Welcome

Cyberresilience: Minimizing the Impact and Cost of a Cyberbreach

Today’s agenda

01 The State of Cyber Risk

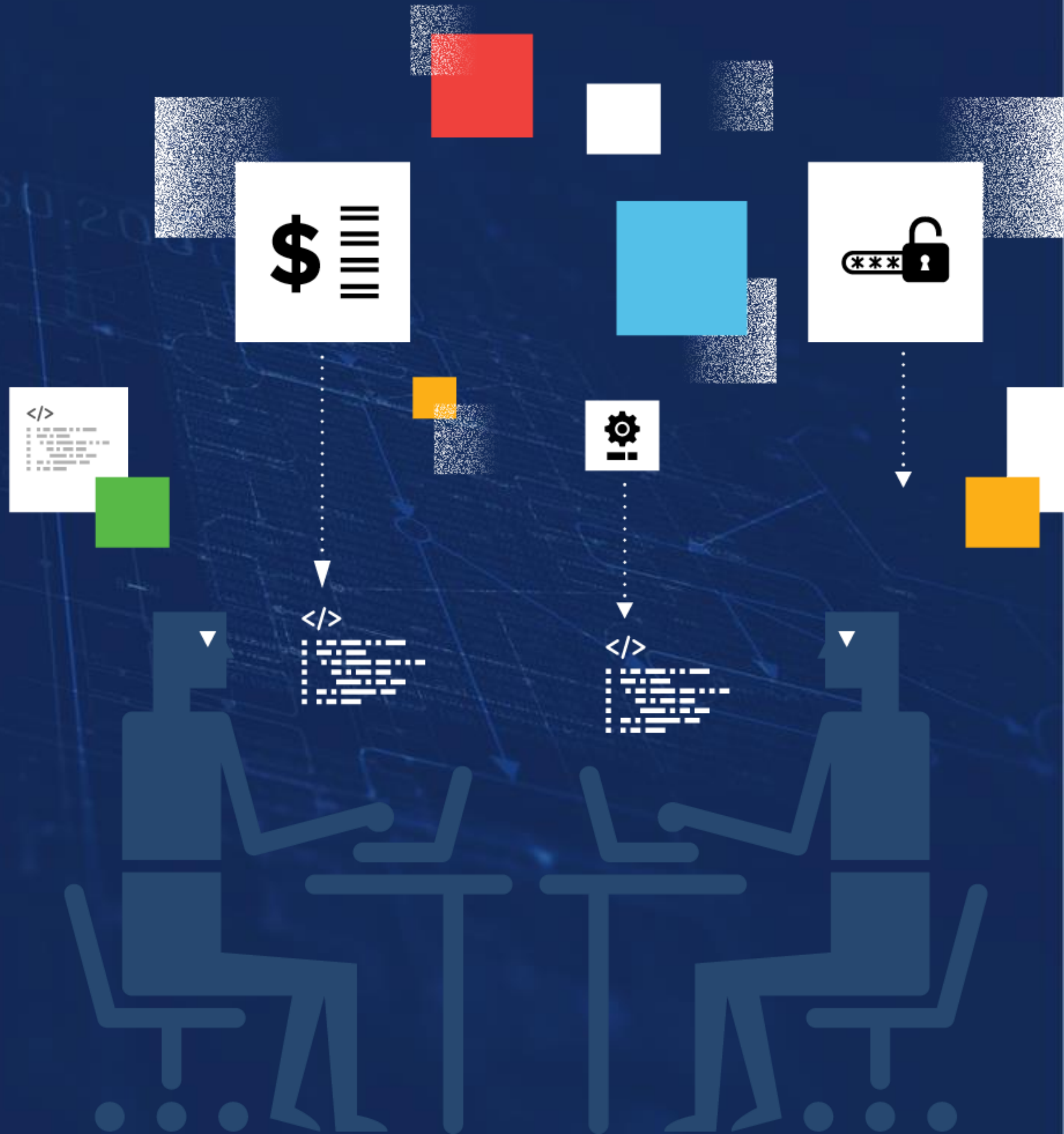
02 Breach Impact and Costs

03 Becoming Cyber Resilient

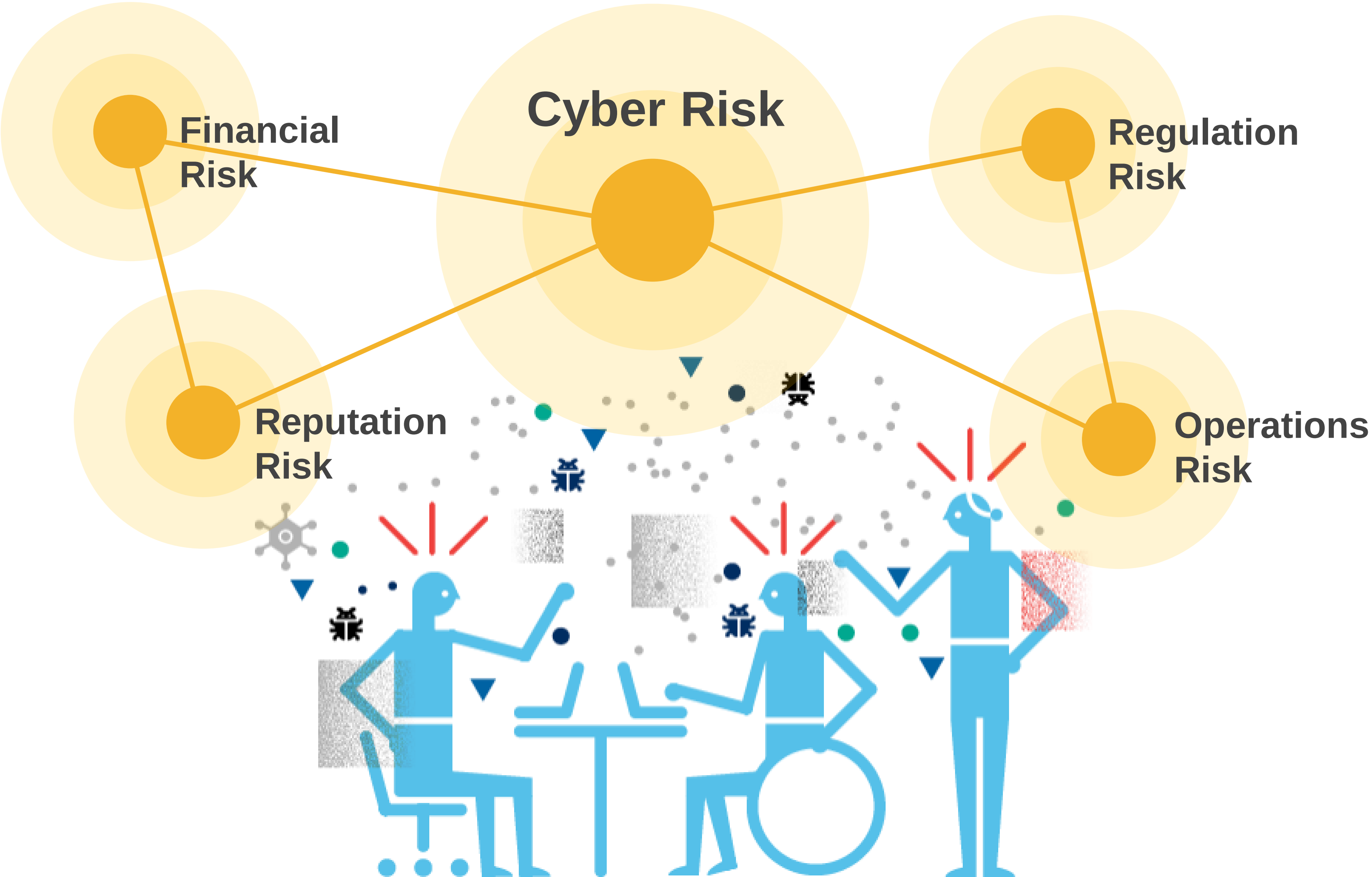
04 Q&A

The State of Cyber Risk

Trends across industries



Cyber risk is top of mind for everyone



90%

of organizations view cyber security as a **top 5 risk** to their organization

The modern threat landscape makes a cyberbreach almost inevitable

Expanding attack surface

- Endpoints
- Network
- Cloud and SaaS
- Users
- Mobile Devices
- IoT

Motivated threat actors

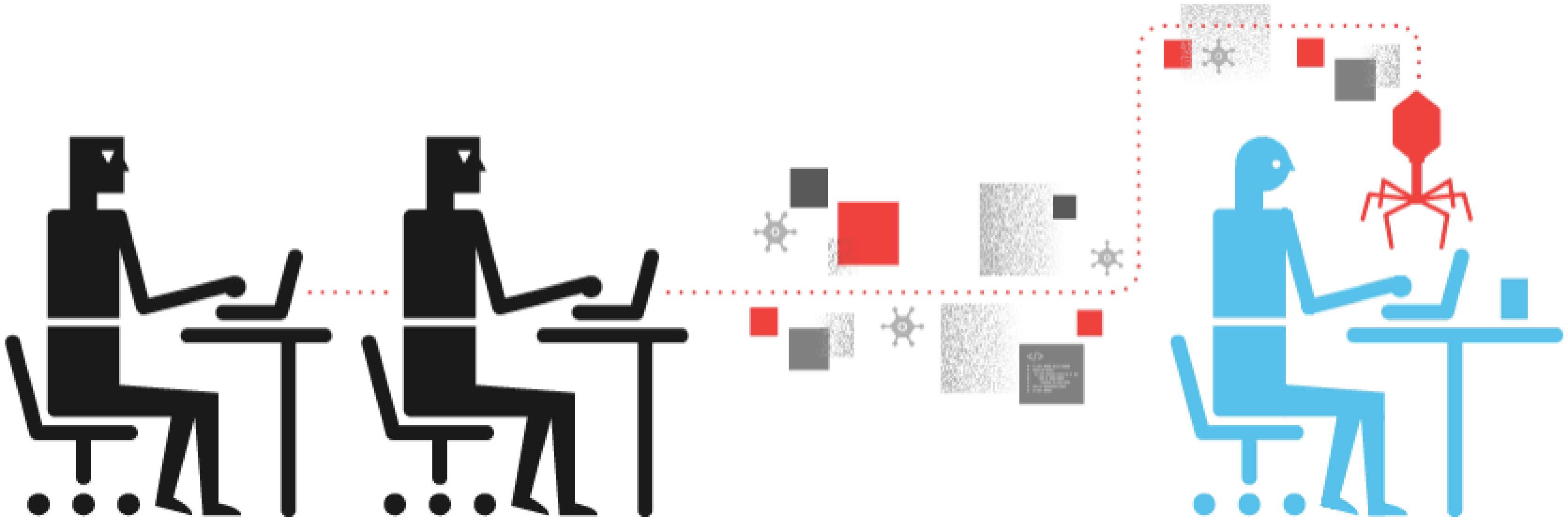
- Malicious insiders
- Terrorists
- Organized crime
- Hacktivists
- Nation states

Sophisticated attack methods

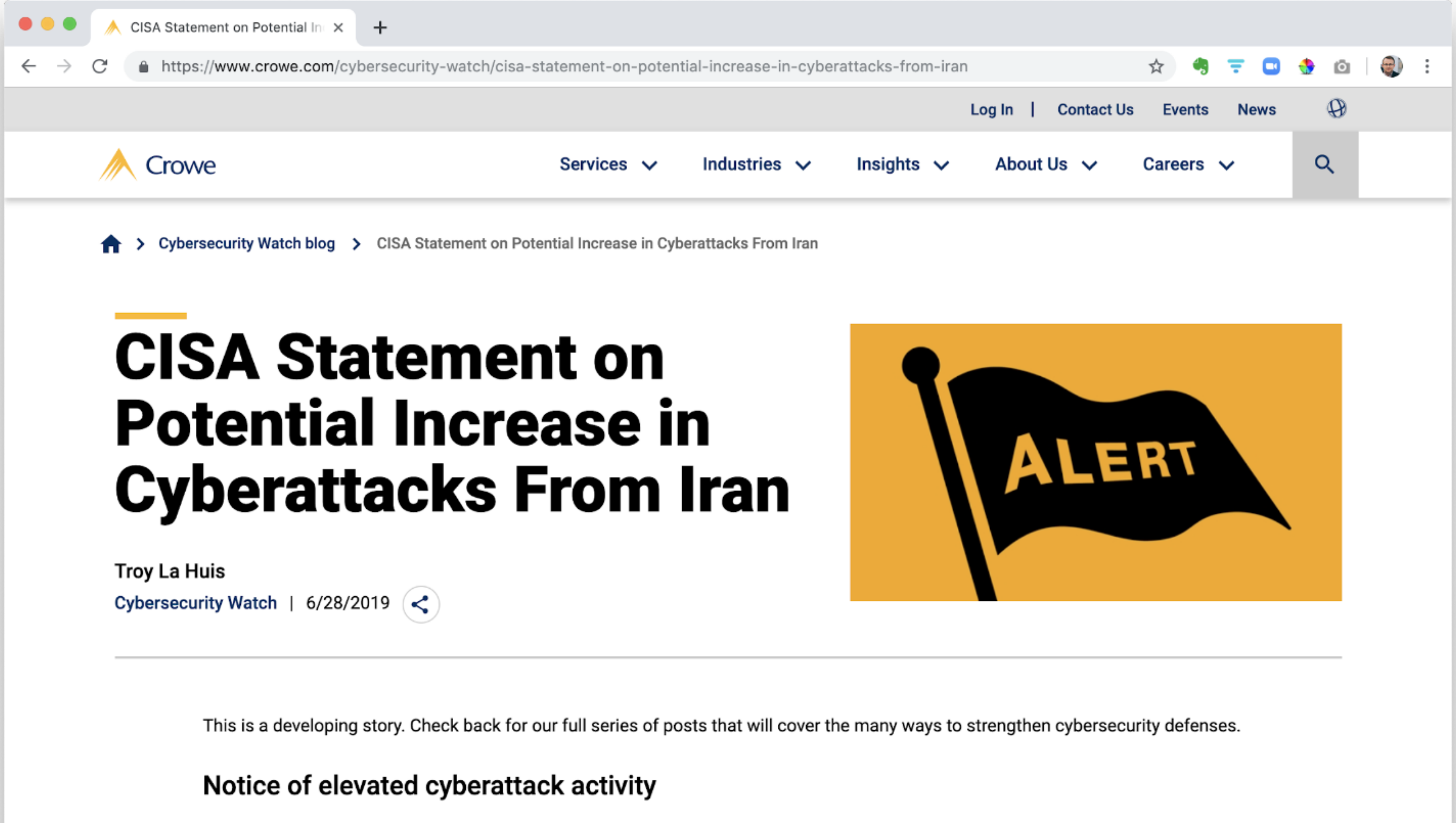
- Spear-Phishing
- Custom Malware
- Zero-Day Exploits
- Social Engineering
- Physical Comprise

1 in 4

odds of experiencing a data breach



EXAMPLE: Iranian attackers attacking US businesses to wipe networks and data



CISA Statement on Potential In
https://www.crowe.com/cybersecurity-watch/cisa-statement-on-potential-increase-in-cyberattacks-from-iran
Log In | Contact Us Events News
Crowe
Services Industries Insights About Us Careers
ALERT

Cybersecurity Watch blog > CISA Statement on Potential Increase in Cyberattacks From Iran

CISA Statement on Potential Increase in Cyberattacks From Iran

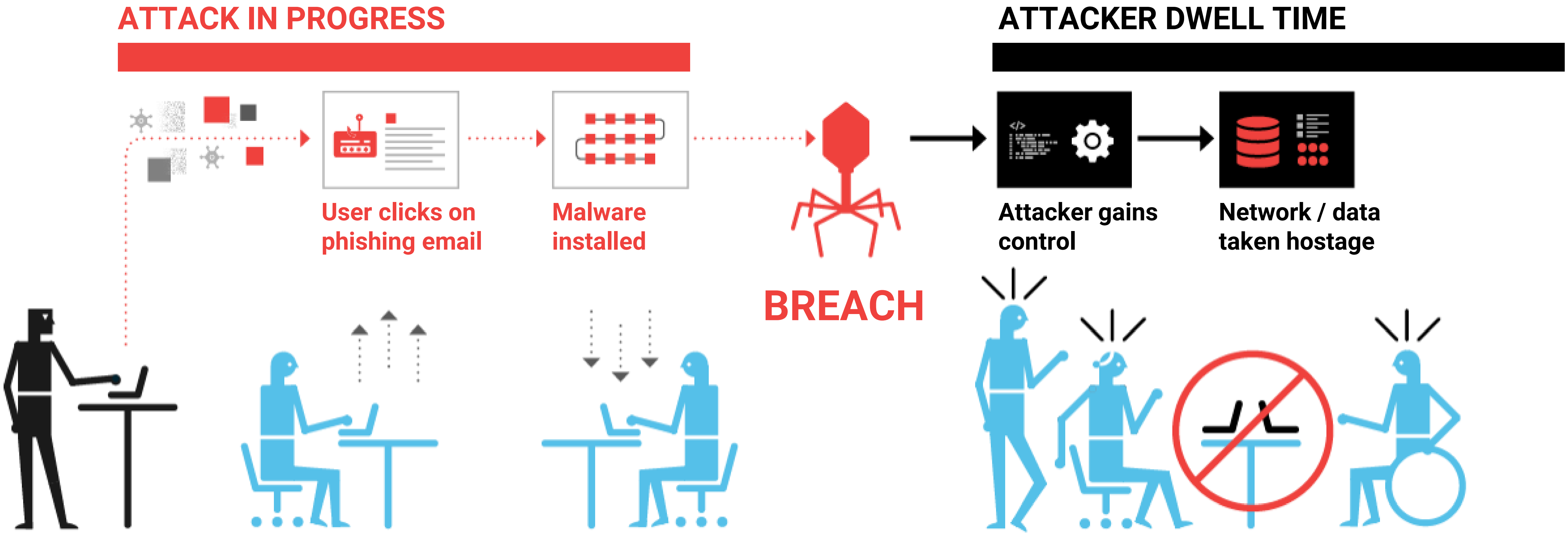
Troy La Huis

Cybersecurity Watch | 6/28/2019

This is a developing story. Check back for our full series of posts that will cover the many ways to strengthen cybersecurity defenses.

Notice of elevated cyberattack activity

EXAMPLE: Ransomware



ATTACK IN PROGRESS

User clicks on phishing email

Malware installed

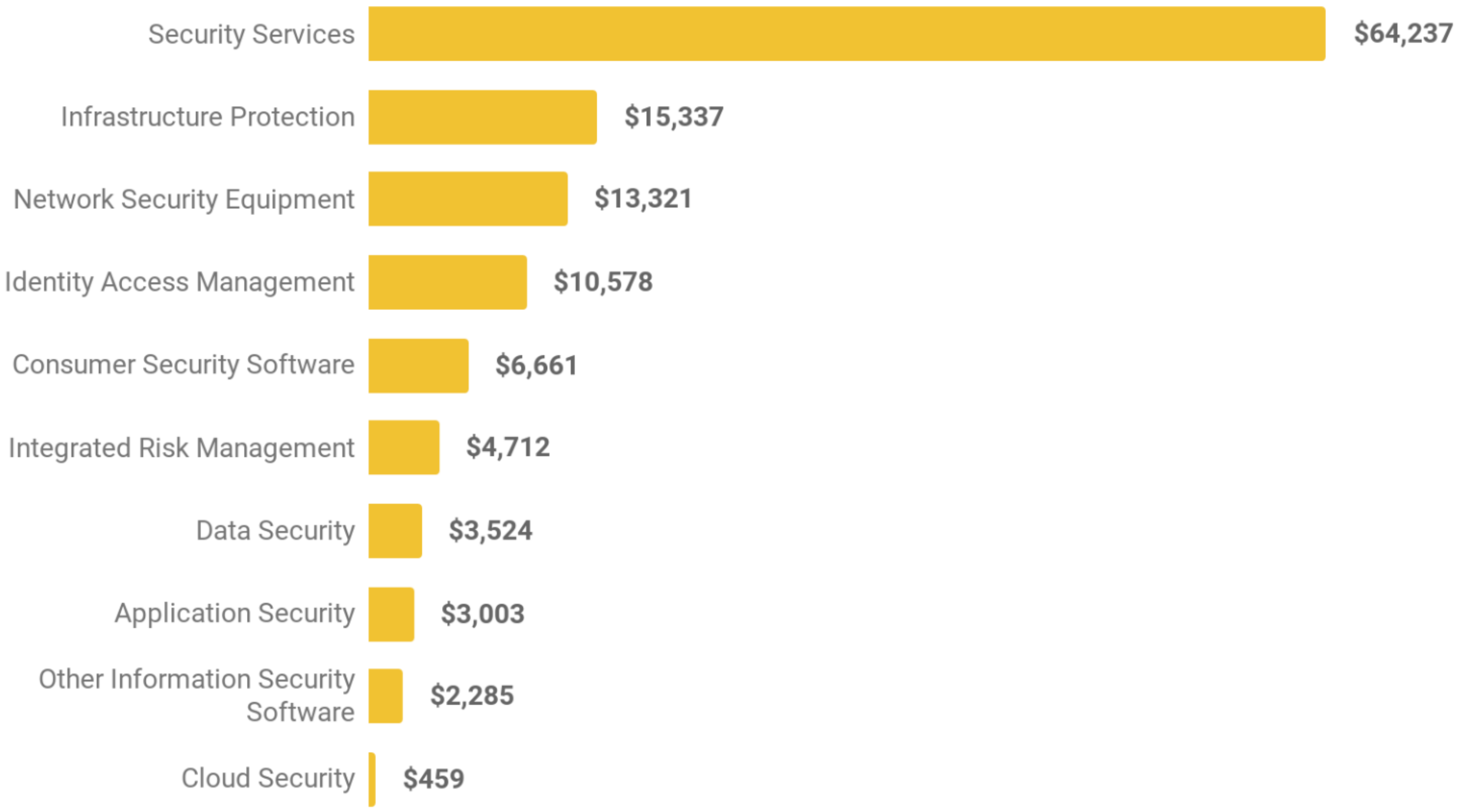
BREACH

ATTACKER DWELL TIME

Attacker gains control

Network / data taken hostage

Cyberbreaches are on the rise despite billions invested in cybersecurity controls



$124B

Worldwide Information Security Spending in 2019 (Gartner)

Cybersecurity investments have historically been focused on prevention and compliance

What security controls do we need to prevent a cyberbreach and **check the box**?

The data tells us that this prevention and compliance investment strategy isn't enough

$124B

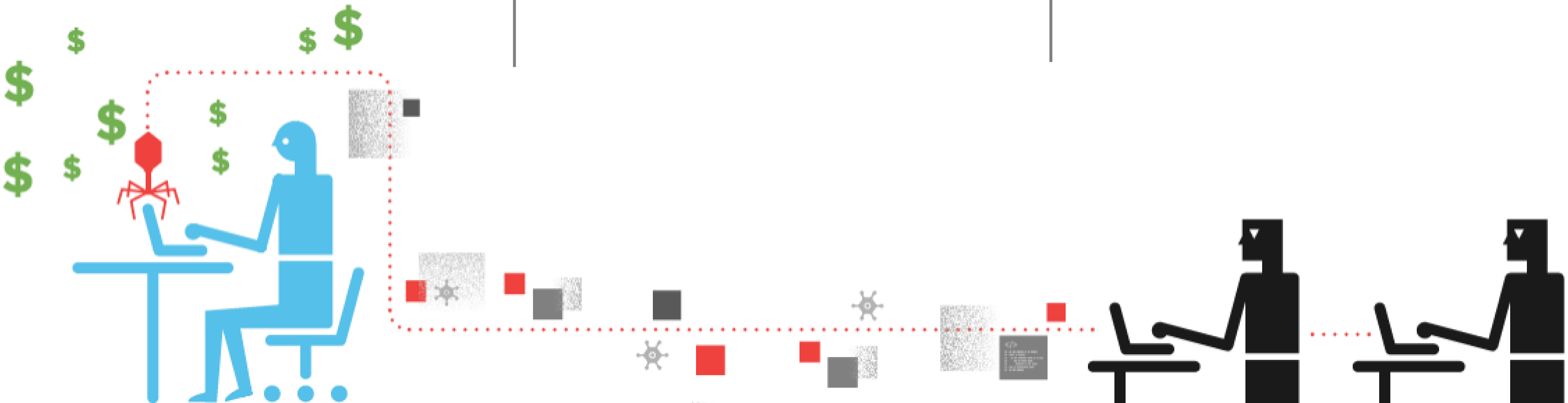
Worldwide Information Security Spending in 2019 (Gartner)

1 in 4

Odds of experiencing a cyberbreach (Ponemon)

$3.8M

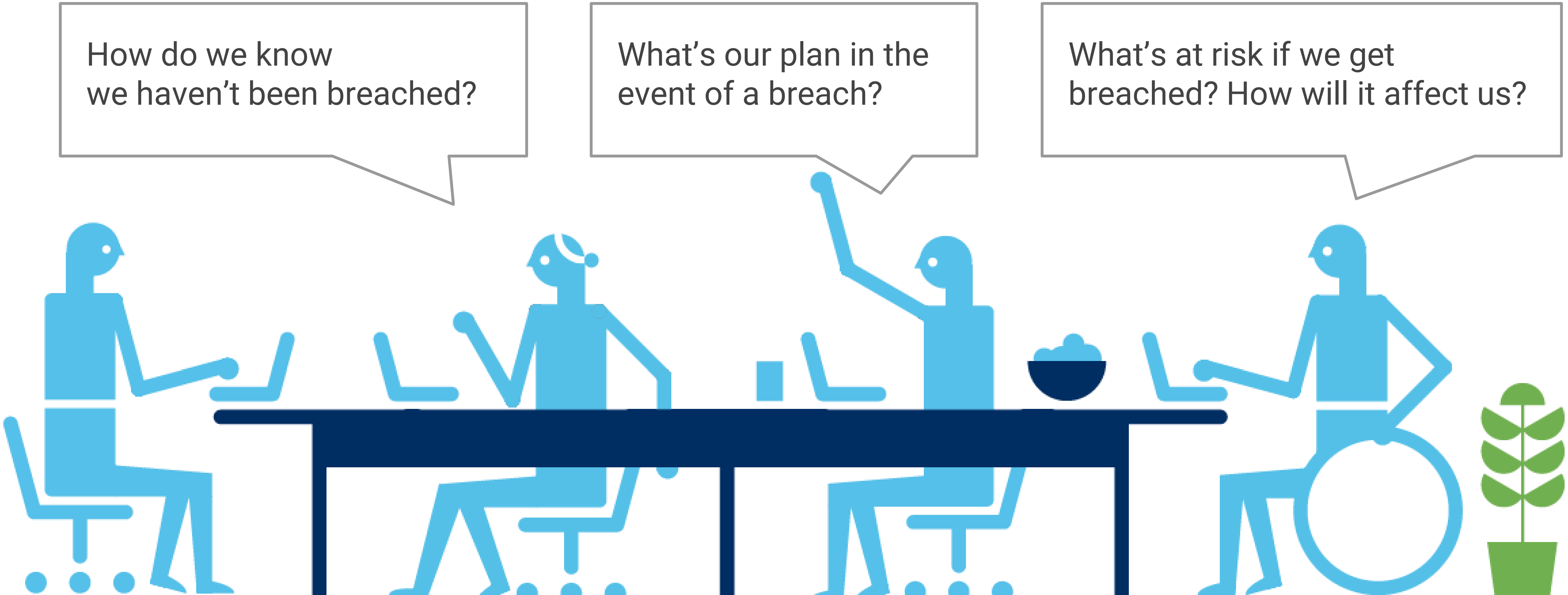
Global average cost of a cyber breach (Ponemon)



A new “cyber resilience” mindset is needed – investing to minimize breach impact

How do we make sure a cyberbreach never causes us to **stop serving customers**?

Questions boards are starting to ask their IT/Security leaders



How do we know we haven't been breached?

What's our plan in the event of a breach?

What's at risk if we get breached? How will it affect us?

Minimizing Breach Impact

Breaking down the costs of a cyberbreach and the keys to minimizing breach impact

Everyone knows that cyberbreaches can be costly. Here’s a breakdown of the typical costs:

$3.8M

Global average cost of a cyber breach

$1.45M
Lost Business Costs

- Customer turnover
- Increased acquisition cost
- Diminished reputation

$1.23M
Detection and Escalation

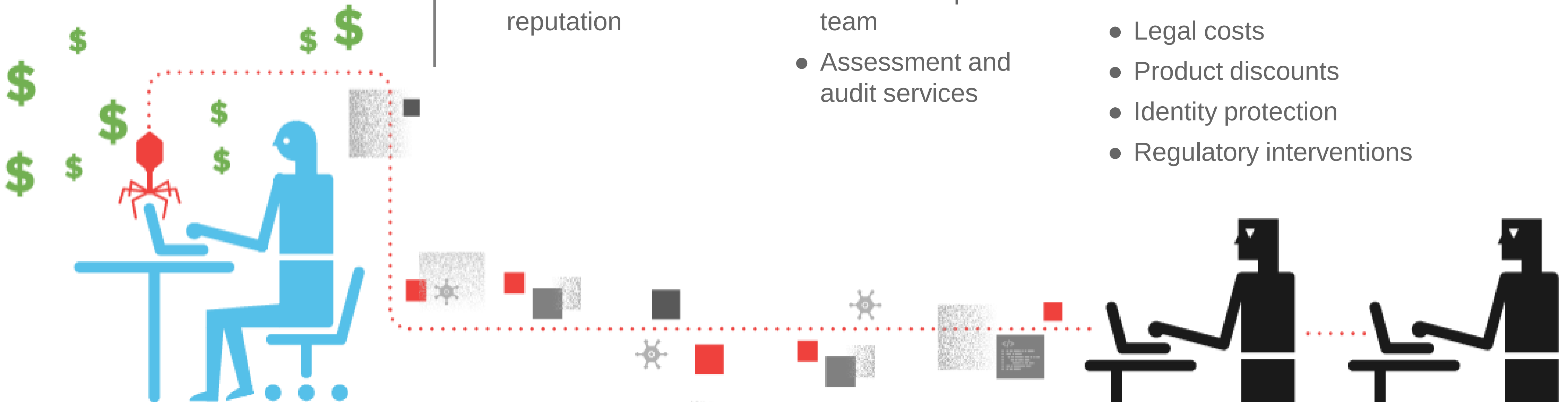
- Forensics
- Root cause determination
- Incident response team
- Assessment and audit services

$1.02M
Post-breach Response

- Help desk
- Inbound communications
- Remediation
- Legal costs
- Product discounts
- Identity protection
- Regulatory interventions

$0.16M
Notification

- Disclosure of data breach to victims and regulators

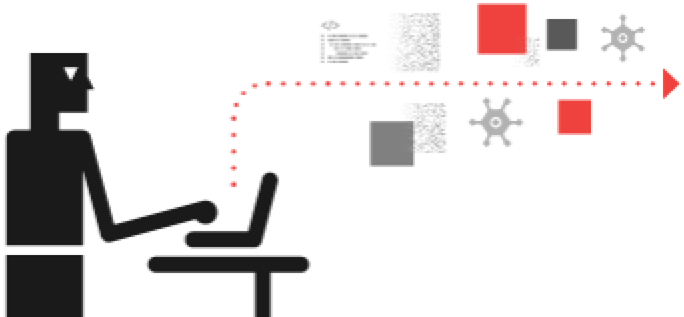


It’s not just a problem for large corporations

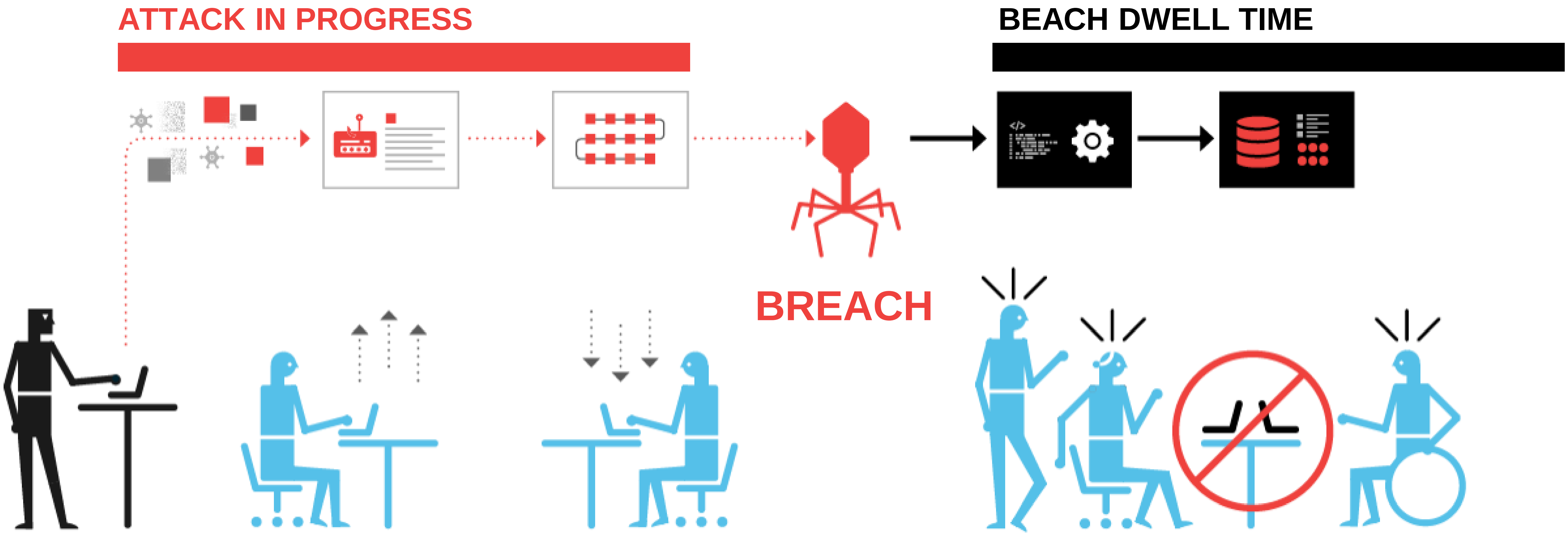
Hackers Breached Virginia Bank Twice in Eight Months, Stole $2.4M

Lake City, Florida votes to pay $460K ransom to hackers to unlock data

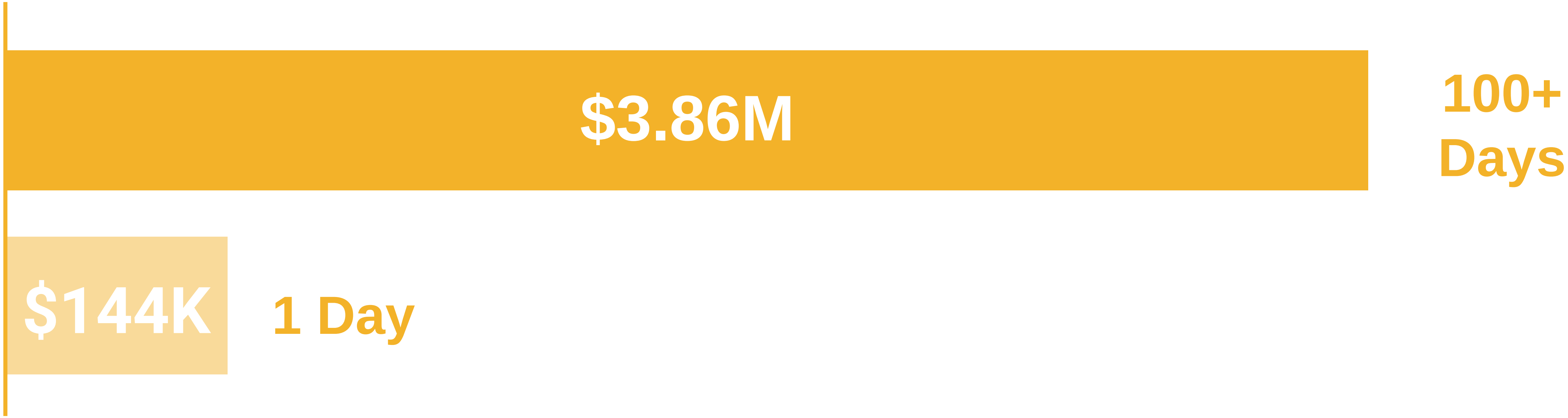
Cyberattacks now cost small businesses $200,000 on average, putting many out of business



The big problem is breach dwell time – how long it takes to detect and contain a cyberbreach



Studies show the longer the breach dwell time, the higher the cost of the breach

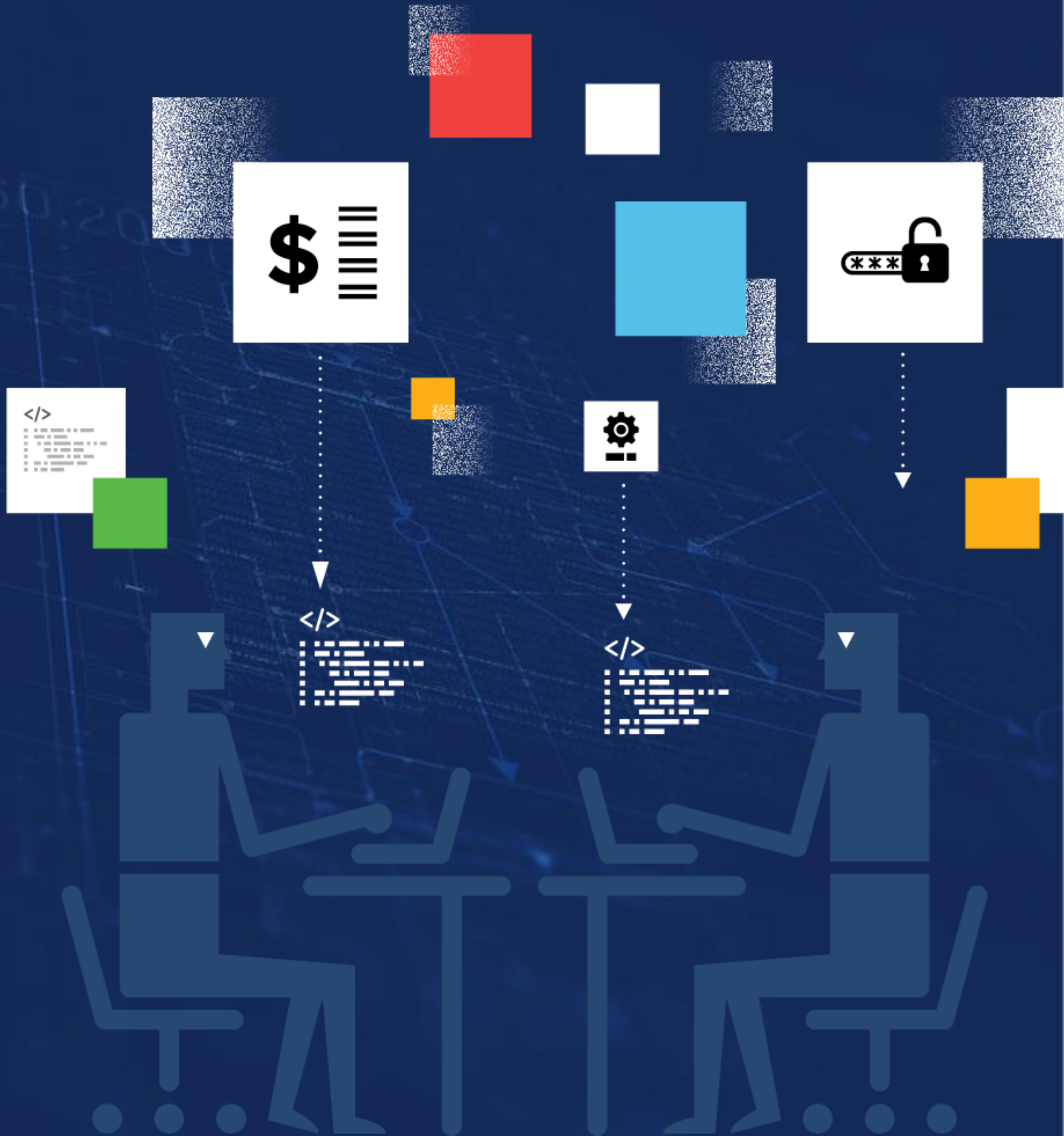


POLL: How long does it take to detect and contain a cyberbreach across all industries?

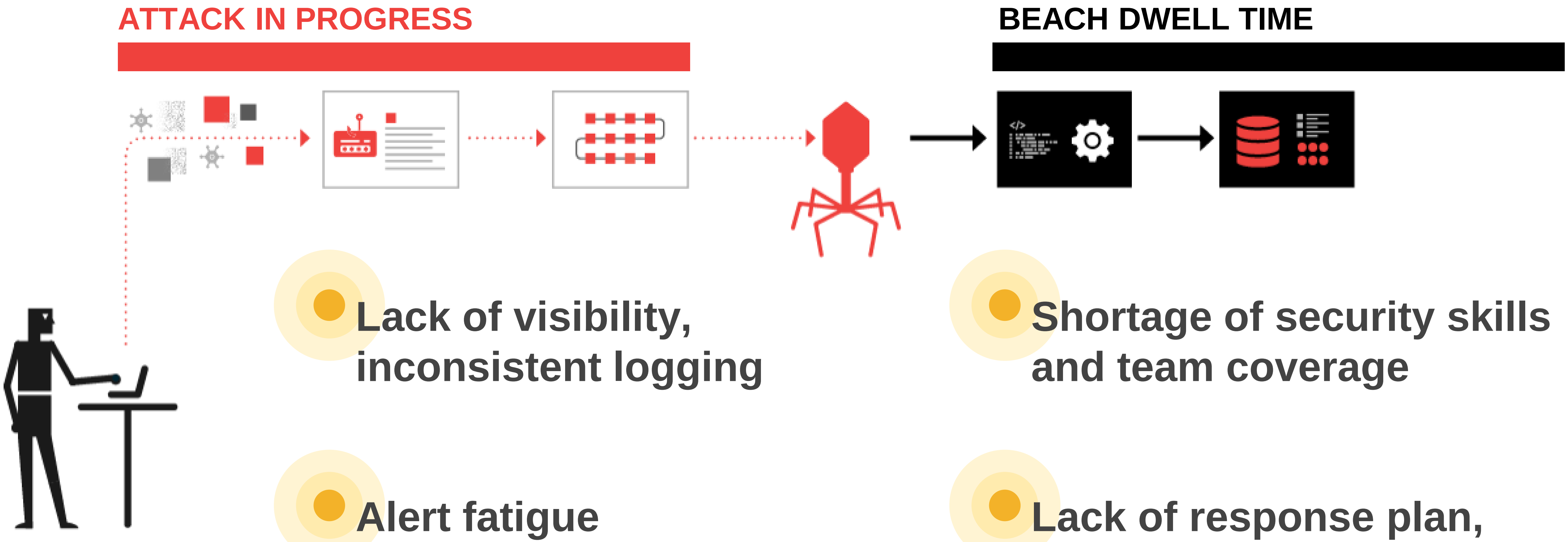
1. 30 days
2. 120 days
3. 266 days
4. 358 days

Number of days it takes to detect and contain a cyberbreach across all industries...

266 days



Why reducing breach dwell time is a challenge



ATTACK IN PROGRESS

BEACH DWELL TIME

- Lack of visibility, inconsistent logging
- Shortage of security skills and team coverage
- Alert fatigue (false positives)
- Lack of response plan, and actionable intelligence

Why reducing breach dwell time is a challenge

Typical moth of activity for a Crowe client

713,677,453 EVENTS
to monitor, collect and correlate

11,293 ALERTS
to filter and prioritize

54 CASES
to investigate and diagnose

4 INCIDENTS
to respond and resolve

Why reducing breach dwell time is a challenge

Typical moth of activity for a Crowe client

713,677,453 EVENTS
to monitor, collect and correlate

11,293 ALERTS
to filter and prioritize

54 CASES
to investigate and diagnose

4 INCIDENTS
to respond and resolve

Becoming Cyber Resilient

Minimizing breach impact and costs with faster detection and response

Going beyond compliance to resilience

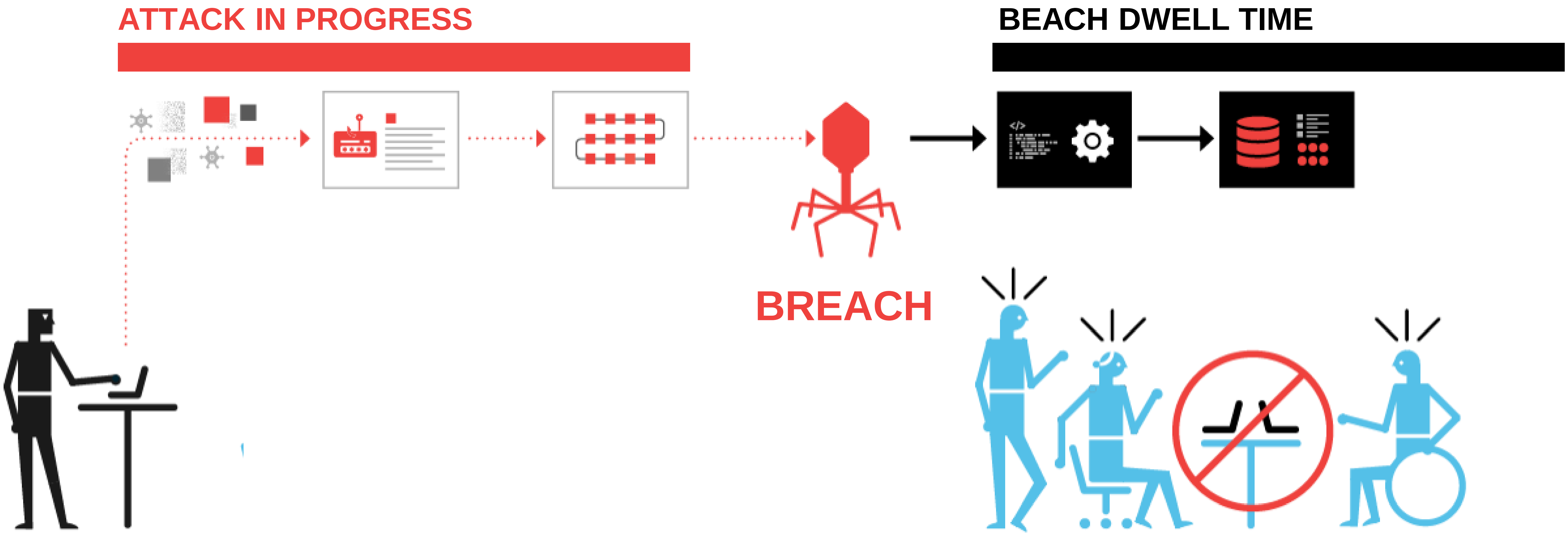
Compliance is the minimum

What security controls do we need to prevent a breach and **check the box**?

Resilience is the goal

How do we make sure a cyberbreach never causes us to **stop serving customers**?

Think about your business? How would it affect you if your network and data was taken hostage?

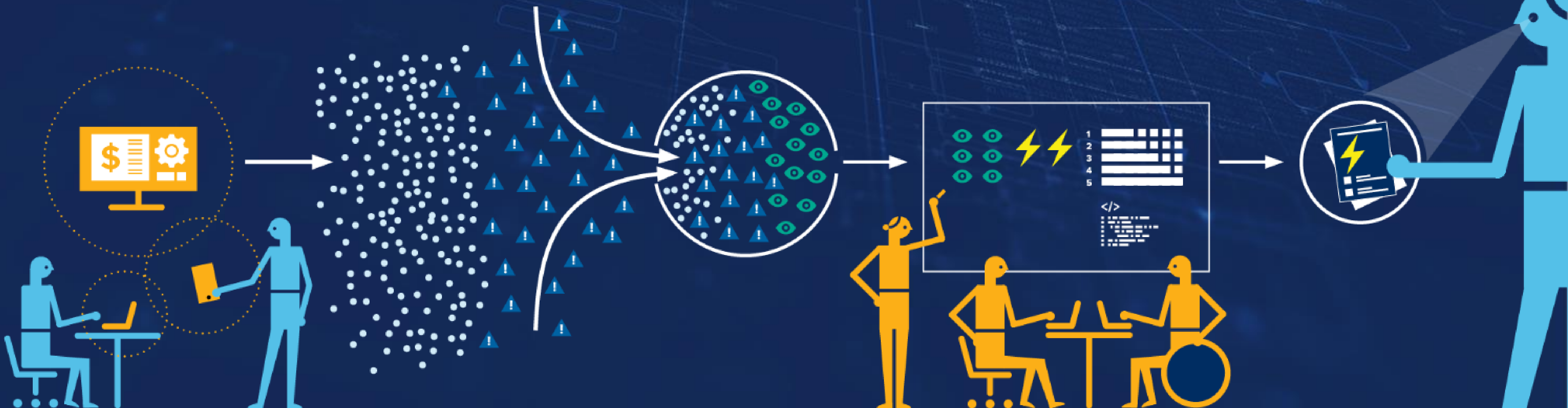


How you monitor, detect, and respond to threats is critical to minimizing breach impact

24/7/365 coverage for monitoring and investigation

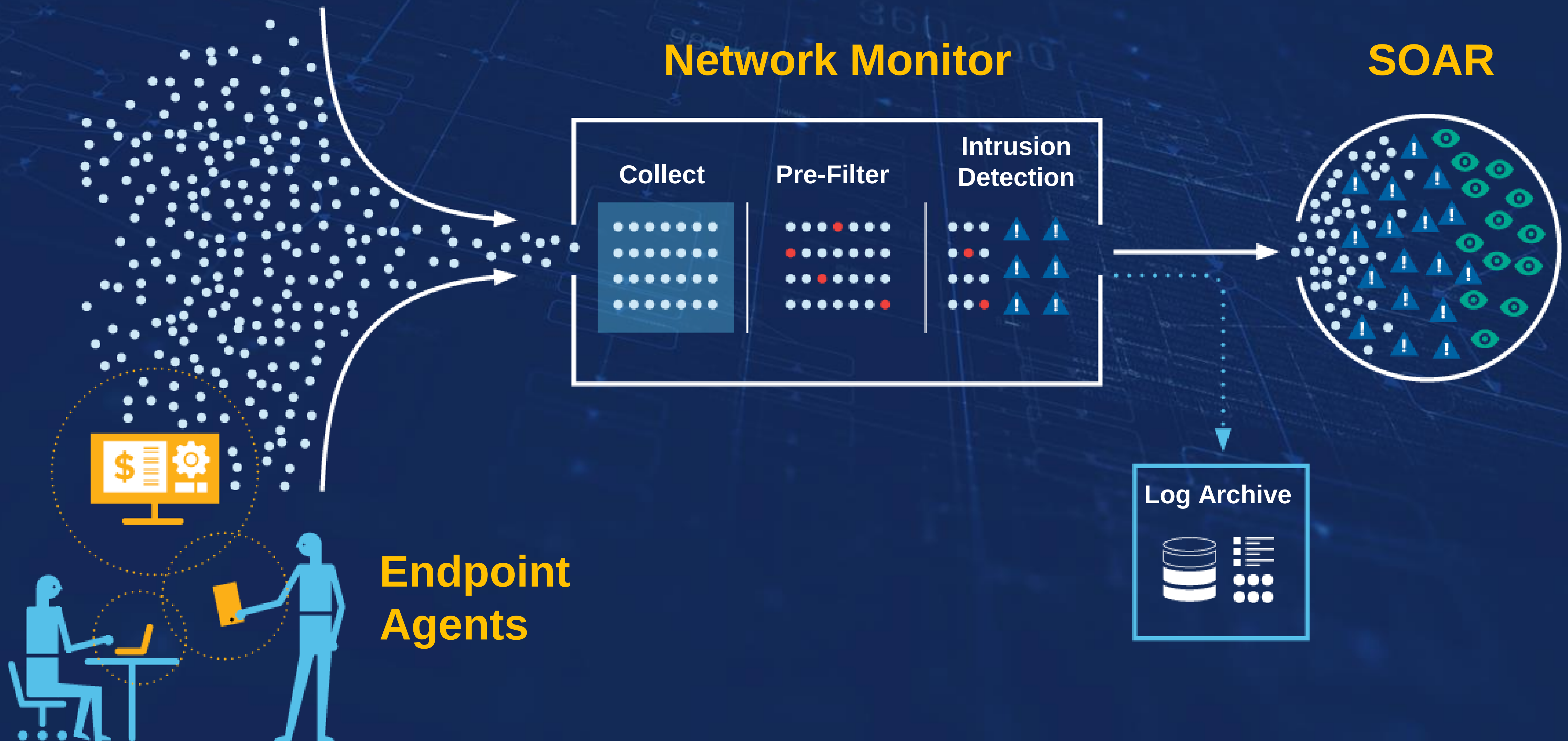
Detect attacks geared to bypass existing controls

Response plan and actionable data to respond to threats

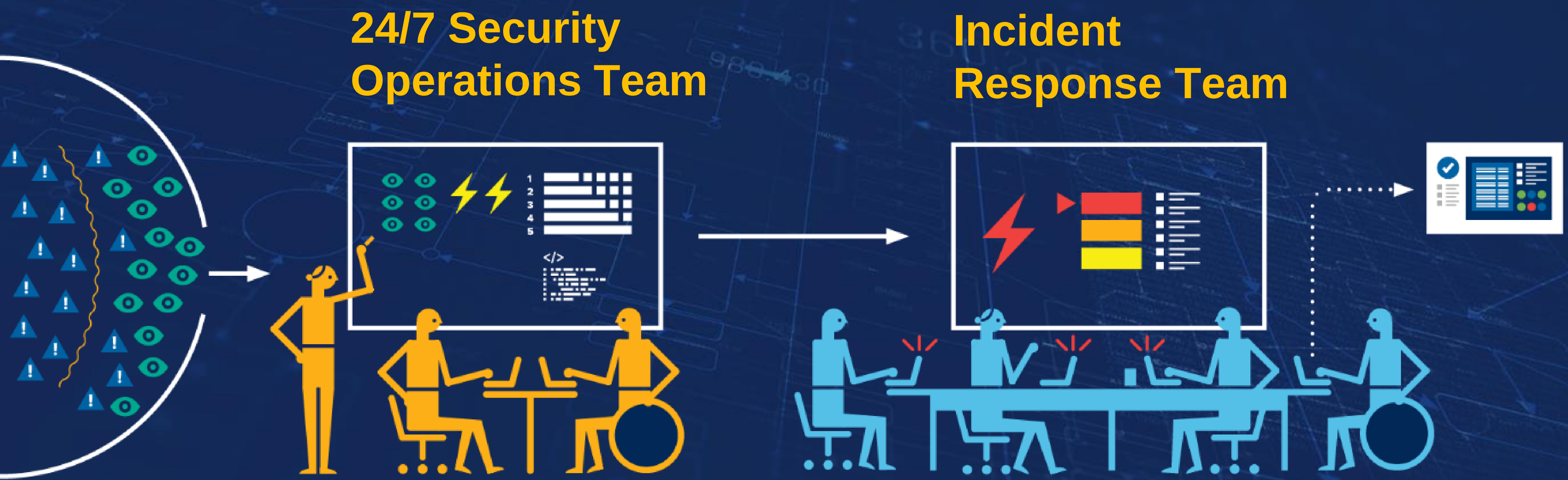


Effective threat detection and response requires the right platform and the right people

Platform – to monitor, collect, filter, and detect



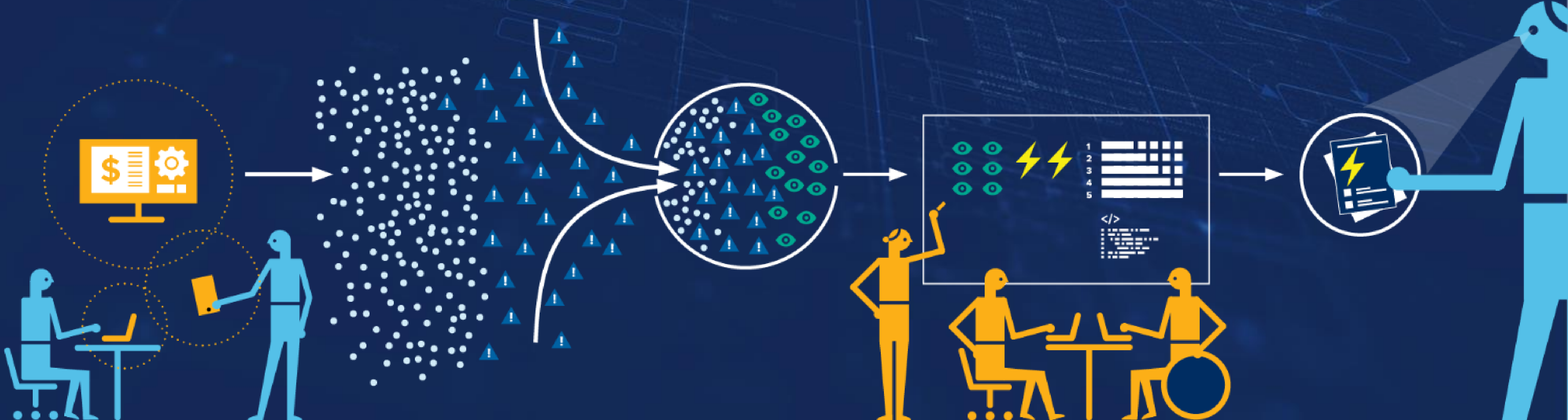
People – to hunt, investigate, and respond



24/7 Security Operations Team

Incident Response Team

How can we afford to invest in the right platform and people for threat detection and response?



Crowe

Ask about Crowe MDR

Leverage Crowe technology and expertise to manage your threat detection and response.

crowe.com/mdr

What we covered

The State of Cyber Risk

Breach Impact and Costs

Becoming Cyber Resilient

Q&A

Crowe

Q&A