AIT

AccountabilIT

Customer Driven IT Services

Cybersecurity Services

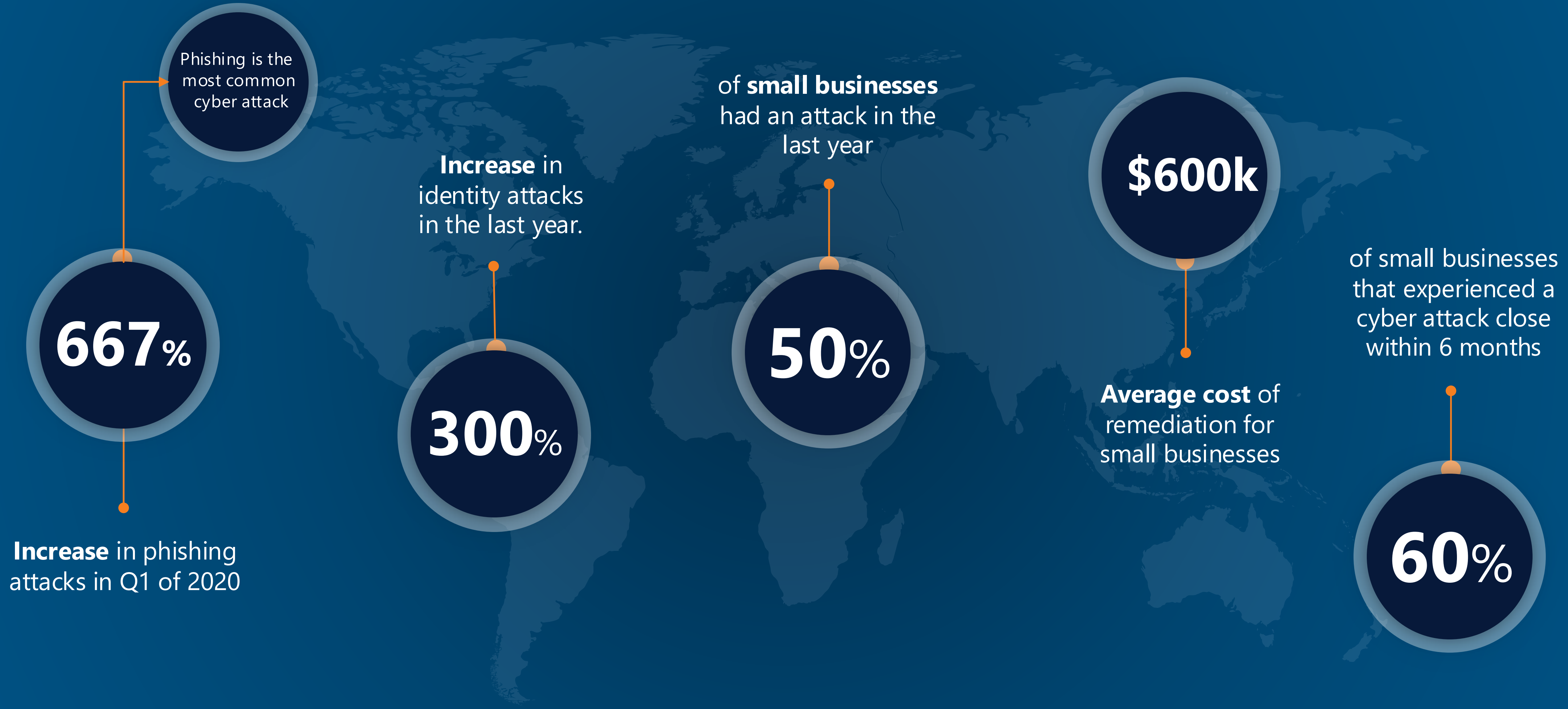
AccountabilIT
Customer Driven IT Services

WELCOME

Our agenda for this presentation includes:

1. Introductions
2. What We See
3. Your Greatest Risks
4. How to Protect Your Business
5. Security Awareness Training
6. Q&A

The Changing Face of Cyber Crime



Phishing is the most common cyber attack

667%

Increase in phishing attacks in Q1 of 2020

300%

Increase in identity attacks in the last year.

50%

of **small businesses** had an attack in the last year

$600k

Average cost of remediation for small businesses

60%

of small businesses that experienced a cyber attack close within 6 months

AccountabilIT
Customer Driven IT Services

Most Common Security Challenges

Increase in Remote Work

Impact of COVID-19 on the workforce has accelerated digital transformation, rapidly and abruptly increasing most companies' attack surfaces.

Security Resistance

Budget and routine resistance to needed security changes. And new security measures or tools.

Lack of Leadership Risk Awareness

Business leaders, lacking a complete view of risks and vulnerabilities, continue to treat security as a business inhibitor due to the lack of a defensible security program that links into business outcomes.

Lack of Clear Security Roadmap

Lack of a prioritized roadmap that clearly links projects and corrective actions to risks, vulnerabilities and the relevant business, technology and environmental drivers.

Understaffed IT Department

Understaffed IT departments are leaving companies vulnerable to attacks. enterprises are struggling to fill security roles due to the time it takes to hire, rising industry salaries, and employee retention issues.

AccountabilIT
Customer Driven IT Services

Your Biggest Risks

AccountabilIT
Customer Driven IT Services

How Bad Actors Get In

Phishing

The cybercriminal poses as a well-known service in the email template to lure the user into clicking on a link.

Top 5 Spoofed Brands:

- Microsoft
- UPS
- Amazon
- Apple
- Zoom

How Bad Actors Get In

Phishing

The cybercriminal poses as a well-known service in the email template to lure the user into clicking on a link.

Top 5 Spoofed Brands:

- Microsoft
- UPS
- Amazon
- Apple
- Zoom

Physical Breach

Security breach of on-site servers, unlocked computers, or corrupted USB flash drives.

How Bad Actors Get In

Phishing

The cybercriminal poses as a well-known service in the email template to lure the user into clicking on a link.

Top 5 Spoofed Brands:

- Microsoft
- UPS
- Amazon
- Apple
- Zoom

Physical Breach

Security breach of on-site servers, unlocked computers, or corrupted USB flash drives.

Business Email Compromise

Techniques used to pose as someone, such as the company CEO, CFO, or the accounts receivable clerk, to fraudulently access a company's system and then pose as that company.

How Bad Actors Get In

Phishing

The cybercriminal poses as a well-known service in the email template to lure the user into clicking on a link.

Top 5 Spoofed Brands:

- Microsoft
- UPS
- Amazon
- Apple
- Zoom

Physical Breach

Security breach of on-site servers, unlocked computers, or corrupted USB flash drives.

Business Email Compromise

Techniques used to pose as someone, such as the company CEO, CFO, or the accounts receivable clerk, to fraudulently access a company's system and then pose as that company.

AccountabilIT
Customer Driven IT Services

What Happens Next?

Ransomware

Vicious malware that locks users out of their devices or blocks access to files until a sum of money or ransom is paid. Ransomware attacks cause downtime, data loss, and possible intellectual property theft.

Data Breach

Allows cybercriminals to gain unauthorized access to a computer system or network and steal the private, sensitive, or confidential personal and financial data of the customers or users contained within

Financial Fraud

Cyber-criminals gain access via phishing emails and viruses, rerouting wire transfers and invoice payments to off-shore accounts.

How to Protect Your Business

AccountabilIT
Customer Driven IT Services

How to Protect Your Business

Multi-factor authentication prevents 99.9% of identity attacks

Multi-Factor Authentication

An electronic authentication method in which a computer user is granted access to a website or application only after successfully presenting two or more pieces of evidence to an authentication mechanism: knowledge, possession, and inherence.

Vulnerability Assessment

The process of identifying, quantifying, and prioritizing the vulnerabilities in a system.

Endpoint Protection

A system for network security management that focuses on network endpoints, or individual devices such as workstations and mobile devices from which a network is accessed.

Security Awareness Training

A formal process for increasing people's security awareness as it relates information security and cybersecurity with the goal of putting proper behaviors in practice and developing a culture of security.

Managed Backups

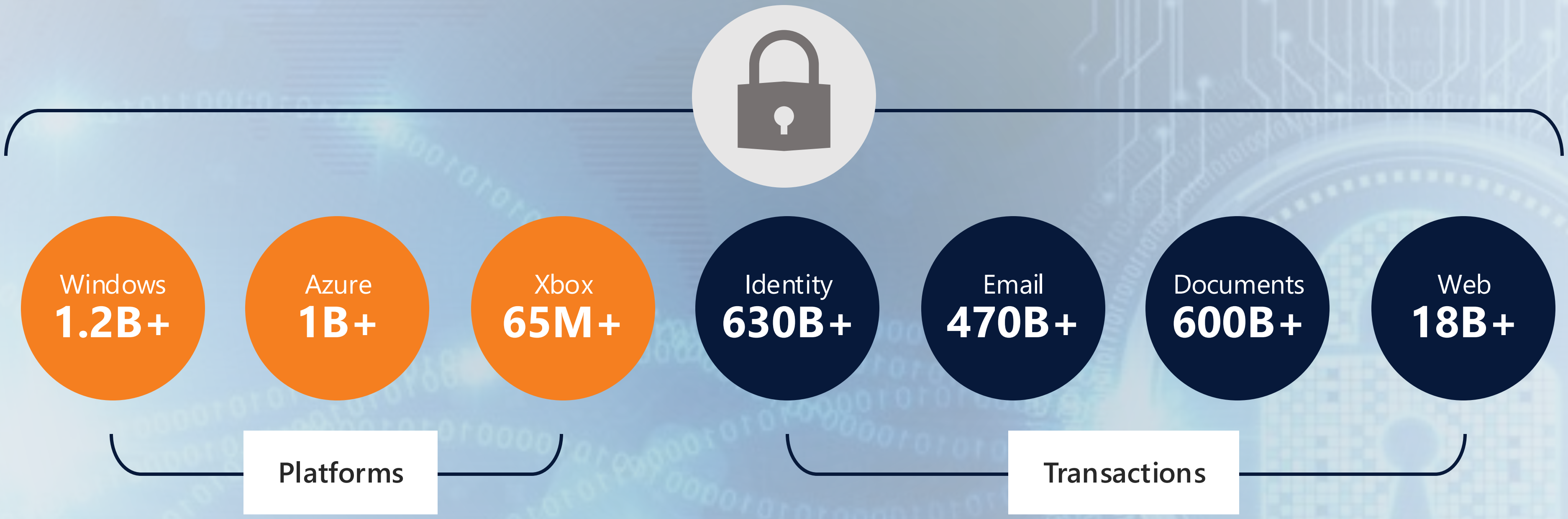
Backups of organizational data that are both secure and off site.

Security Monitoring

A system of people, process and technology that allows for real time alerting of breach activities to stop attacks before they impact the business.

AccountabilIT
Customer Driven IT Services

Microsoft’s unique vantage point on security



Windows 1.2B+

Azure 1B+

Xbox 65M+

Identity 630B+

Email 470B+

Documents 600B+

Web 18B+

Platforms

Transactions

300B

User activities profiled and analyzed in 2019

2.3B

Endpoint vulnerabilities discovered daily

11B

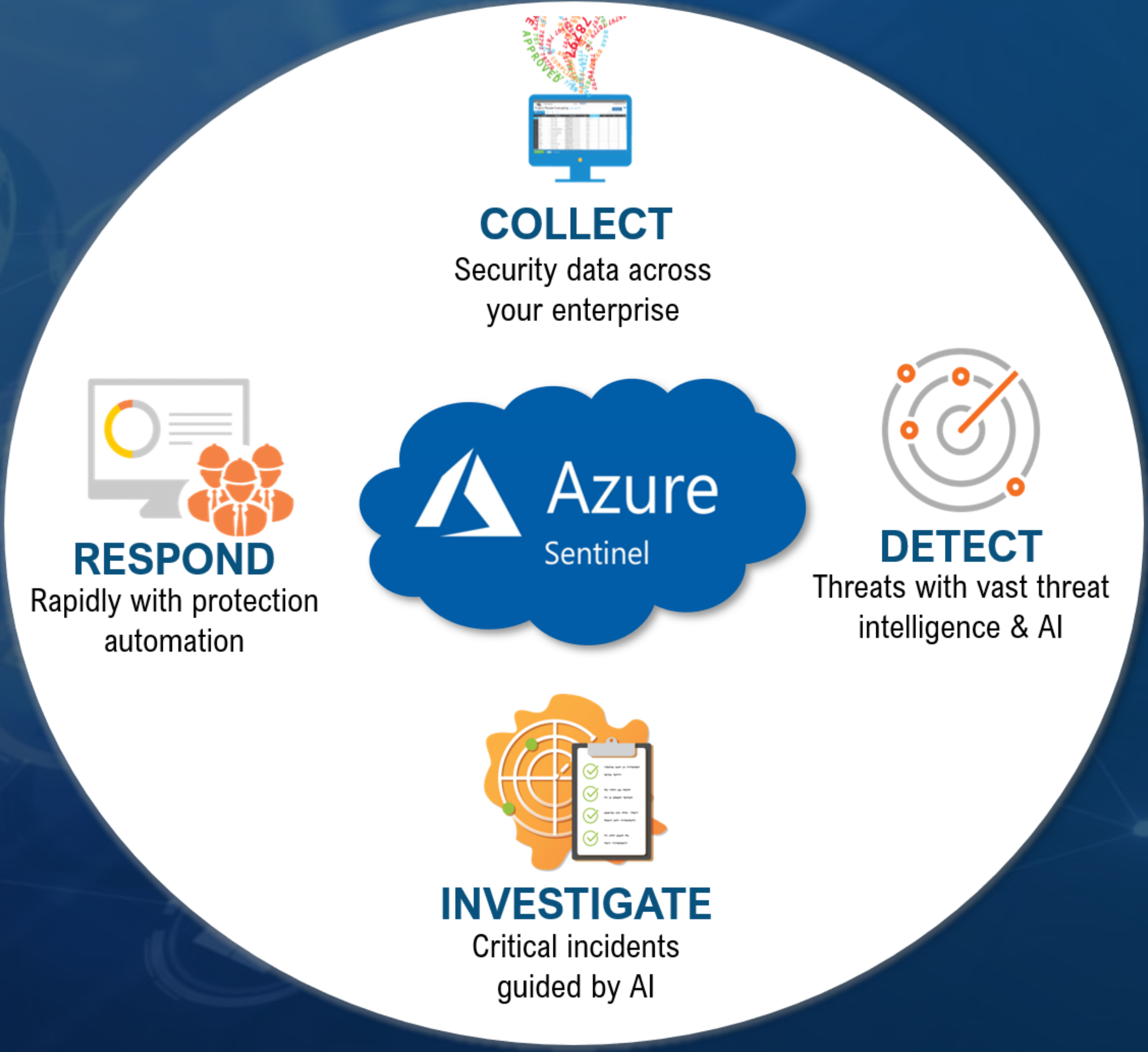
Malicious and suspicious messages blocked in 2019

12B

Cloud activities inspected, monitored, and controlled in 2019

Microsoft Azure Sentinel SIEM and SOAR

- **Collect data at cloud scale** across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds.
- **Detect previously undetected threats**, and minimize false positives using Microsoft's analytics and unparalleled threat intelligence.
- **Investigate threats with artificial intelligence**, and hunt for suspicious activities at scale, tapping into years of cyber security work at Microsoft.
- **Respond to incidents rapidly** with built-in orchestration and automation of common tasks



COLLECT
Security data across your enterprise

DETECT
Threats with vast threat intelligence & AI

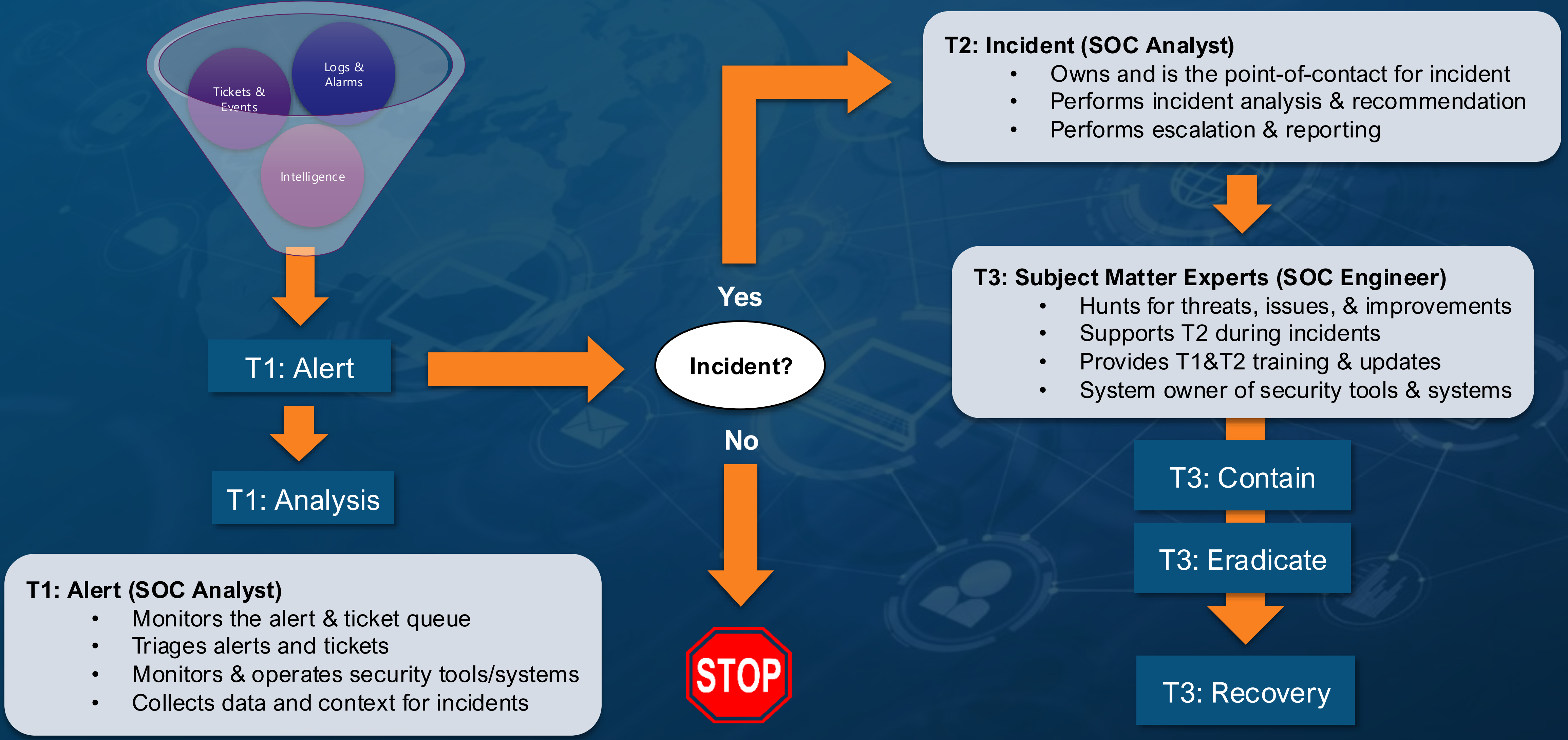
Azure
Sentinel

RESPOND
Rapidly with protection automation

INVESTIGATE
Critical incidents guided by AI

AccountabilIT
Customer Driven IT Services

Sentinel Managed Detection and Response Process



T1: Alert (SOC Analyst)

- Monitors the alert & ticket queue
- Triages alerts and tickets
- Monitors & operates security tools/systems
- Collects data and context for incidents

T2: Incident (SOC Analyst)

- Owns and is the point-of-contact for incident
- Performs incident analysis & recommendation
- Performs escalation & reporting

T3: Subject Matter Experts (SOC Engineer)

- Hunts for threats, issues, & improvements
- Supports T2 during incidents
- Provides T1&T2 training & updates
- System owner of security tools & systems

KnowBe4 Security Awareness Training

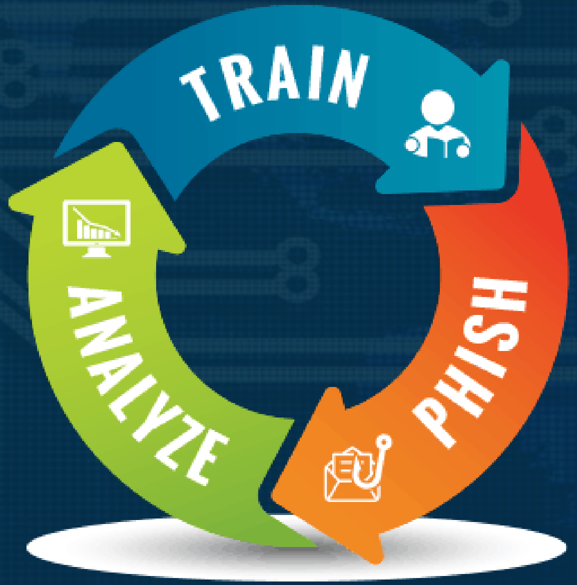
Today, your employees are frequently exposed to sophisticated phishing and ransomware attacks.

Baseline Testing
Assess the phish-prone percentage of your users with a free simulated attack.

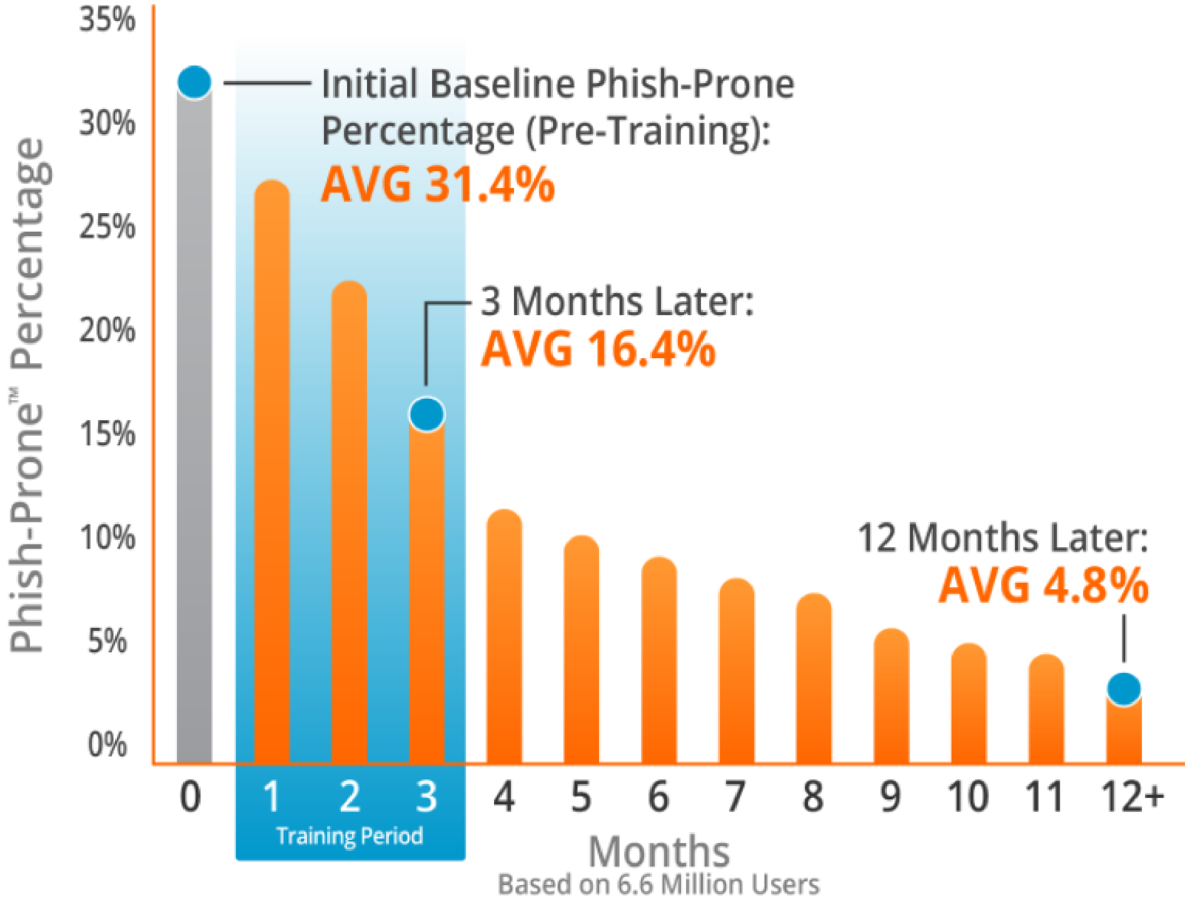
Train Your Users
The world's largest library of security awareness training content; including interactive modules, videos, games, posters, and newsletters. Automated training campaigns with scheduled reminder emails.

Phish Your Users
Best-in-class, fully automated simulated phishing attacks, thousands of templates with unlimited usage, and community phishing templates.

See the Results
Enterprise-strength reporting, showing stats & graphs for training and phishing, ready for management. Show the great ROI!



This Really Works!



Source: 2021 KnowBe4 Phishing by Industry Benchmarking Report

Nearly 7 million users were analyzed over the course of 12 months (2020). The overall industry initial phish-prone percentage was 30%!

Fortunately, the data showed that this 31% can be brought down by about half to just 16% in only 90 days by deploying new-school security awareness training. The 365-day results show that by following these best practices, the final phish-prone percentage can be minimized to 5% on average.

Benefits of Working with a Managed Security Services Partner

AccountabilIT
Customer Driven IT Services

Security Costs

Salary $85-100k
Security Engineer

Salary $85-100k
Security Engineer

Salary $85-100k
Security Engineer

Salary $85-100k
Security Engineer

Salary $85-100k
Security Engineer

Salary $85-100k
Security Engineer

Salary $85-100k
Security Engineer

AccountabilIT’s Security Operations Team

Efficiency and Urgency

Rapid Incident Response and Event Investigation. Efficiency and urgency needed to stop attacks before they cause damage.

24x7

Avoid alert fatigue with monitoring and oversight, 24 hours a day, 7 days a week, 365 days a year.

Fracton of the cost of hiring 24x7 security experts in-house

Extend Your Team

- No need to have internal IT be the expert.
- Better utilization of existing tools.
- Easily scale

Decrease Risk

Stay up to date up to date with ongoing security initiatives. Decrease risk and increase compliance.

AIT AccountabilIT
Customer Driven IT Services

Locations: Scottsdale, AZ (HQ); Little Rock, AR; Denver, CO; New Delhi, India
www.accountabilit.com

- **24/7 Security Operations Center**
- **Azure IP Co-Sell Ready Partner**
- **ECIF certified**

Why AccountabilIT?

- MSP + MSSP (security remediation ability)
- Microsoft Cloud MVP on co-sell team
- First-mover advantage- advanced automation/machine learning
- Private Partner Preview Program- only MSP
- Azure Lighthouse deployments keep customer's deployment within their own Azure tenant (rare)
- Enterprise-level operations for SMC market (HIPAA, SOC II Compliant & pricing/operations sophistication)

RCP 350 TOP U.S. MICROSOFT PARTNERS

2019 TOP 200 MSSPs
www.MSSPAlert.com/top200

Microsoft Partner
Microsoft

Gold Cloud Platform
Gold Cloud Productivity
Gold Datacenter

Key Differentiators

- 24x7x365 NOC & SOC. Provides a deep bench for both detection and analysis but more importantly remediation and recovery.

- Not a startup around Microsoft security services. AIT brings mature process and procedure to Sentinel orchestration and operation from years of 24x7x365 Security Operations Center operations.

- Your Azure subscription. AIT does not hold your data or security position hostage. Everything from daily operation to tuning and optimization is done in your subscription.

AIT ADVANTAGE

AIT
AccountabilIT
Customer Driven IT Services

AccountabilIT is an MSP and MSSP based out of Scottsdale, AZ. With our extensive security expertise utilizing SIEM tools within customer environments, we were strategically positioned when Sentinel came into the market last year to quickly become the go-to partner for Microsoft and its' customers.

- 22 years of experience managing apps, data, security
- and hybrid cloud environments.
- Microsoft Gold Partner
- 24 x 7 Security Operations Center
- HIPAA, ISO, SOC II Compliant

2019 TOP200 MSSPs
www.MSSPAlert.com/top200

RCP 350
TOP U.S. MICROSOFT PARTNERS

Microsoft
Cloud Solution Provider

Microsoft Partner
Microsoft

Gold Cloud Platform
Gold Cloud Productivity
Gold Datacenter

Q & A

Have More Questions?

Sean Coe

Account Development Manager

☎ (480)818-0859

✉ Sean.Coe@AccountabilIT.com