

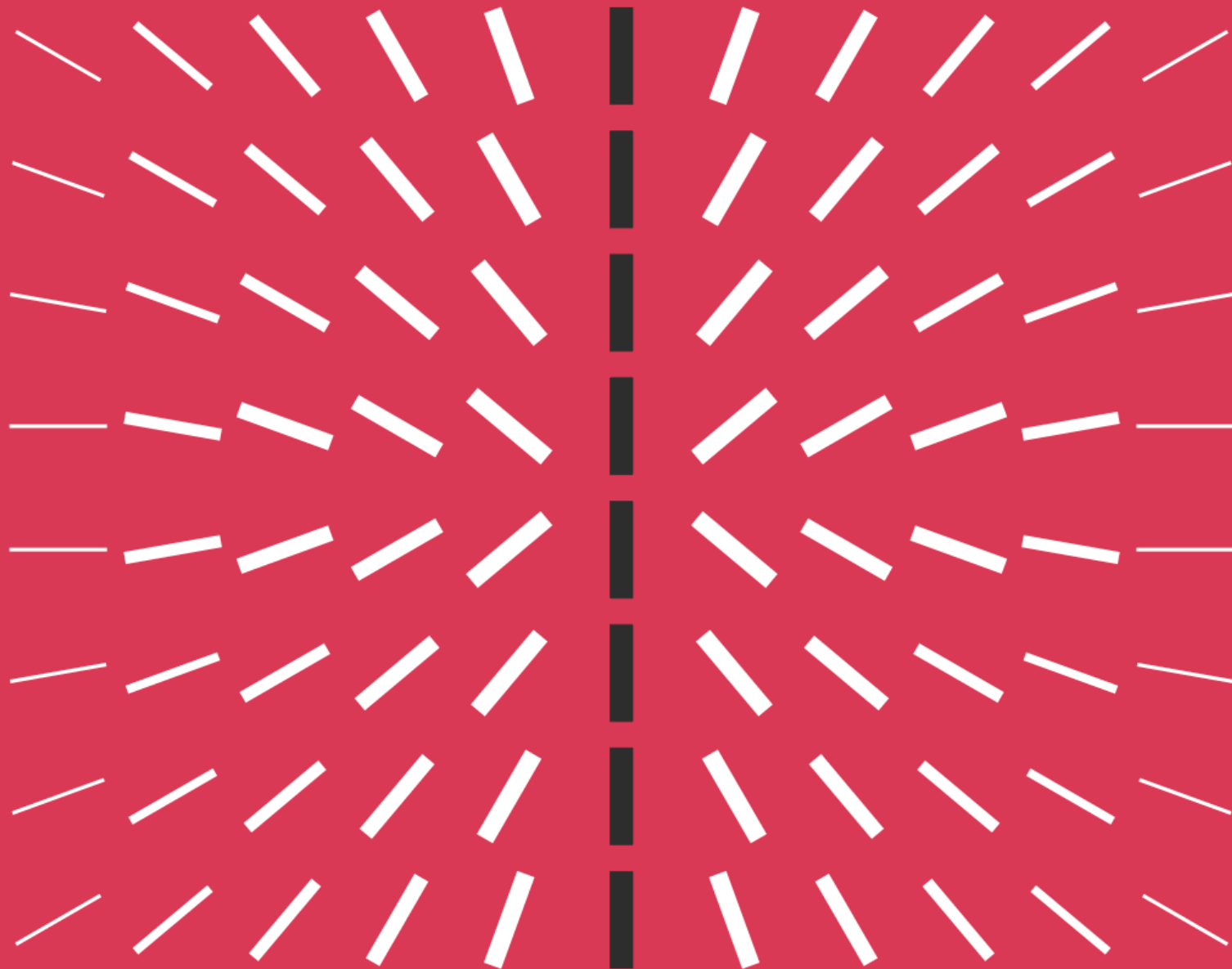


# Ransomware Defence and Response

## Minimising the Risk of an Increasing Threat

Gabriel Currie and Will Oram

9 October 2020



# Introduction



**Will Oram**

**@willoram**

Lead PwC UK's Cyber Threat Advisory team

Help clients deliver rapid improvements after cyber attacks

Manage and coordinate the response to major cyber security incidents

Deliver purple team and transformation engagements



**Gabriel Currie**

**@gabrielcurrie**

Lead PwC UK's Cyber Threat Advisory team

Help clients proactively improve threat detection and response capabilities

Manage and coordinate the response to major cyber security incidents

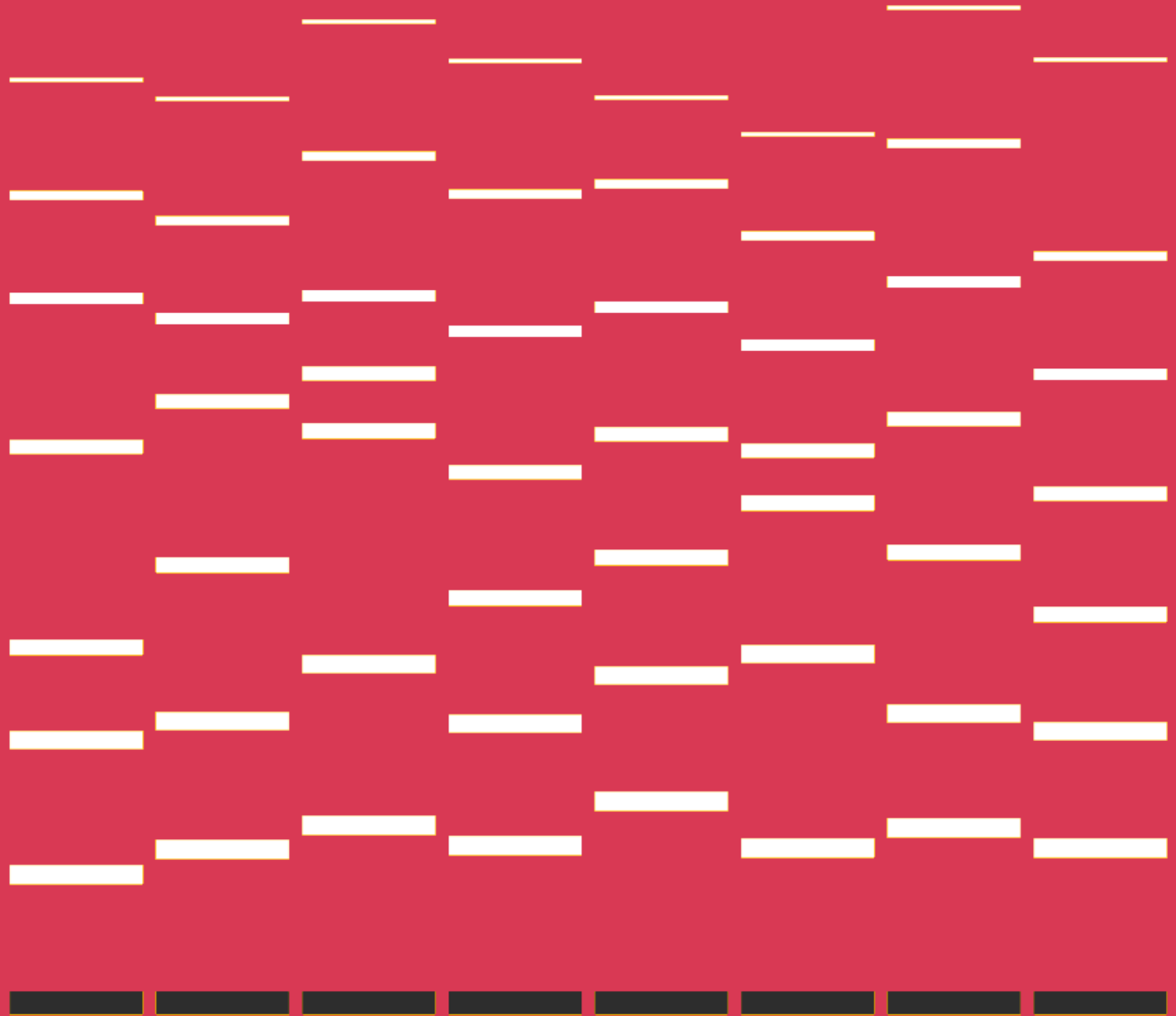
Architect post-incident remediation programmes

# Agenda

- 01 Human-operated ransomware attacks**
- 02 Preventing ransomware attacks**
- 03 Managing the response to an attack**

# 01

Human-operated  
ransomware  
attacks



# Human-operated ransomware attacks

**Human-operated ransomware is now one of the top priority cyber threats faced by most organisations. These attacks represent a more challenging threat than previous well-known ransomware attacks, such as NotPetya and WannaCry.**

- The 'human-operated' element means there are skilled and adaptable financially-motivated people behind these attacks who can identify and overcome defences.
- Attackers use techniques commonly seen in APT intrusions to gain access, spread widely over months, and deploy ransomware for maximum impact.
- Attackers are increasingly stealing and exfiltrating sensitive data (often posted to publicly accessible leak sites) to further extort victims, significantly complicating how organisations respond.
- Organisations who have not already taken steps to understand and reduce their vulnerability to these attacks should act now.



DoppelPaymer



Bitpaymer



REvil



Maze



Ryuk

# How human-operated ransomware attacks work

## Automated and mass scale



**Phish employees** and deploy malware to workstations



**Exploit vulnerabilities** in Internet-facing services

## 'Human-operated' and targeted



**Compromise privileged accounts** by exploiting common IT/AD hygiene issues



**Move laterally** and establish footholds using common offensive security tools



**Exfiltrate sensitive data** to attacker operated infrastructure



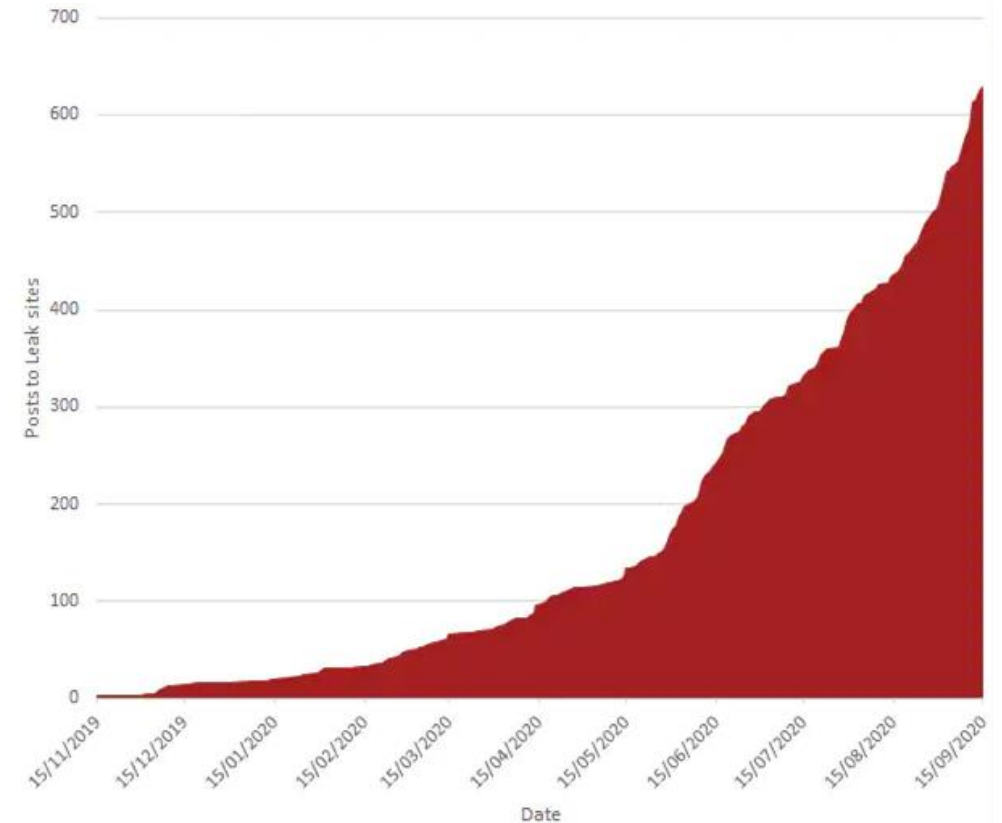
**Deploy ransomware** as widely as possible to for maximum impact

# The ransomware threat landscape

## The arrival of new affiliate schemes in 2020 has led to the growth in attacks

The rapid growth in ransomware attacks has been driven by:

- 01** Growing number of attackers attracted by **perceived easy revenue**.
- 02** Popularity of **affiliate programmes**, lowering the barrier to entry for newcomers.
- 03** Emergence of **leak sites**, placing additional pressure on victims to pay ransom demands.
- 04** Arrival of **new attackers**, some of which are highly aggressive (e.g., targeting healthcare).

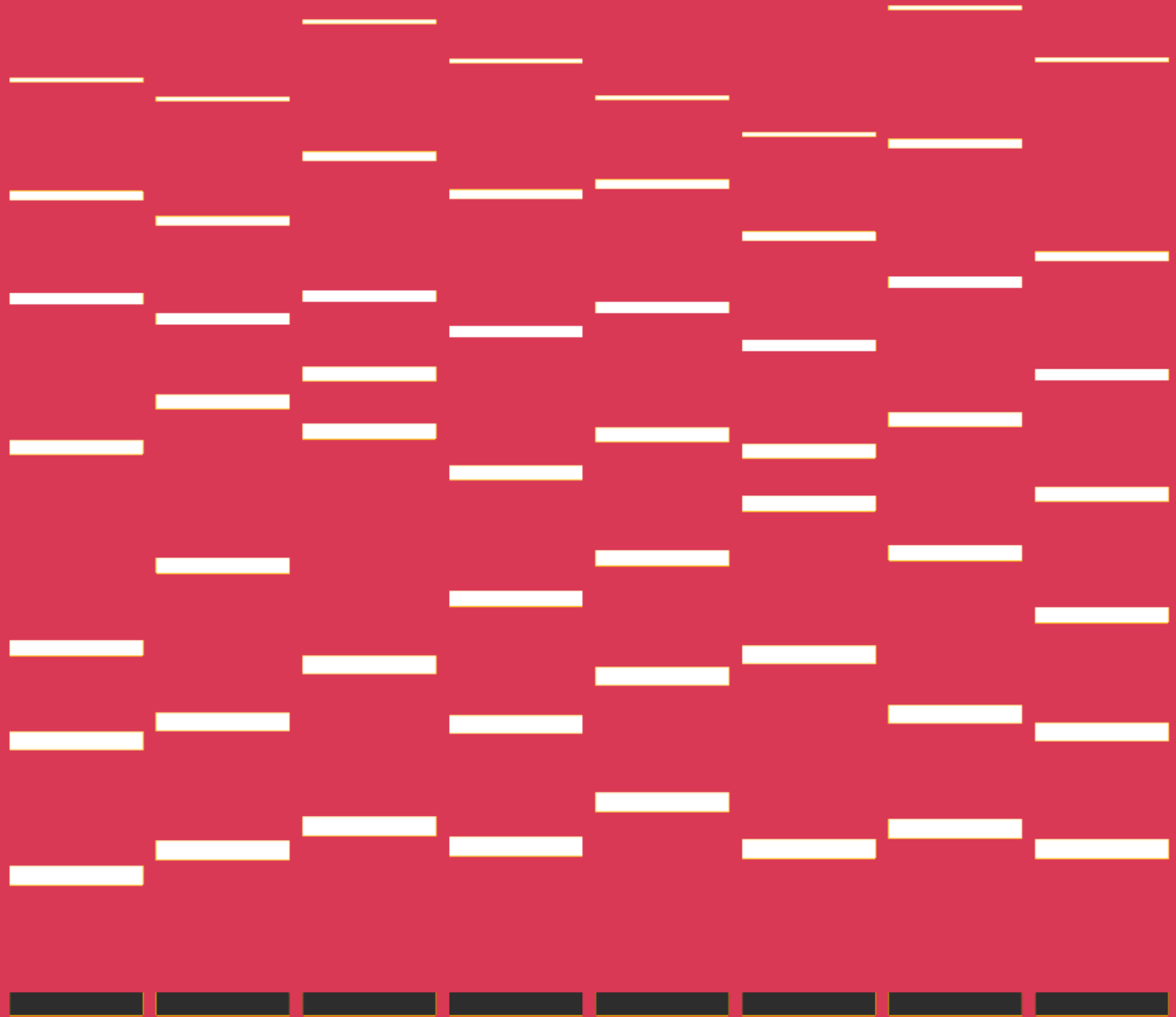


**Running total of ransomware data leaks**  
(November 2019 - September 2020)



# 02

Preventing  
ransomware  
attacks



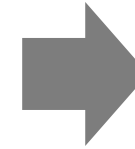
# Threat intelligence informs an effective defence

Initial access is often **opportunistic** and not carried out directly by ransomware actors. Other (criminal) actors use automated and mass scale techniques to gain access.



**Reduce attack surface**

Almost always opportunities to **detect and contain** attacks in their early stages. Deployment of ransomware is the final stage of an often lengthy intrusion.



**Reduce attackers' dwell time**

Attacker seek to cause **maximum impact** by targeting as many systems as possible and causing the most disruption.



**Limit blast radius of unauthorised access**

There are **skilled and adaptable** financially-motivated people behind these attacks who can identify and overcome defences.



**Prepare rapid isolation and recovery options**

# Four priorities to mitigate human-operated ransomware

## Reduce attack surface

### Internet-facing

External vulnerability management

Multi-factor authentication for email and remote access

### Phishing

Effectively configured email and web security tooling

Hardened endpoints to restrict execution of scripts / executables

Restrictions on the execution of Microsoft Office macros

Controls to prevent day-to-day usage of administrator accounts

## Reduce attackers' dwell time

Endpoint detection and response tooling on workstations / servers

Rules configured to detect common attacker techniques

Security tooling to monitor for compromise of privilege accounts

Automated remediation of 'commodity malware' infections

Rapid and effective investigation and containment of security alerts

## Limit blast radius of unauthorised access

### Privileged Accounts

Controls to protect privileged accounts from compromise

Eliminated common IT and AD hygiene issues to 'increase cost'

Securely architected and configured Active Directory

Segmented networks, including high-risk networks such as OT

Host-based firewalls on workstations with inbound blocks

Cloud-based SaaS services for employee email and file-sharing

## Prepare rapid isolation and recovery options

Endpoint protection tooling that blocks mass file encryption

Exercised incident and crisis management processes

Validated offline backups with a tested recovery strategy

Visibility of systems and ability to query and conduct forensics

Ability to isolate parts of network and understand impact

Ability to turn off applications and understand impact

# Preventing human-operated ransomware attack by delivering targeted tactical and strategic improvements

01

## Understand your vulnerability to the threat

Assess whether you can prevent / detect the techniques used in these attacks

### Recommendations

- ✓ Prioritise techniques with threat intel
- ✓ Align to MITRE ATT&CK framework
- ✓ Assess vulnerability with security testing

02

## Deliver tactical improvements to immediately reduce risk

Drive at pace improvements to detect and prevent techniques, and increase “cost to the attacker”

### Recommendations

- ✓ Collaborate with IT teams
- ✓ Use agile approaches and tools
- ✓ Driven by security testing

03

## Deliver sustainable cyber risk reduction

Address root-causes with strategic initiatives designed to deliver sustainable cyber risk reduction

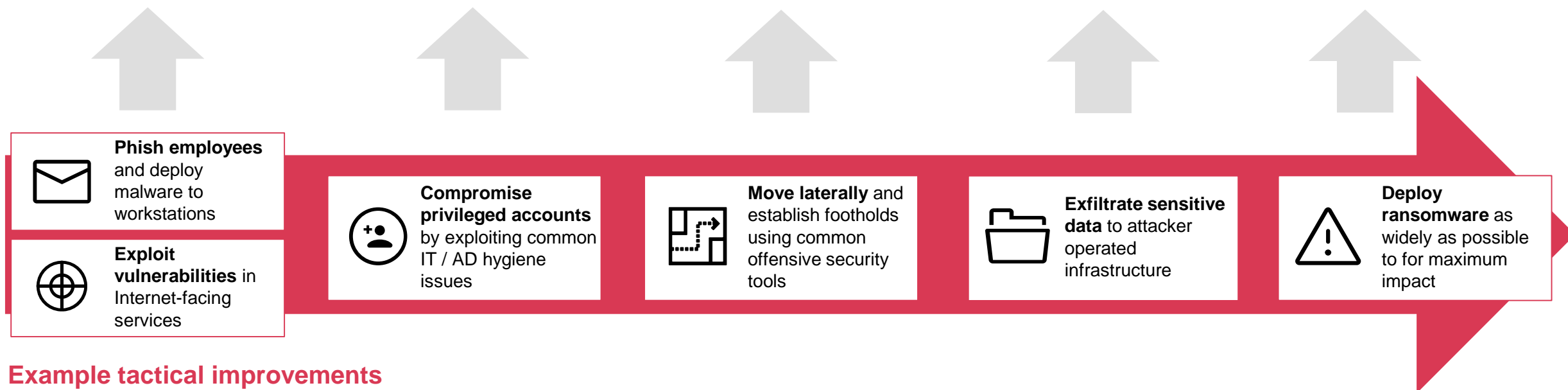
### Recommendations

- ✓ Bring in security architects
- ✓ Engage with the wider-organisation
- ✓ Make IT securable

Provide ongoing reporting to execs on your vulnerability to ransomware attacks, clearly demonstrate the impact of improvements made, using the results of this threat-based approach - “technique coverage” + “cost to the attacker”

# Targeted tactical improvements can significantly decrease risk

**Increase 'cost to the attacker' at every stage**  
**Create opportunities to detect and contain attacker**



## Example tactical improvements

Restrict files users are able to download and receive by email

Restrict the use of domain administrator accounts

Remove users and groups from local administrator groups

Remove or restrict access to sensitive data on network shares

Configure EPP/EDR tools to detect and block ransomware behavior

Restrict the execution of scripts and macros by users on workstations

Set strong passwords on service accounts and restrict privileges

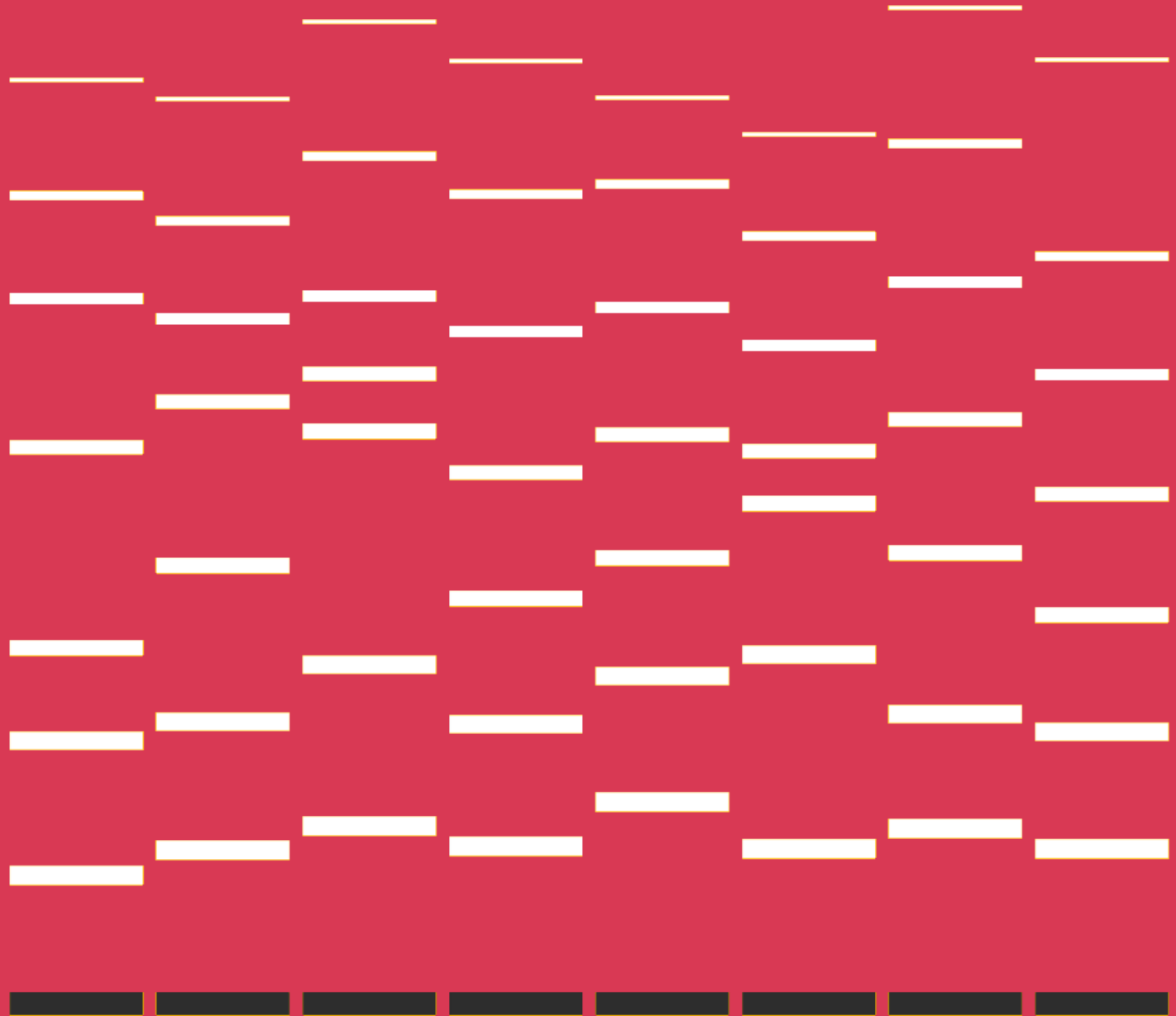
Remediate critical remote code vulnerabilities on internal servers

Effectively configure rules in data loss prevention tooling

Restrict Active Directory trust relationships

# 03

Managing the  
response to an  
attack



# Key challenges in ransomware response

## **Paying the ransom**

Conflicting ethical/legal/operational considerations, changing attacker tactics

## **Relying on insurance**

Understanding whether you are covered and how you can maximise the chance of this

## **“Realities of recovery”**

IT environments are complex, restoration more so

## **Constructively engaging with regulators**

Understanding your obligations, managing the response, taking defensible actions

## **Managing and coordinating the response and recovery**

Organisations are often not prepared for the rapid and complex response required

## **Preventing further attacks and 'making IT securable'**

Effectively addressing the vulnerabilities and root-causes, and sustainably reducing risk

# The “hard basics” of ransomware response

	What's happened?	What's the plan?	Who's in charge?
<b>What we see:</b>	No clear understanding of the facts which matter	Lack of “operational rhythm” or programme management  No clear strategy and objectives driving the response efforts	Lack of leadership and accountability  No clear or suitable incident management structures
<b>Consider:</b>	What attacker activity has been identified (initial entry, lateral movement, data impact, exfiltration)?  What systems have been impacted?  What are the business risks/impacts?	How do we want to respond to the attacker activity identified?  How and who will deliver this response?  How will we identify if the incident escalates and how will we respond?	Who is leading the response, and who are they accountable to?  Who is leading each individual element of the response?  Do we have the right expertise and experience needed?



# Four management tools for an effective ransomware response

## 01 Teams

The structure of a response needs to flex based on the organisation and incident.

- Senior oversight, strategic direction, challenge and decision making.
- Programme control and management with strong business input.
- Defined workstreams focused on resolving key IT and business challenges.

## 02 Artefacts

Documented artefacts can be critical to both managing the live response, and enable after-action review.

- Strategy and objectives.
- Team leadership and structure.
- Plans, including with key milestones, timelines, effort.
- Status reporting.
- Risks, assumptions, issues, dependencies.
- Tasks and actions.

## 03 Reporting

Timely and accurate reporting is critical to ensure the right people have the right information.

- Content: Who is the audience, what do they need to know and why?
- Cadence: How often is it useful or relevant to report?

## 04 Meetings

Crisis situations can result in meeting paralysis.

Properly structured and effectively run meetings to enable communications and decision making are key.

- Do we need to meet?
- What's the purpose of the meeting: decisions, discussion, or dissemination?
- How can we maximise effectiveness?

# Executing an effective response to ransomware attack

## Immediate Actions

Establish response structures to coordinate decision making

Identify stakeholders and develop comms strategy

Determine extent of attack

Determine business impact

Rapidly identify critical business processes and enact continuity plans

Determine ransom strategy

Manage legal and regulatory implications

## Short-term Actions

Fully investigate nature and extent of attack

Prioritise business processes to guide remediation and recovery

Securely recover and rebuild

Analyse attack paths to identify weaknesses

Deliver targeted protection and detection improvements

Rapidly enhance detection and response capabilities as compensating control

## Medium-term Actions

Assess protection and detection capabilities to identify quick-win improvements

Build sustainable detection and response capability

Rapidly uplift security capabilities in key areas

Review technical and business response to the incident and implement lessons learnt

## Long-term Actions

Understand root-cause issues

Identify key control and capability gaps to prevent incident reoccurring

Re-align existing strategic programmes

Plan and deliver cyber security strategy and transformation programmes

Make IT “securable”

# Any questions?

Ask Us (Almost) Anything About Cyber Defence @ 4:25 CDT

Or get in touch with us... @willoram

@gabrielcurrie

[pwc.co.uk/cybersecurity](https://pwc.co.uk/cybersecurity)

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.

© 2020 PricewaterhouseCoopers LLP. All rights reserved. PwC refers to the UK member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see [www.pwc.com/structure](https://www.pwc.com/structure) for further details.