

Security Concierge

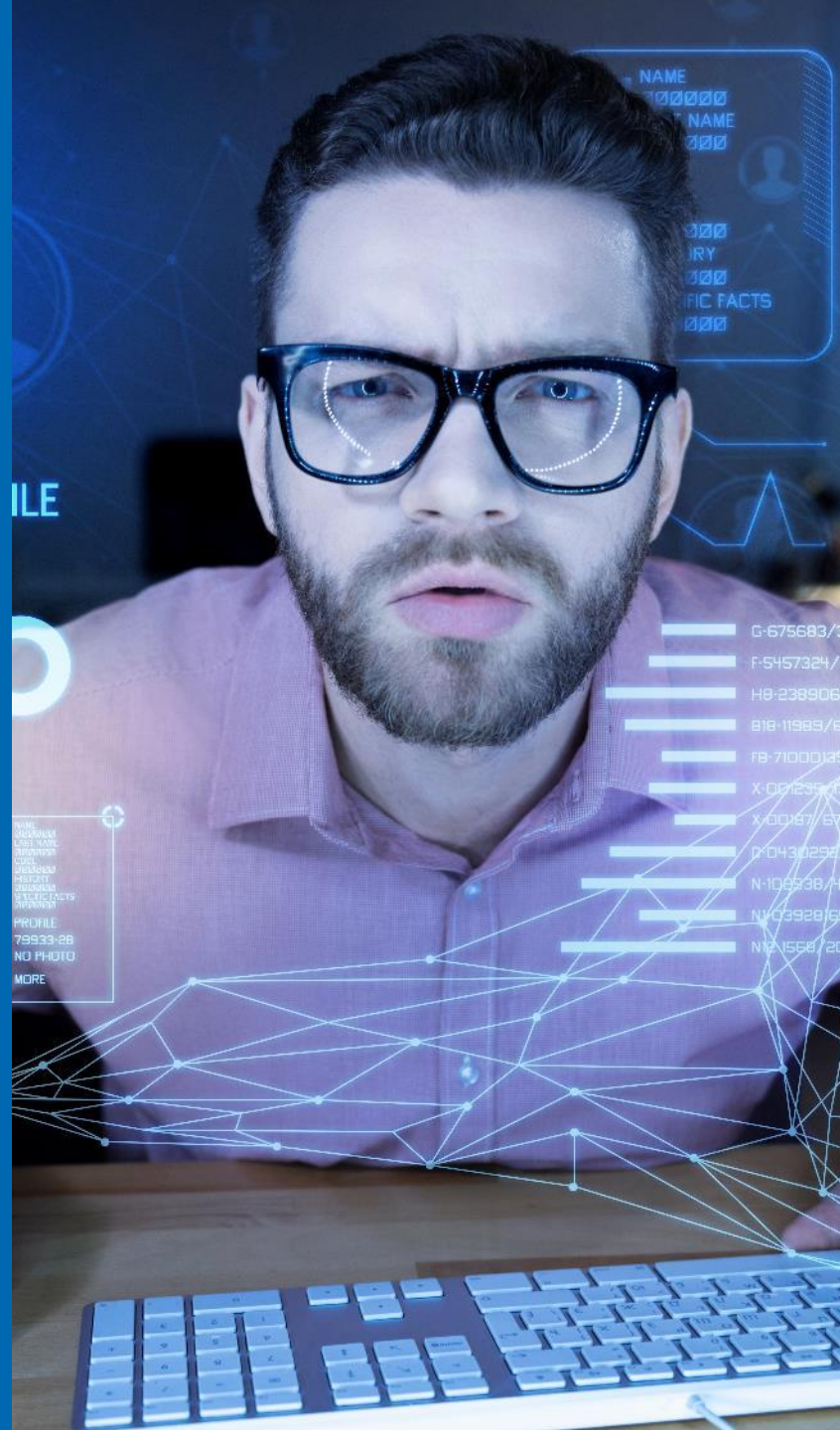
Protect Your Business Against Cyber- threats
and Information Loss with Cybersecurity
Managed Services

A man with short dark hair, a beard, and glasses is wearing a dark suit jacket over a white shirt and a dark tie. He is sitting at a desk with a laptop in front of him, looking down at the screen with a thoughtful expression, his hands clasped together. The background is a dark, solid color. In the top left corner, there is a white square. In the bottom right corner, there is a small green plant and a blue square containing the number 2.

Are you concerned about Cyberthreats in your Organization?

Small and Medium-Sized Businesses (SMBs) lose around **\$80K** annually due to cyberthreats.

Personally identifiable information (PII)



Organizations can be fined an average of **\$150** per record containing PII, which includes:

- First and last name, or a first initial and last name
- Social Security number
- Driver's license
- Financial account
- Credit or debit card numbers
- Passwords, PINs, or access information for financial accounts

The Facts



3 out of 4 SMBs say they lack sufficient personnel to address IT security.

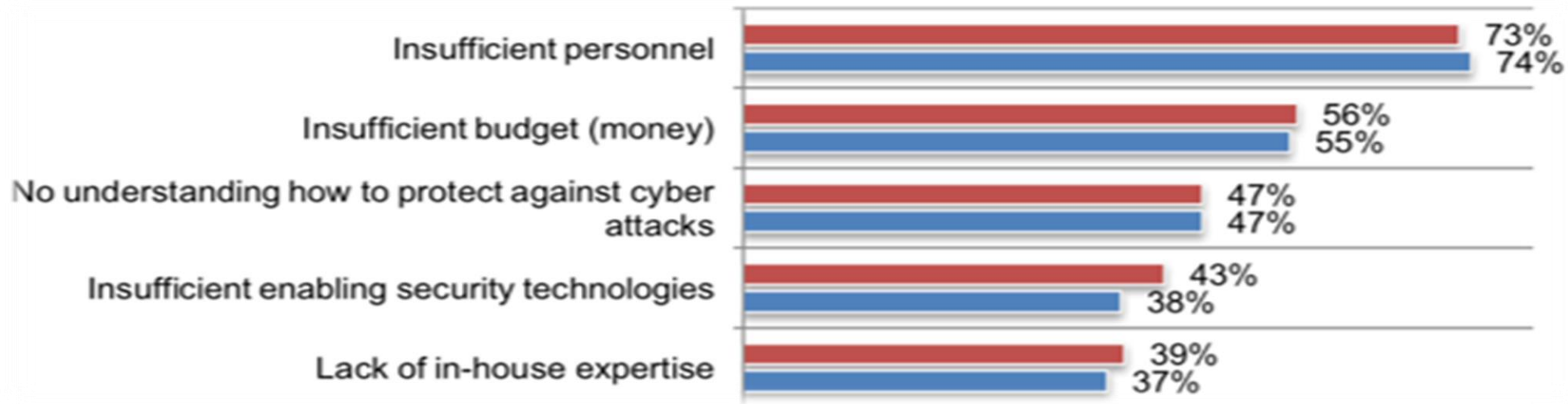
82%

of SMBs Reported attacks where malware was able to get by their Anti-Virus Software.

The Solution: Many SMBs are turning to MSSPs for help.

Why an MSSP?

Reasons why customers turn to an MSSP for their cybersecurity needs.



Source: Ponemon/Keeper 2020 State of Cybersecurity in Small & Medium Size Business

Have you ever been the victim of a phishing attack?

- **90%:** of data breaches are due to phishing attacks
- **+65%:** growth per year in phishing attempts
- **76%:** of businesses reported being victim of a phishing attack

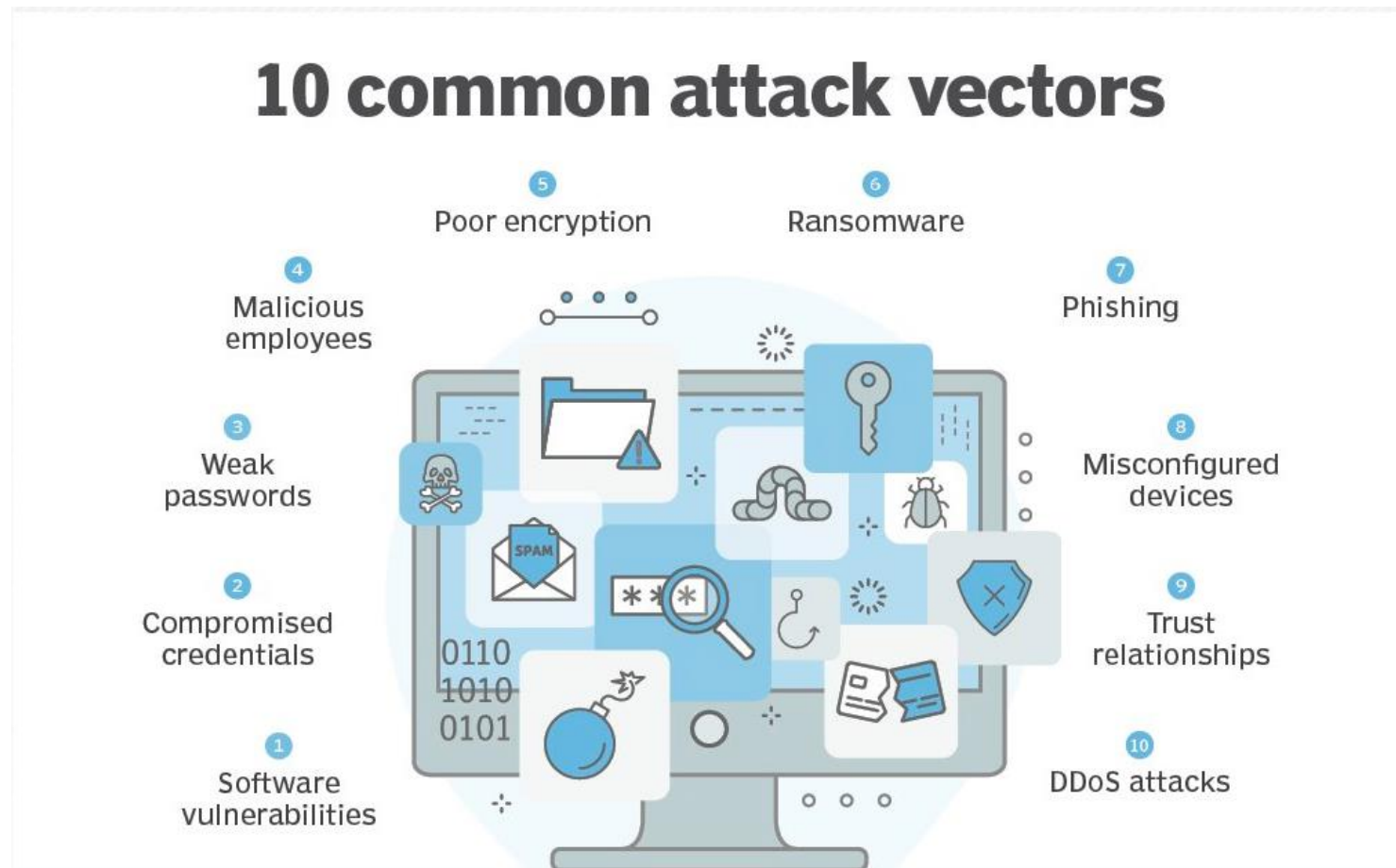
Source: APWG Phishing Activity Trends Report <http://www.apwg.org>



CyberSecurity Today

Attack Vectors

Attack vectors – defend your organization from the methods that adversaries use to breach or infiltrate your network.



Security Protection by Vectors

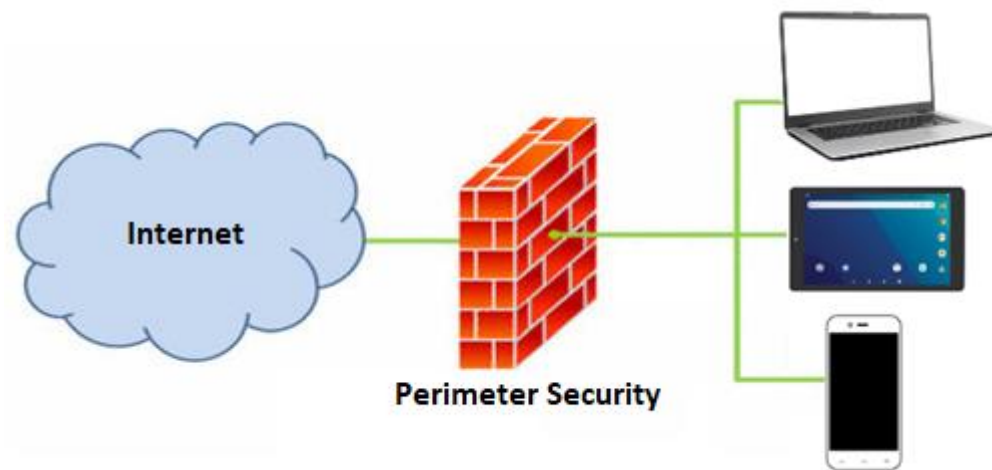
- Perimeter Security
- Endpoint Security
- Office 365 Security (Email & Collaboration)
- Identity Protection
- Vulnerability & Patch Management
- Security Awareness Training and Attack Simulations
- Dark Web Monitoring



Security Protection by Vectors

Perimeter Security

- Robust perimeter protection by creating a secure IT network.
- Consistently manage next-generation firewall defenses and keep firewalls properly configured and updated.
- Integrate firewall and third-party perimeter security platforms to the SIEM to correlate events and take preventive actions.



Security Protection by Vectors

Endpoint Security

- Protect End User Devices Including Laptops, Desktops, Servers, and Mobile Devices.
- Actively monitoring and control endpoint devices, behavior and connections.
- Block malware and viruses from downloading in real-time.



User trying to download a virus off the web:



Security Protection by Vectors

Office 365 Security (Email & Collaboration)

- Leverage the Office 365 Security Policies and configurations.
- Proactive Monitoring security policies, alerts and events.

Below are some common alerts from Office 365 security platforms:

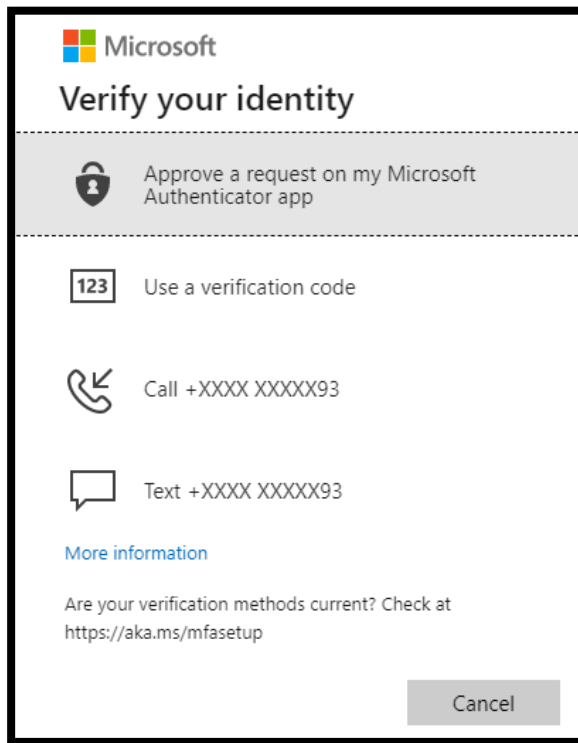
● Medium	Activity from a Tor IP address
● Medium	Activity from infrequent country
● Informational	Creation of forwarding/redirect rule
● Low	Elevation of Exchange admin privilege
● Informational	Email messages containing malicious URL removed after delivery

Security Protection by Vectors

Identity Protection

- Gain visibility and control of user data and access permissions.
- Leverage Conditional Access and MFA.
- Apply risk-levels to suspicious users.

User prompted to use MFA during login:



List of risky users:

Risky users (Preview)

Learn more Download Select all Confirm user compromised Dismiss user risk

Show dates as: Local Risk state : 2 selected Status : Active Add filters

USER	RISK STATE	RISK LEVEL
Administrator	At risk	Medium
<input checked="" type="checkbox"/> Oisín Johnston	At risk	Low
Nancy Anderson	At risk	Low
Sanjay Patel	At risk	Low
James Ryan	At risk	Medium







Security Protection by Vectors

Vulnerability and Patch Management

- Vulnerability Scans and patch management services.
- Identify vulnerabilities in your systems and provide recommended actions to take.



Recommended actions to remediate vulnerabilities:

Recommendation	Exposed devices	Threats	Impact
Update Microsoft Windows 10 (OS and built-in applic...	79	 	▼ 33.13
Update Microsoft Office	78	 	▼ 20.98
Block JavaScript or VBScript from launching downloa...	95	 	▼ 19.18 +9.00

Security Protection by Vectors

Security Awareness Training and Attack Simulations

- Security awareness trainings will elevate employees' level of knowledge regarding cybersecurity topics, becoming part of the security solution.
- Attack simulations will be conducted regularly to test the knowledge of employees regarding basic cybersecurity topics.



Attack simulation process can be seen above:

Security Protection by Vectors

Dark Web Monitoring

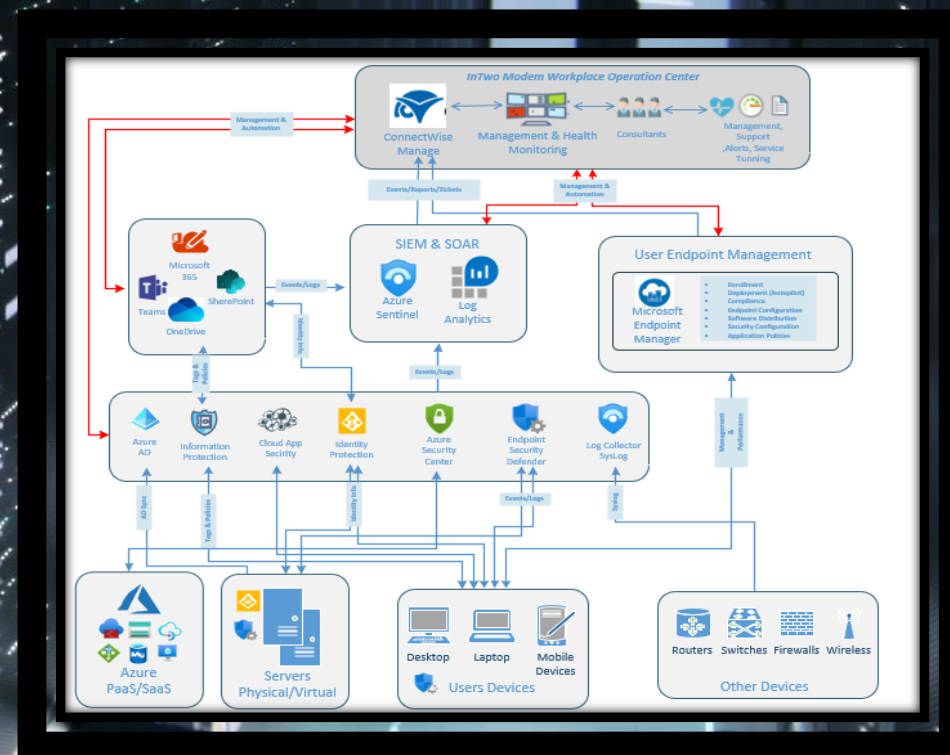
- Actively monitor for compromise users & business data.
- Identify PII that may be found in the dark web.

Compromised user accounts and passwords found in the dark web:

Date Found	Email	Password Hit	Source	Type
03/27/20	*****@bird.com	liny****	id theft forum	Not Disclosed
03/26/20	*****@bird.com	ab3c****	id theft forum	Not Disclosed
03/19/20	*****@bird.com		id theft forum	Not Disclosed
03/16/20	*****@bird.com	DRAG****	id theft forum	Not Disclosed
02/19/20	*****y18@bird.com	ilov****	id theft forum	Not Disclosed
02/19/20	*****@bird.com		id theft forum	Not Disclosed
02/17/20	*****@bird.com		id theft forum	Not Disclosed
02/17/20	*****@bird.com		id theft forum	Not Disclosed
02/17/20	*****@bird.com		id theft forum	Not Disclosed
02/17/20	*****@bird.com		id theft forum	Not Disclosed
02/17/20	*****@bird.com		id theft forum	Not Disclosed
02/17/20	*****@bird.com		id theft forum	Not Disclosed
02/17/20	*****@bird.com		id theft forum	Not Disclosed
02/17/20	*****@bird.com		id theft forum	Not Disclosed
02/17/20	*****3@bird.com		id theft forum	Not Disclosed
02/17/20	*****@bird.com		id theft forum	Not Disclosed

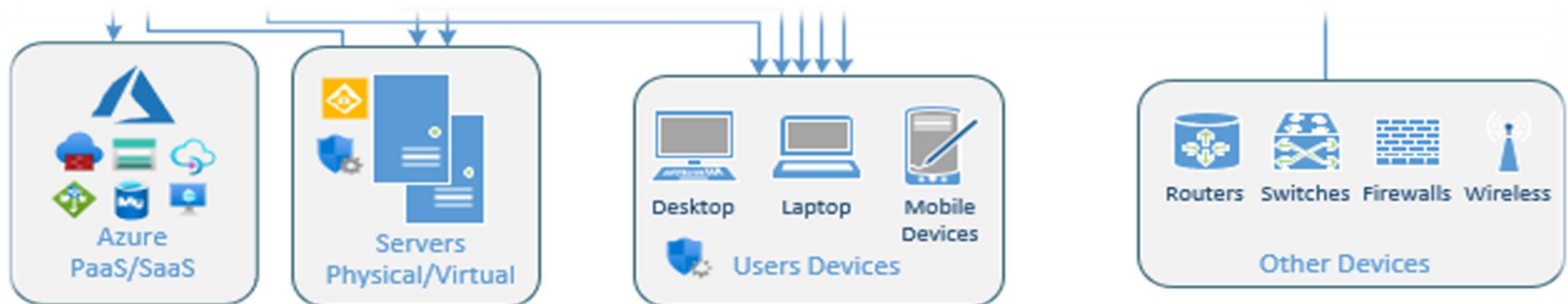
Overview of InTWO's Platform and Event Correlation

- Managed Threat Detection & Response



Platform and Event Correlation

- Ingest logs from multiple vectors.
- Monitor multiple security vectors.
- Security data collection.
- Cover a wide scope of attack surfaces.
- Complete overview of user and device activity.



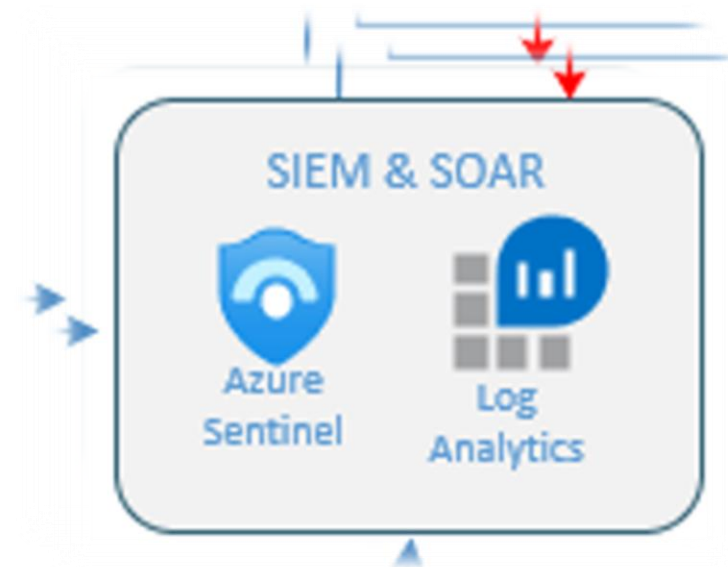
Platform and Event Correlation

- Receive logs from multiple vectors.
- Learn of unusual or suspicious behaviors.
- Halt attacks in real-time.
- Block malware and virus downloads.
- Take action based on user risk levels.
- Identify impossible travel.
- Detect shadow IT.



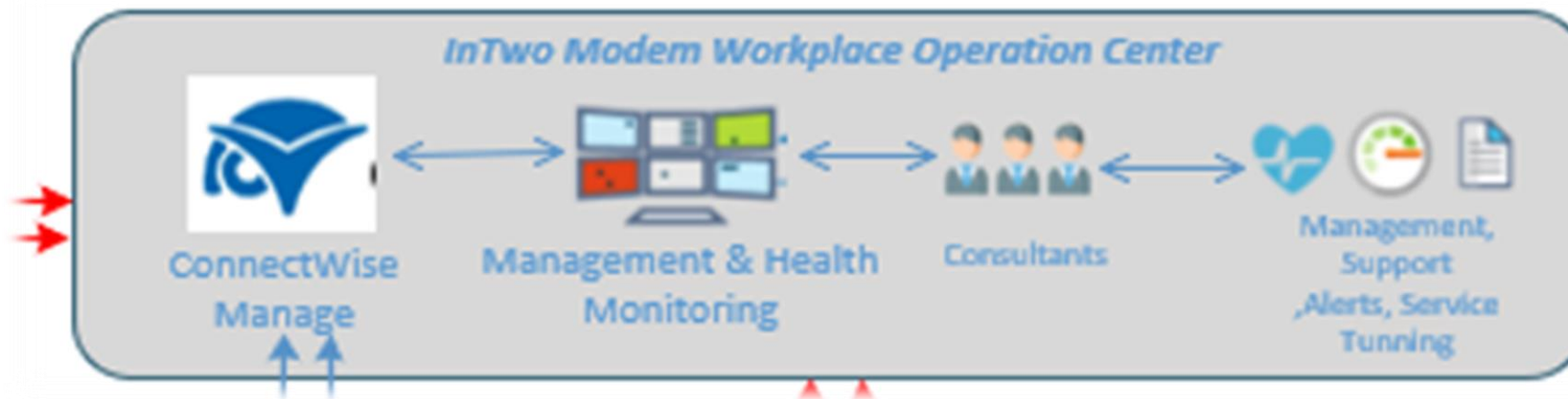
Platform and Event Correlation

- Microsoft Sentinel (SIEM) - Centralized log management, event correlation, analysis, and reporting capabilities.
- Correlate logs and behavior from different platforms, devices and identities.
- Know who and what is connected to your environment.
- Learn of unusual or suspicious behaviors in your environment.
- SOAR capabilities to communicate incidents and alerts to customers and cybersecurity analysts.
- Automated process to create incident tickets.

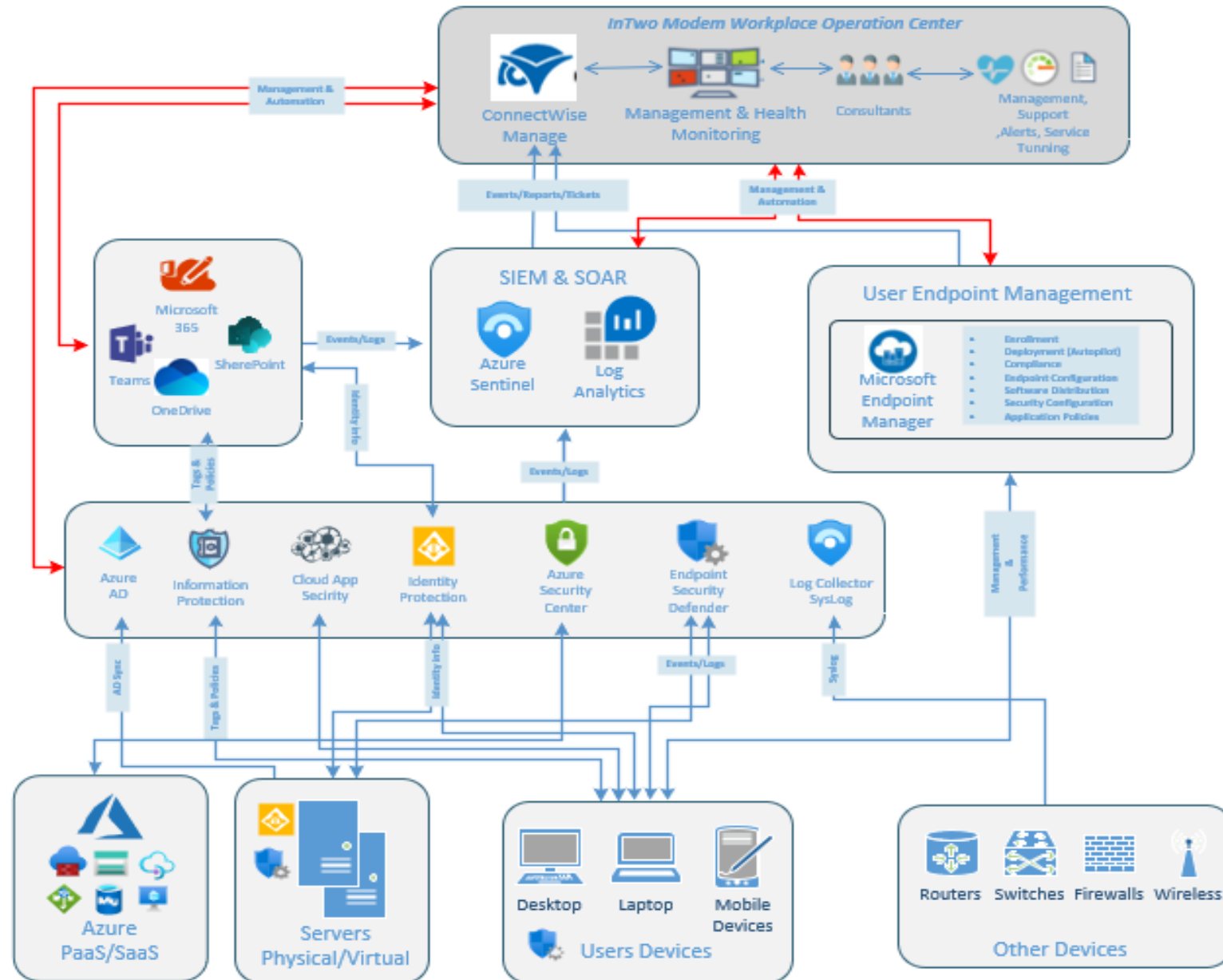


Platform and Event Correlation

- Cybersecurity analysts react to all alarms and customer reports.
- Ticket creation and documentation on all incidents.
- Support available 24/7.
- Quick response to ensure your business stays protected.
- Access to customer ticket database.

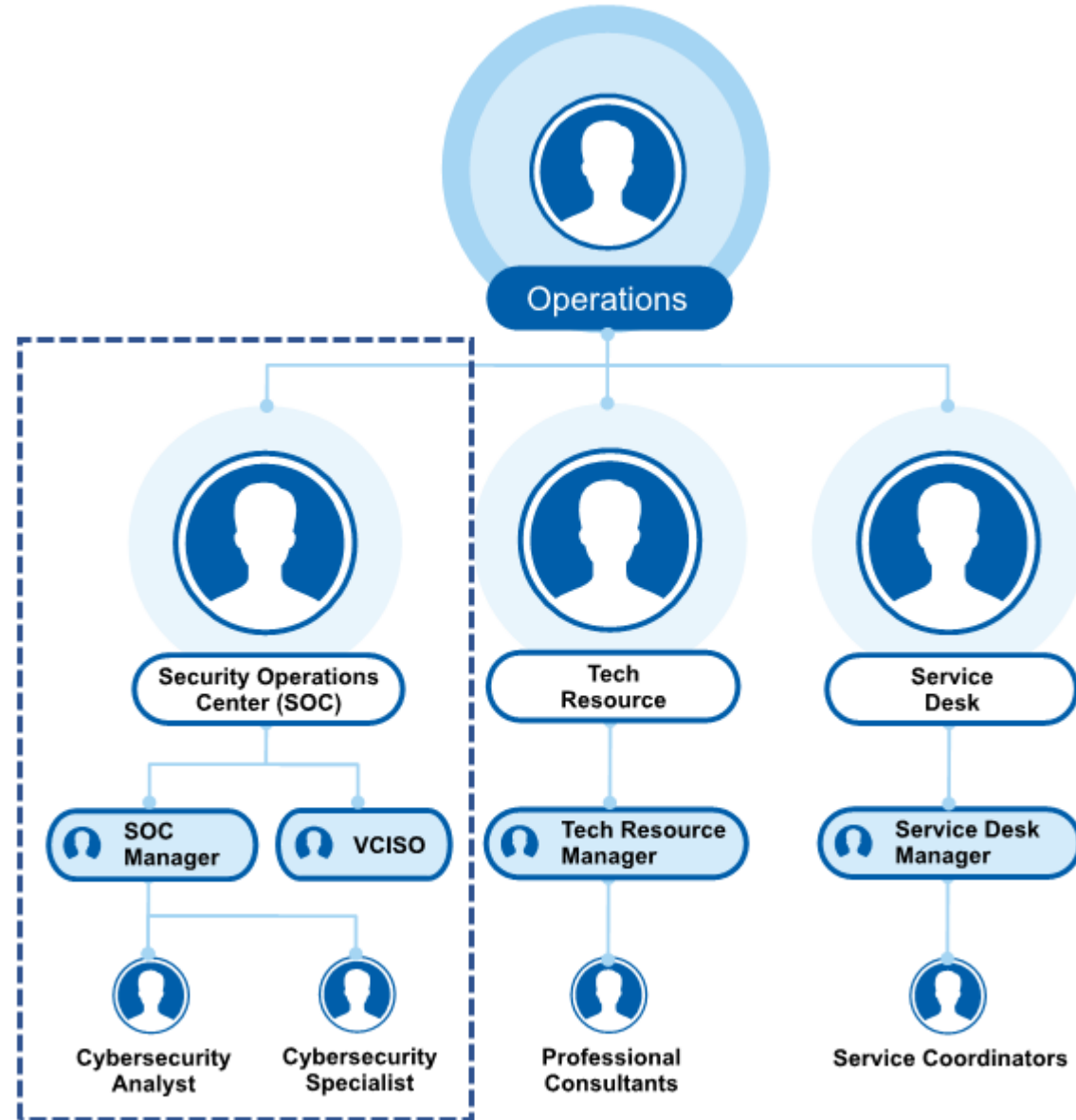


InTWO's Platform and Event Correlation – Overview



SOC Organizational Structure

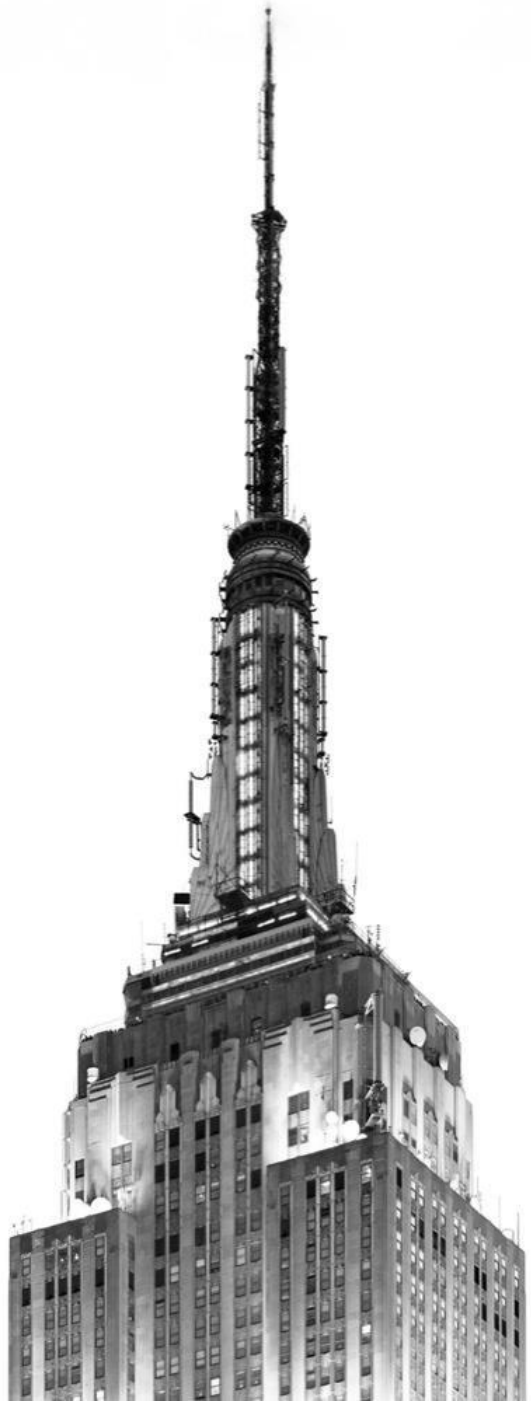
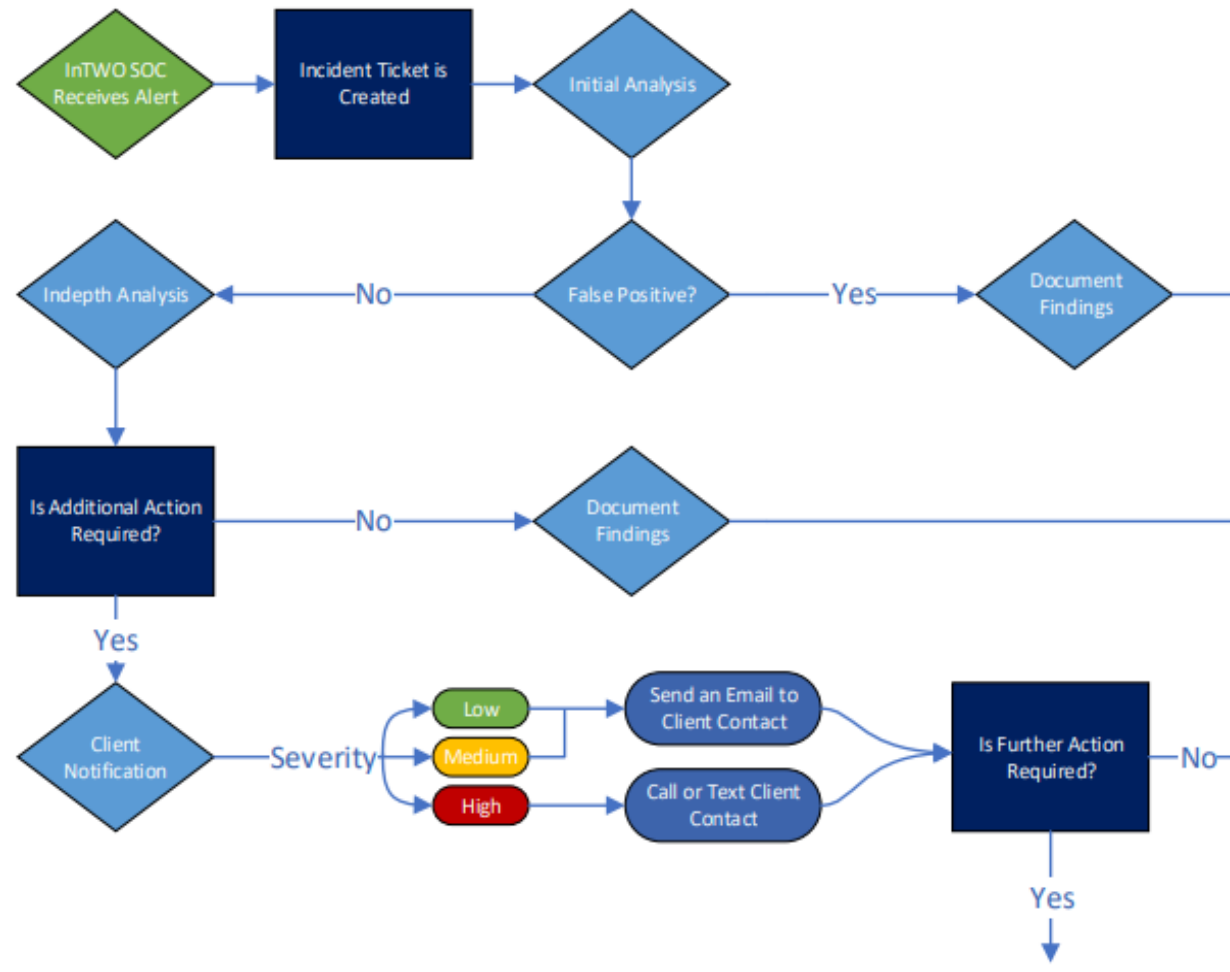
- Segmented by department
- Structured to comply with standards and regulations

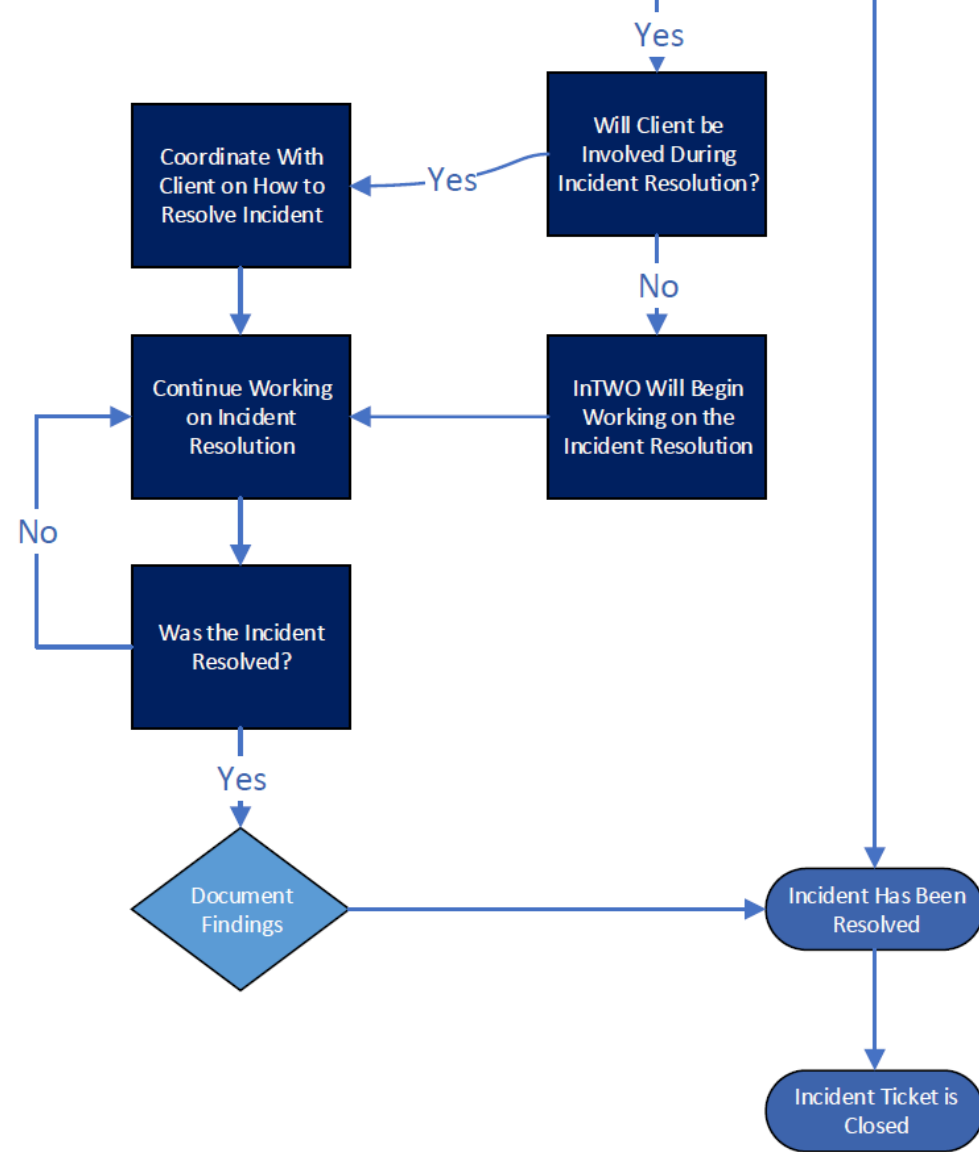


InTWO's Cybersecurity Services Deployment

- Onboarding (Management & Monitoring Tools configuration and deployment)
- Security Assessments
- Corporate Security Policies Definition
- Users Security Awareness Training
- Endpoint Security Policies Deployment
- Identity Security Policies Deployment
- Microsoft 365 Security Policies Deployment

Incident Response Workflow





Reporting

Types of Reports Provided:

- Cloud Assessments
- Network Assessments
- Security Assessments

With InTWO's recurring SOC reports you will be able to:

- Provide the executive team with security updates
- Gain insights on your cybersecurity posture
- Stay up to date with current cybersecurity trends
- Identify and remediate vulnerabilities in your systems

Cloud Assessments

This section contains a summary of issues detected during the assessment process and is based on industry-wide best practices.

Risk Report

<p>Domain Users Not Forced to Elevate during Network Location Setting (90 pts each)</p> <p><i>Current Score:</i> 90 pts x 101 = 9090: 1.67%</p> <p><i>Issue:</i> Unimplemented Microsoft Control: Control Network Location Setting.</p> <p><i>Recommendation:</i> Determines whether to require domain users to elevate when setting a network's location. Selecting an incorrect network location may allow greater exposure of a system</p>
<p>Local Administrators Can Create Firewall Rules (90 pts each)</p> <p><i>Current Score:</i> 90 pts x 101 = 9090: 1.67%</p> <p><i>Issue:</i> Unimplemented Microsoft Control: Prevent Firewall Rules Access <u>By</u> Local Admin.</p> <p><i>Recommendation:</i> Controls whether local administrators are allowed to create local firewall rules that apply together with firewall rules configured by Group Policy. When in the Public profile, there should be no special local firewall exceptions per computer. These settings should be managed by a centralized policy - merging local firewall rules with group policy firewall rules may weaken intended group policy firewall configurations.</p>
<p>Autorun Commands Allowed (90 pts each)</p> <p><i>Current Score:</i> 90 pts x 101 = 9090: 1.67%</p> <p><i>Issue:</i> Unimplemented Microsoft Control: Restrict Use of Autorun Commands.</p> <p><i>Recommendation:</i> Determines whether Autorun commands are allowed to execute. Autorun commands are generally stored in autorun.inf files. They often launch the installation program or other routines. Allowing autorun commands to execute may introduce malicious code to a system without user intervention or awareness. Configuring this setting prevents autorun commands from executing.</p>

Cloud Assessments

Management Plan Report

The Management Plan ranks individual issues based upon their potential risk to the network while providing guidance on which issues to address by priority.

High Risk			
Risk Score	Recommendation	Severity	Probability
90	<p>Unimplemented Microsoft Control: Admin Multi-factor Authentication. You have 1 users with administrative roles that are not registered and protected with MFA. See Users section in Azure AD Report for details.</p> <p>Requiring multi-factor authentication (MFA) for all administrative roles makes it harder for attackers to access accounts. Administrative roles have higher permissions than typical users. If any of those accounts are compromised, critical devices and data is open to attack.</p>	H	H
90	<p>Unimplemented Microsoft Control: Remove Dormant Accounts.</p> <p>An easy and quiet path deep into your organization is through inactive accounts that are a part of sensitive groups. Removing dormant account access rights or deleting the account will help protect your organization's sensitive data and prevent further compromise. Accounts become dormant if they are not used for a period of 180 days.</p>	H	H

Network Assessments

Consolidated Risk Report

The Consolidated Risk Report aggregates risk analysis from multiple assessments performed on the network, providing both a Consolidated Risk Score and an overview of the health and security of the network.

Issue	Severity	Risk Score	Instances	Weighted Risk Score	Assigned Priority
Anti-spyware not up to date	High	90	12	108	1
User password set to never expire	Low	30	176	528	1
Operating system in Extended Support	Low	20	6	120	1
Inactive computers	Low	15	152	22	1
User has not logged on to domain in 30 days	Low	13	173	224	1
Insecure listening ports	Low	10	1	10	1
Un-populated organization units	Low	10	10	100	1
Admin Multi-factor Authentication Not Registered	High	90	1	90	1
VPN Based Detection Not Configured	High	90	1	90	1
Inactive User Accounts Identified	High	90	1	90	1
Legacy Authentication Not Blocked	High	90	1	90	1
Customer Lockbox Not Enabled	High	90	1	90	1
Integrated Apps Not Regulated	High	90	1	90	1
Multi-factor Authentication Not Registered	High	90	1	90	1
Password Age Policy Enabled	High	90	1	90	1
Sign in Risk Policy Not Enabled	High	90	1	90	1
User Risk Policy Not Enabled	High	90	1	90	1

Security Assessments

Security Report Card

The Security Report Card assesses individual computers at a high level based on various security criteria.

Computer	Overall Grade	Anti-virus	Anti-spyware	Local Firewall	Failed Logins	System Aging	Supported OS
Computer	B	A	B	A	A	A	C
Computer	B	A	A	A	B	A	A
Computer	B	A	A	A	A	B	B
Computer	A	A	A	A	A	A	A
Computer	A	A	A	A	A	A	A
Computer	A	A	A	A	A	A	A
Computer	B	A	A	A	A	A	B
Computer	B	A	A	A	B	A	A
Computer	B	A	A	A	A	A	B
Computer	A	A	A	A	A	A	A
Computer	B	A	A	A	A	C	B
Computer	A	A	A	A	A	A	A
Computer	A	A	A	A	A	A	A

Security Assessments

Data Breach Liability Report

Total Potential Liability

\$15,000

This report identifies instances of personal identifiable information (PII) throughout your network and calculates the potential monetary liability based upon industry published research.

Computer	IP Address	Missing Critical Patches	Anti-virus	Sensitive Data Count	
Computer Name	192.168.2.1	1	✓	50	\$5,000
Computer Name	192.168.2.1	0	✓	0	\$0
Computer Name	192.168.2.1	0	✓	0	\$0
Computer Name	192.168.2.1	0	✓	0	\$0
Computer Name	192.168.2.1	2	✓	100	\$10,000
Computer Name	192.168.2.1	0	✗	0	\$0
Computer Name	192.168.2.1	0	✓	0	\$0
Computer Name	192.168.2.1	0	✓	0	\$0



Thank you!

www.intwo.cloud