



# What every business owner needs to know about Cybersecurity

---



# Speaker Introductions



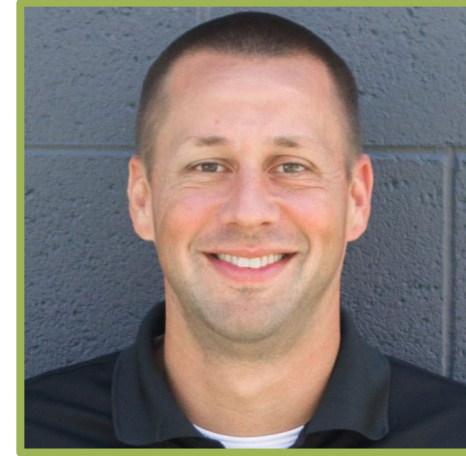
**Jason Bowra**

Scantron Technology Solutions  
Sr. VP of Managed Services



**Dave Koopmans**

Scantron Technology Solutions  
Solutions Engineer Manager



**Jim Peterson**


ConnectWise  
Principal Solution Advisor



# What is Cybersecurity?

*Cybersecurity is the practice of protecting systems, networks and programs from digital attacks.*

*That's true but businesses really need a comprehensive solution that protects businesses information, reputation, and continuity!*



# Cybersecurity

*A compressive protection solution includes more than blocking attacks, it includes:*

- *Cyber Tools*
- *BCDR Solutions*
- *Processes*
- *Assessments*
- *Teams*



# Data Protection Facts

67% of companies believe they will experience a major security breach in the next year (*black hat*)

More than 800,000 cyber crime-related complaints filed in 2022 (FBI.GOV)

58% of business don't have the funds to recover from an attack (*black hat*)

Only 39% of companies claimed they could recovery in 24 hours even with the right equipment (*information-age.com*)

Each week 140,000 hard drives fail (*small business trends*)

34% of backup jobs fail & 38% of restore jobs fail within their required SLA (*Veeam*)



# Cybersecurity Terms

## Attack

An attempt to bypass security measures implemented by an organization

## Incident

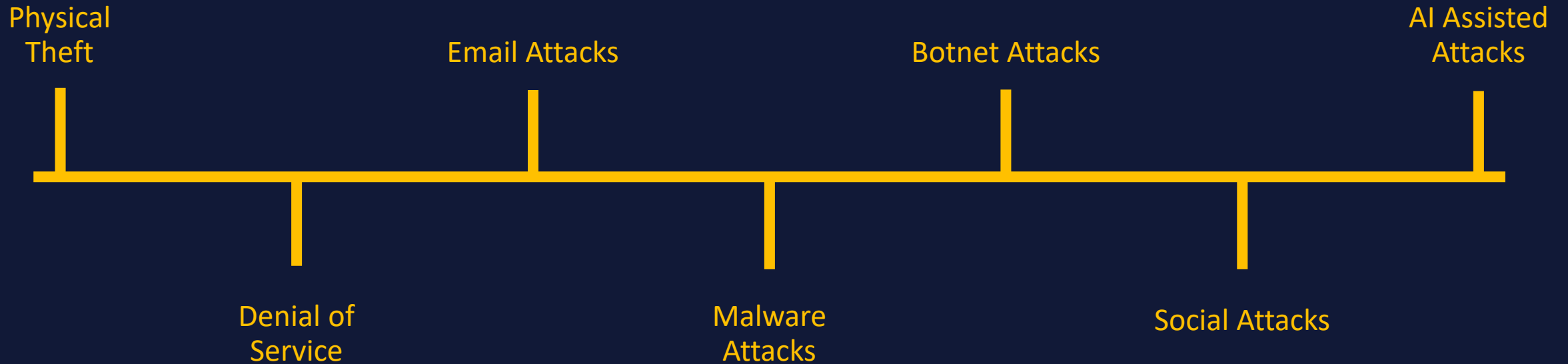
Bypassing one or more of the security measures implemented by an organization

## Breach

Manipulating, extracting, or making data unavailable



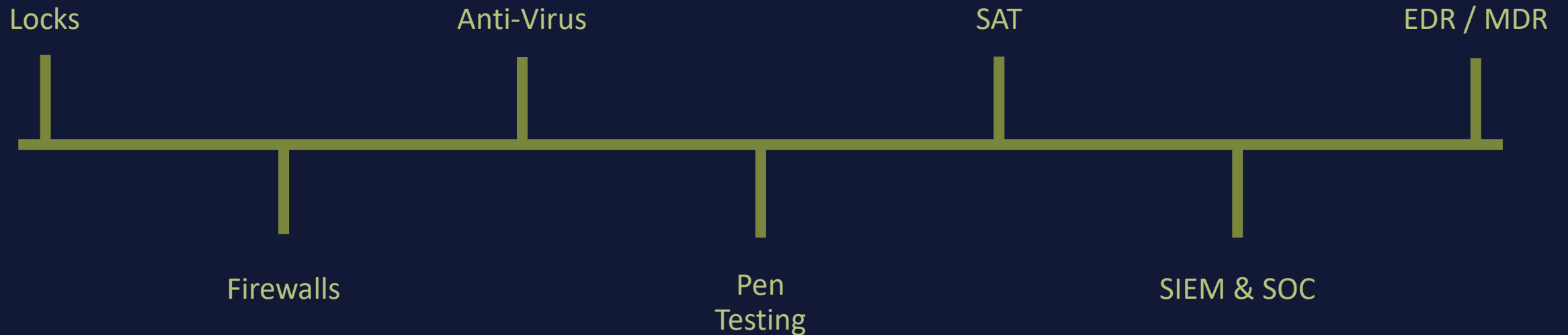
# History of Cyber Threats



**Cyber Attacks Repeat Themselves**



# History of Security Solutions



Close a Door, Open a Window





# Bad Actors

## Basement Bandits



## Nation States



## Organized Crime



**Your data is valuable to Bad Actors, because it's valuable to you!**



# Gaining Access

*Bad actors work to find access into corporate systems through social engineering and testing, and environment vulnerabilities!*

- *Credentials (49%)*

*Solution: Multi-Factor Authentication (MFA)*

- *Phishing (17%)*

*Solution: Security Awareness Training / Email Filter*

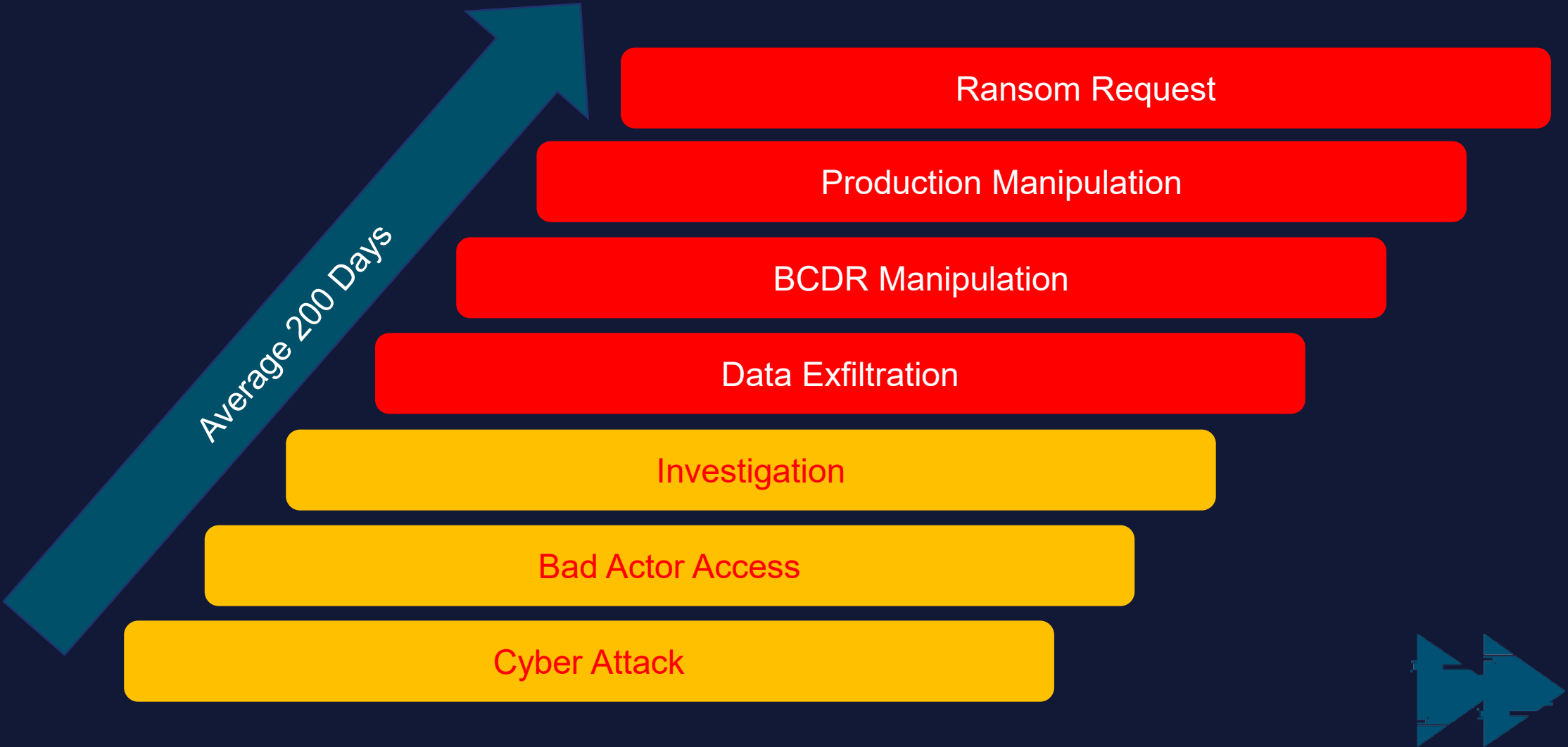
- *Exploits (9%)*

*Solution: System Patching*

\*Verizon 2023 DIBR Report



# Gaining Access is just the start



# What are the driving factors?

*Unfortunately, many SMBs do not believe they are at risk from cyber attacks because they are 'too small'. There is no 'too small', if you have valuable data then you are a target!*

- *Financial (95%)\**
- *Espionage (4%)\**
- *Ideology (>1%)\**
- *Grudge (>1%)\**
- *Other (>1%)\**

**\$10.3 Billion in 2022\*\***

\* Verizon 2023 DIBR Report  
\*\* FBI – Internet Crime Report





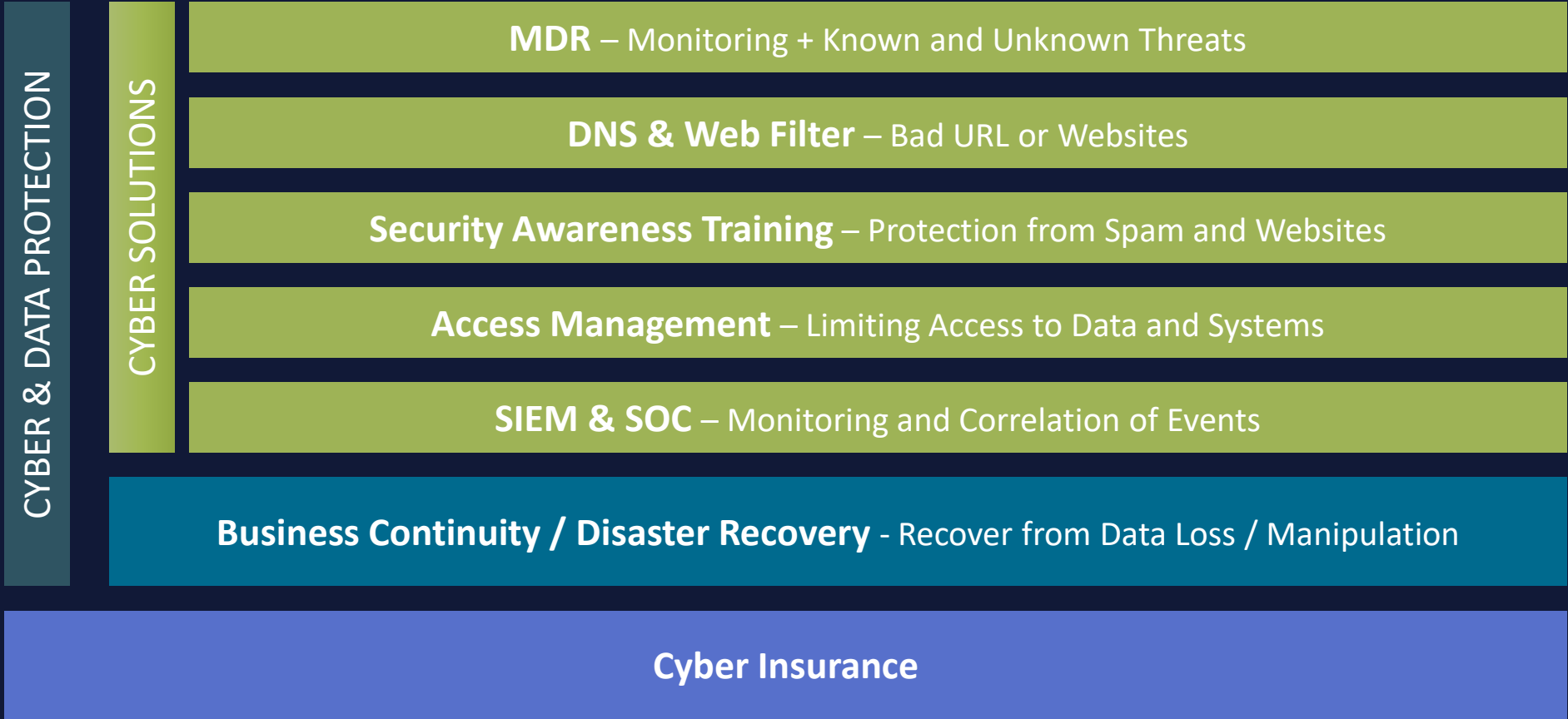
# What about AI?

*AI turns anyone into a sophisticated hacker*

*AI lowers the barrier to attack similar  
to Ransomware as a Service (RaaS)*



# Cybersecurity Layering Options



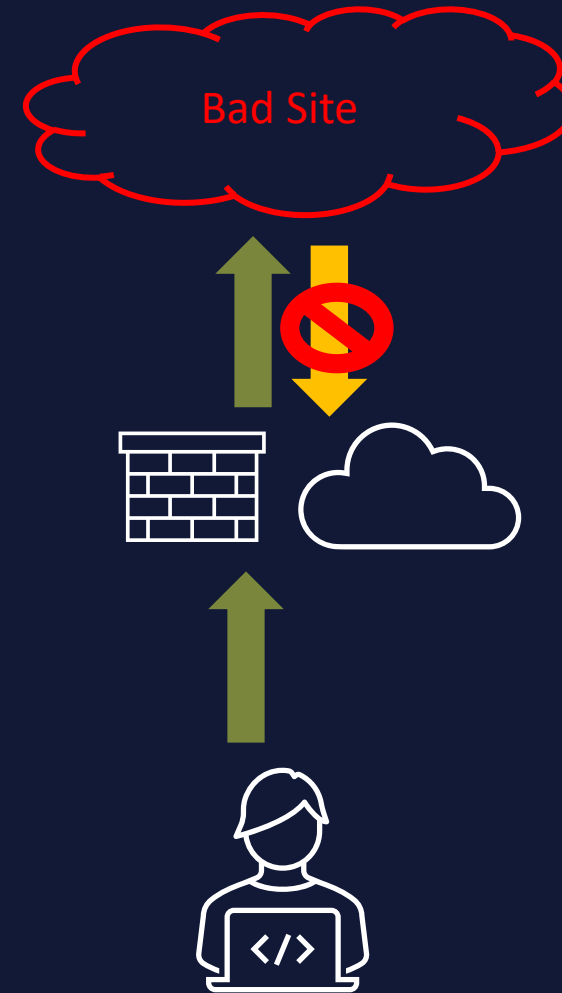
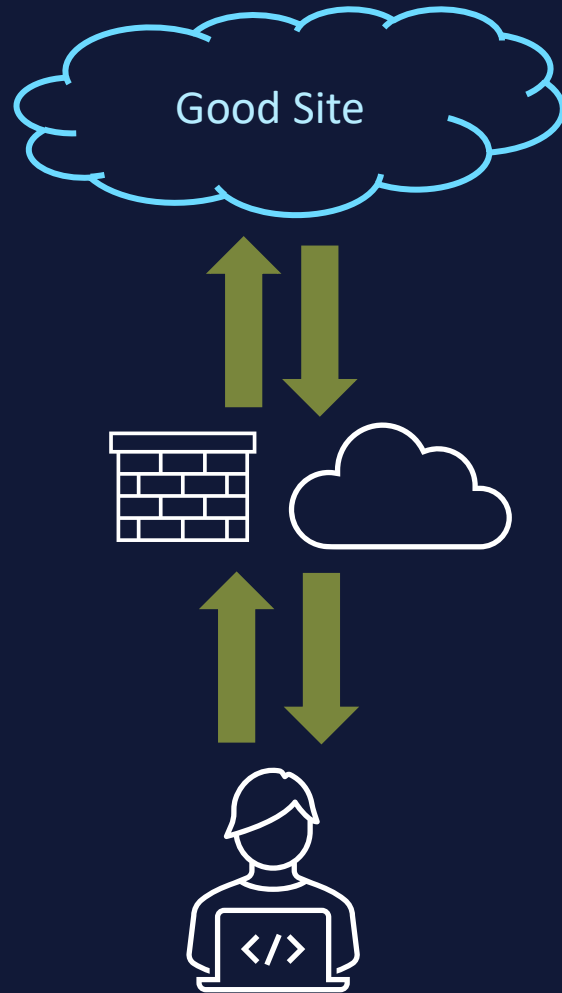
# Front Line: Managed Detection and Response

*A few terms to help understand MDR*

- *AV: Endpoint Software that stops known threats*
- *EDR: Endpoint Software that stops known and unknown threats*
- *MDR: EDR Monitored and Managed 24x7x365*
- *SOC: Security Operations Center, the team monitoring and managing*



# DNS & Web Filtering





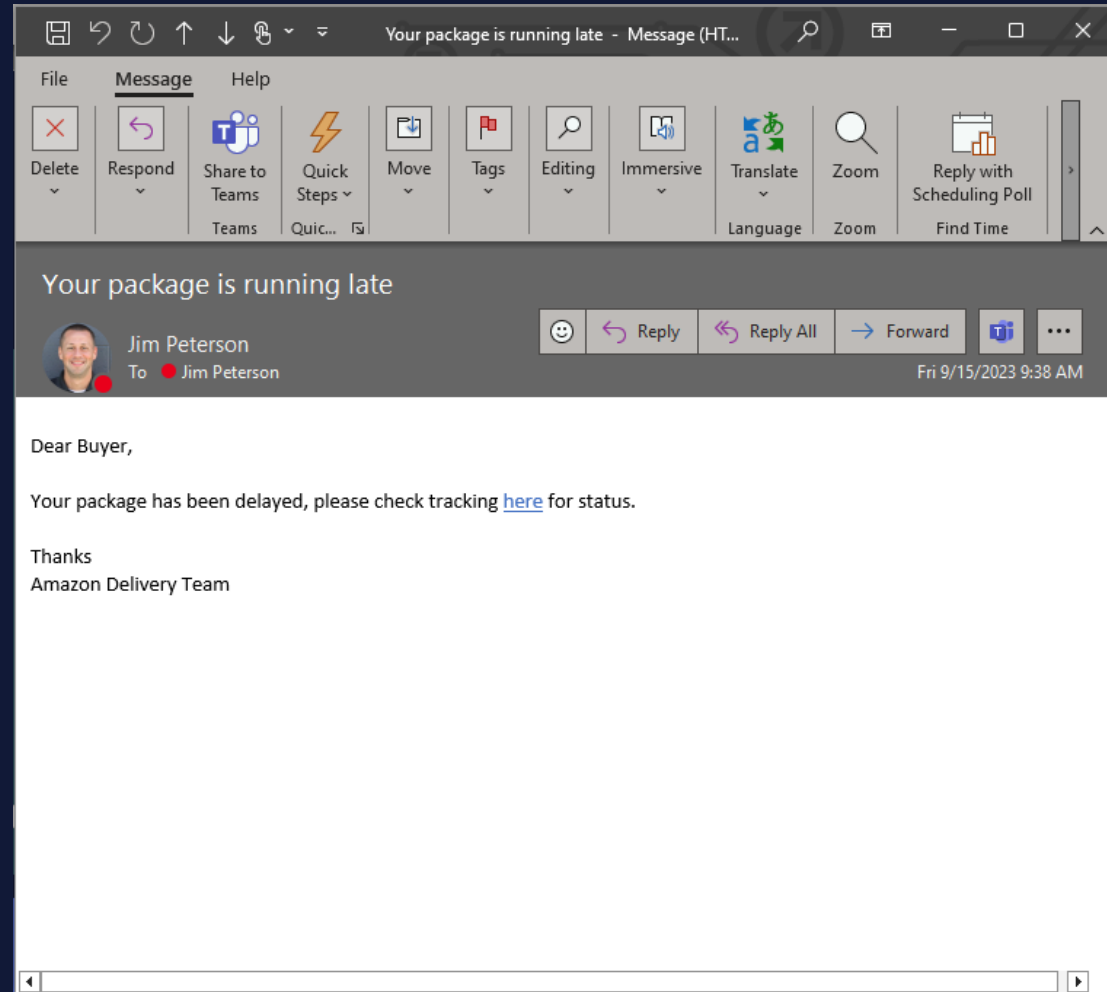
# Security Awareness Training

## Education

SAT focuses on bringing awareness to common and uncommon security threats. From phishing & smishing to wire transfer fraud, SAT helps individuals spot threats.

## Testing

As part of the education process, SAT has testing options to help re-enforce education. By sending fake messages that have common threats, employees can spot them and report them.



# Access Management

## IAM vs PAM

*Identity and Access Management typically revolves around people,  
Privileged Access Management typically revolves around systems*

### Primary Goals

1. Identify who is trying to do something
2. Identify if they are allowed to do it
3. Make this all manageable
4. Audit access and changes



# SIEM & SOC in Action

## Business Example

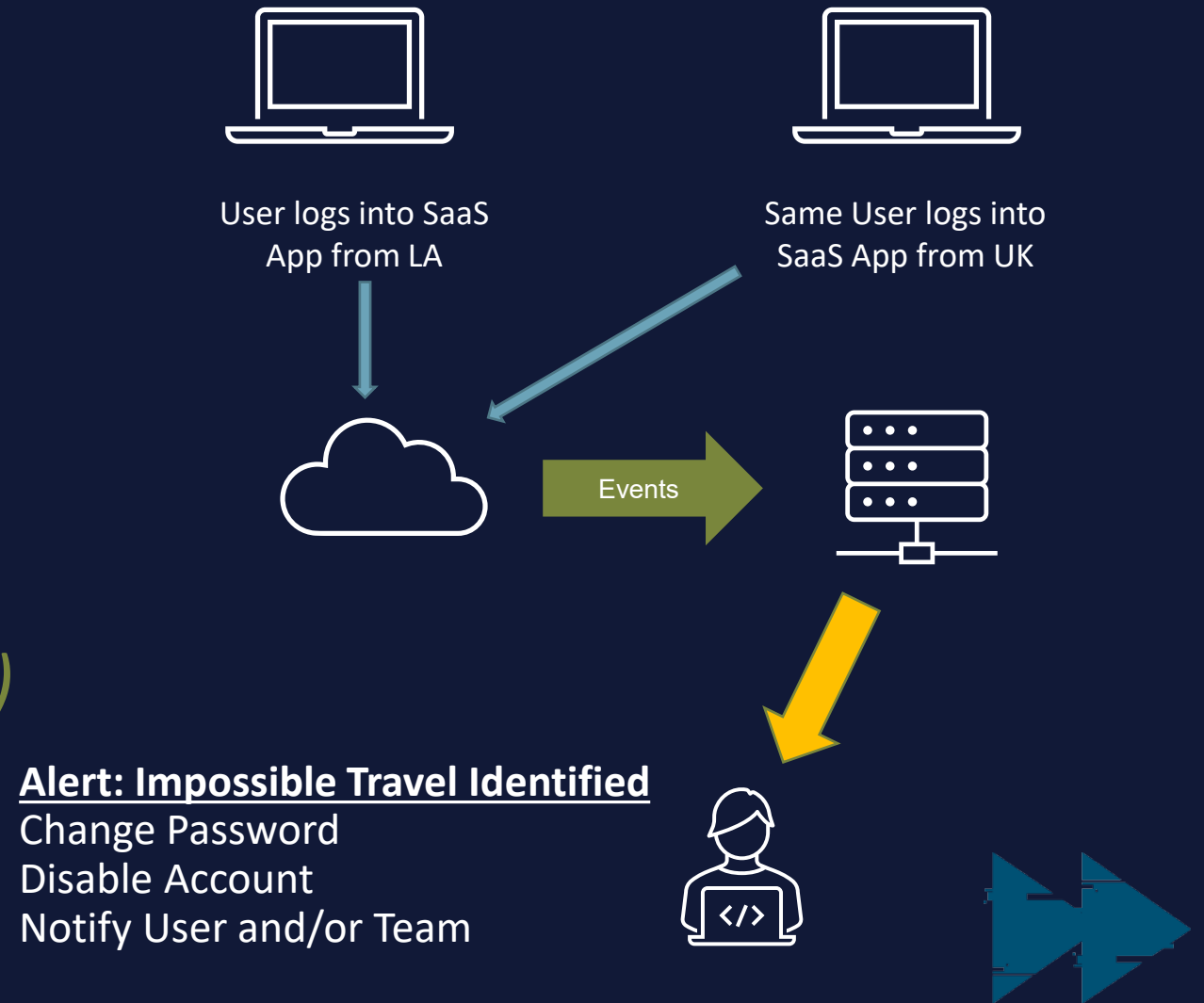
25 – Users

5 – Servers

3 – Sites

2 – SaaS Applications



*= ~430 Events per Second (EPS)*





# What is BCDR?

*Business Continuity and Disaster Recovery (BCDR) is a solution that combines technology, processes, and people to ensure that a business can continue their operations (BC) and recover from a disaster (DR) in a manner that supports their business needs!*



# Why do we care about BCDR?

*BCDR ensures that you can recover your environment when all else fails!*



## Backup is not enough

Having a copy of your data does not help figure out who does what and when



## Last Line of Defense

Just because you can eventually recover your data does not mean your business will recover



## Data is Everywhere

Work from anywhere = data everywhere



## Financial Impact

Being shutdown is expensive for short periods of time and business threatening for long timelines



# Working from Anywhere = Data Everywhere



# Wrapping it up!

*Building a comprehensive cyber strategy is critical to ensuring your business-critical data is always protected!*



## Everyone is a Target

Ability and willingness to pay outweighs business size.



## Build a Layered Defense

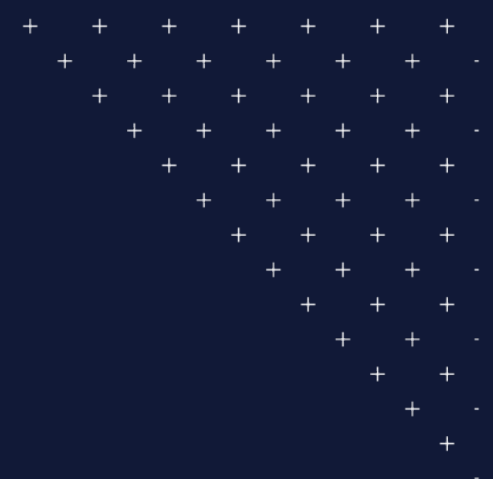
There is no magic bullet for cyber protection. Layers of solutions provide the best defense.



## Know Your Risks

Building a great protection strategy starts with knowing your businesses individual risks.





# Questions?







# Thank You!

