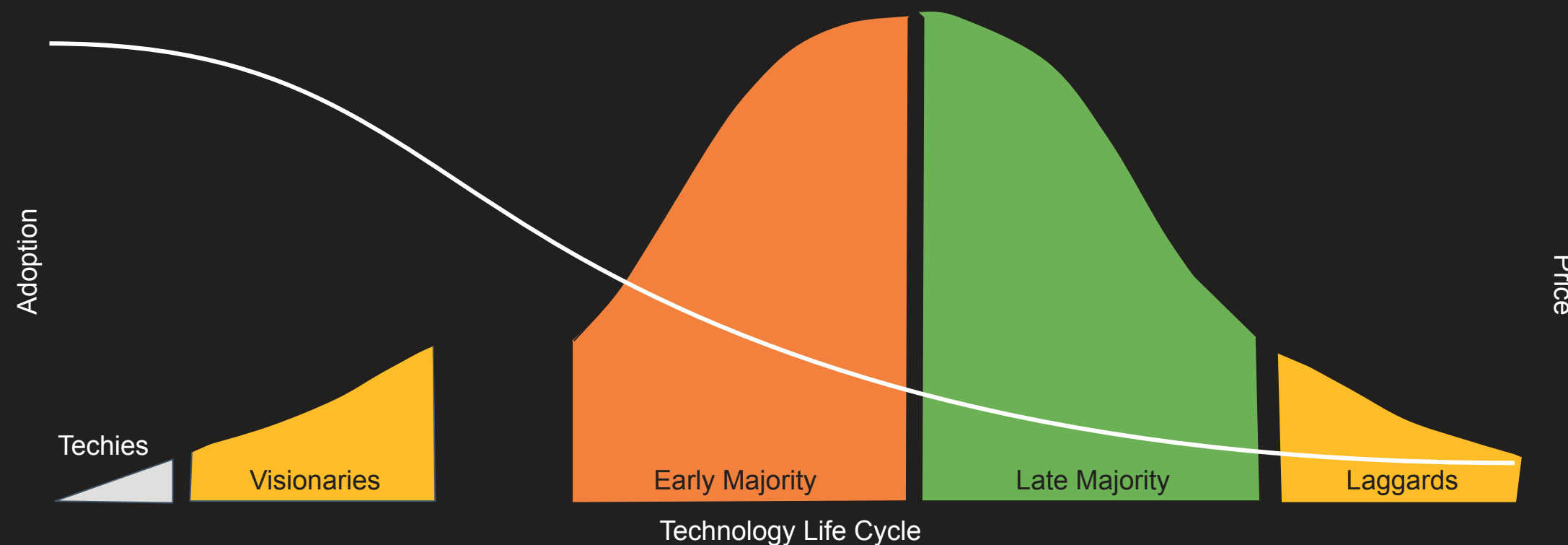
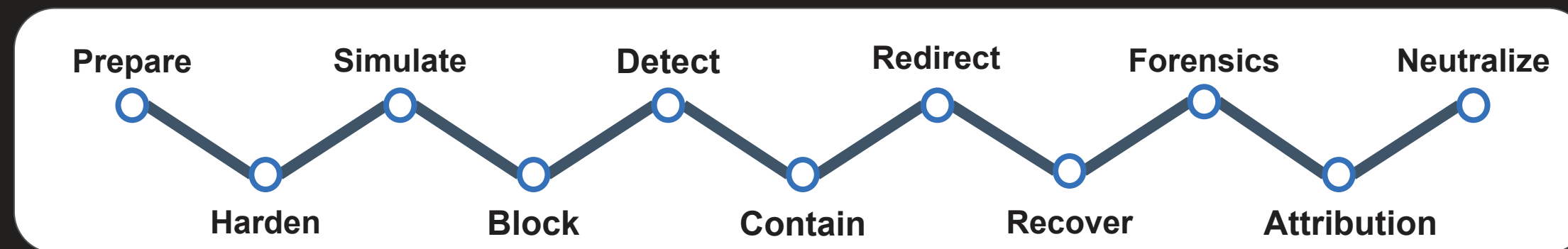
1. What happens when you encounter a breach?
2. Who does what, when, how, and why?
3. What roles will legal, IT, law enforcement, marketing, and company officers play?
4. Who is spearheading the effort and what authority do they have?
5. What resources are available when you need them?



OPTIMISING ANNUAL BUDGETING



Review expenditure plans by mapping them against the Cyber Response Chain, rebalance the budget to ensure coverage



KEY POINTS



The increasing scale and impact of cyber threats is resulting in more oversight

The Cyber Response Chain is an effective tool for assessing security capabilities

Use the framework to understand incidents, identify gaps in security, plan mitigations

GROUP-IB



QUESTIONS?

Interested in the whitepaper: a.wells@group-ib.com