proarch

Going 24x7:

How to Detect and Respond to Cyber Threats

We listen closely, understand deeply and solve strategically.

Accelerating value and increasing resilience for our clients.

Founded in 2006

3 countries

300+ employees

Atlanta, GA
Syracuse, NY
Rochester, NY

London, UK
Hyderabad, India
Bangalore, India

Presenter

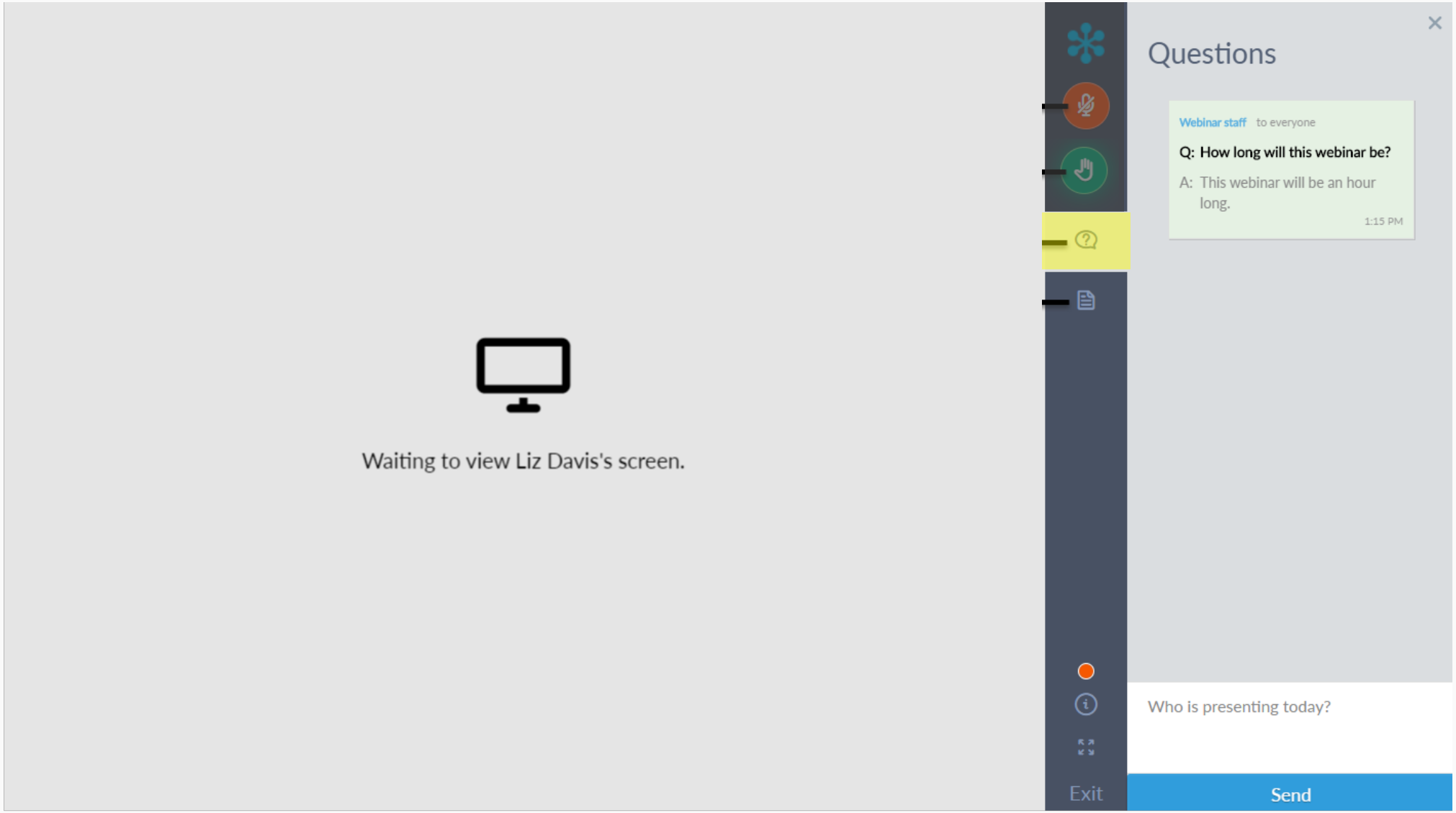
Michael Montagliano
Chief of Innovation

CISSP, CEH, CDRP, MBCI

Mike Wurz
Security Consultant Team Lead

CEH, GIAC-PEN

proarch


Waiting to view Liz Davis's screen.
Questions
Webinar staff to everyone
Q: How long will this webinar be?
A: This webinar will be an hour long.
1:15 PM
Who is presenting today?
Exit
Send

Agenda

State of security threats

What it takes to stop threats

MDR vs MSSP

The MDR investment

Current State of Threats

The Current State

Attackers aren't slowing down

December 2020	March 2021	May 2021	June 2021
SolarWinds	**Microsoft Exchange Servers Zero-Day Vulnerabilities**	**Colonial Pipeline Attack**	**JBS Attack**

U.S. DEPARTMENT OF ENERGY

OFFICE OF CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE

DOE Kicks Off **100-Day Plan to Address Cybersecurity Risks to the U.S. Electric System**, Seeks Input from Stakeholders on Safeguarding U.S. Critical Energy Infrastructure

Attackers Have the Advantage

280 Days

Average number of days for organizations to identify and contain a breach.

76%

Percentage of ransomware events that occur outside of work hours.

3.1M

Number of cybersecurity jobs that went unfulfilled in 2020.

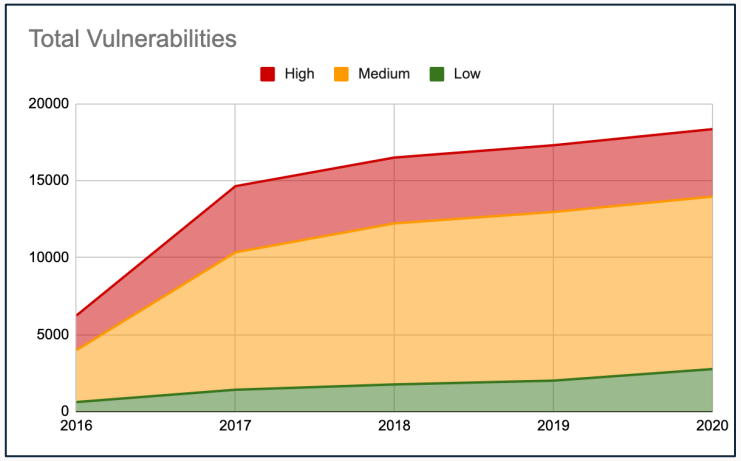
IBM 2020 Cost of a Data Breach Report
FireEye 2020 Ransomware Deployment Trends

Vulnerability Overload

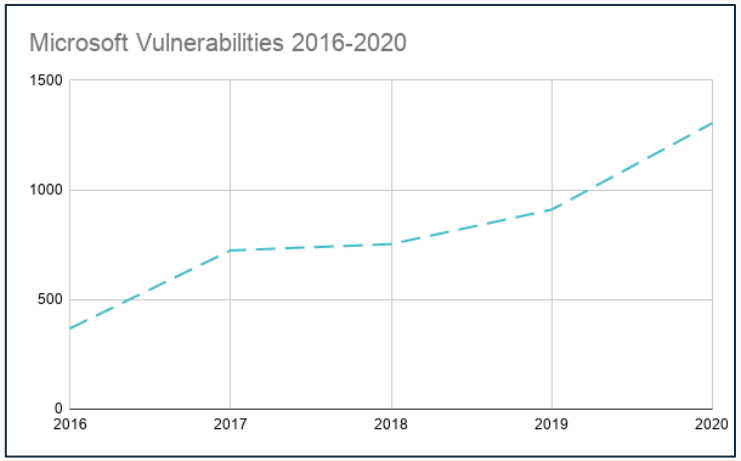
Since 2016 the number of new vulnerabilities released each year has almost tripled

Microsoft patches have more than tripled since 2016

The growth in reported vulnerabilities has made it impossible for most organizations to track and patch all vulnerabilities a timely fashion.



Source: NIST Vulnerability Database



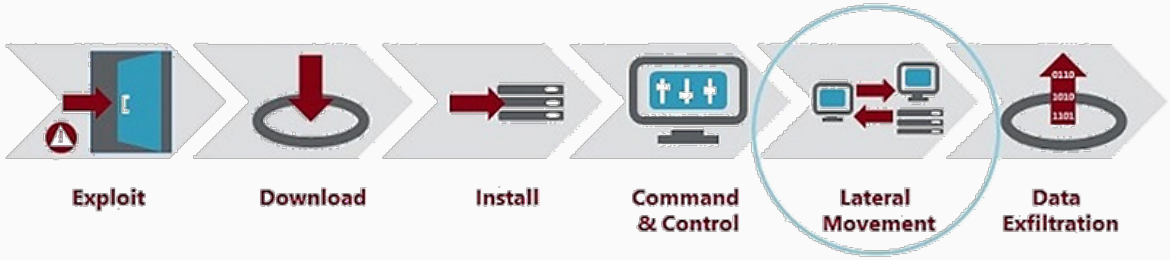
Source: Microsoft

“Breakout Time Window” for Response

1 hour and 58 minutes.

The average amount of time between the initially compromised machine and lateral movement across the network to attain other assets or accounts.

Was 4 hours and 37 minutes two years ago.



MDR vendors follow the 1-10-60 rule:

- **1 minute** to detect threats (Mean-Time to Detection)
- **10 minutes** to complete investigations (Mean-Time to Respond)
- **60 minutes** to remediate the incident (Mean-Time to Resolve)

The shorter the MTTD/MTTR values, the faster to recovery.

What it Takes to Really Stop Threats

What You Need to Keep Threats Out

People, process, and technology

Ability to pinpoint attackers across corporate resources

Across the entire modern attack surface

- Endpoints: laptops, mobile devices, servers
- Identities
- On-premises
- Cloud
- Custom sources

24x7 team of security responders to remediate threats

Analyzing cases and performing threat investigation to confirm indicator of compromise or false positive- 24 hours a day

Long-term risk reduction and management plan

Measurable time to detect and time to respond metrics

Manageable impact and cost of security incidents

Aligned with compliance requirements

Breaking Down Managed Detection and Response (MDR)

Skilled Security Teams and Advanced Threat Technology that Stop Attackers in Their Tracks

24x7 extension of internal security team

Advanced threat visibility across resources

Skilled security threat responders:

- eliminate false positives
- identify malicious activity
- investigate & contain threats
- escalate to Incident Response

Extended Detection and Response (XDR)

End-to-end attack prevention across corporate resources and custom log sources.

On-premises and cloud networks, endpoints, and identities.

Endpoint Detection and Response (EDR)

Keep threats off devices that are a clear path to corporate resources.

Workstations, servers, virtual machines, and mobile devices.

Identity Detection and Response (IDR)

Prevent account compromises that lead to data breaches.

On-premises and cloud corporate accounts (Active Directory)

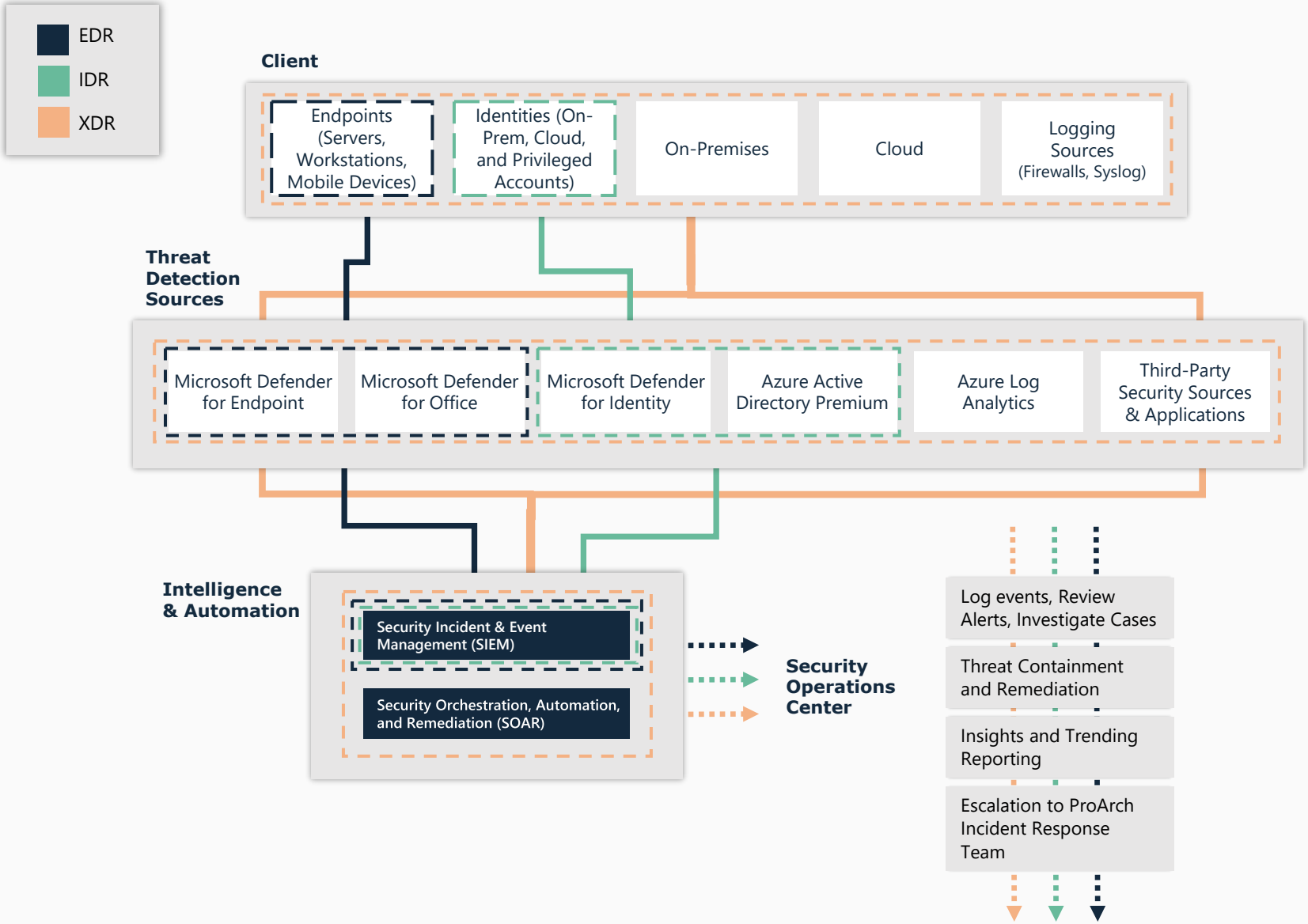
The Details: How MDR works

Threat detection sources and sensors are deployed across networks, cloud services, endpoints, and identities collecting and analyzing telemetry- making it possible to track down root cause quickly.

Threat intelligence backed by deep context, customer information, and the MITRE ATT&CK framework enhances alerts to categorize and prioritize.

The ProArch SOC team analyzes cases and performs a thorough threat investigation to confirm indicator of compromise or false positive- 24 hours a day.

Transition to ProArch Incident Response in the event of compromise.



The Tactics: How Hackers work – MITREATT&CK Framework

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
Any access, action, or configuration change to a system that gives an adversary a persistent presence on that system.	The result of techniques that cause an adversary to obtain a higher level of permissions on a system or network.	Techniques an adversary may use for the purpose of evading detection or avoiding other defenses.	Techniques resulting in the access of, or control over, system, domain, or service credentials that are used within an enterprise environment.	Techniques that allow an adversary to gain knowledge about a system and its internal network.	Techniques that enable an adversary to access and control remote systems on a network.	Techniques that result in execution of adversary-controlled code on a local or remote system.	Techniques used to identify and gather information, such as sensitive files, from a target network prior to exfiltration.	Techniques and attributes that result or aid in an adversary removing files and information from a target network.	Techniques and attributes of how adversaries communicate with systems under their control within a target network.

MITREATT&CK Framework: Enterprise

proarch

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 39 techniques	Credential Access 15 techniques	Discovery 27 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Credentials from Password Stores (5)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Build Image on Host	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Clipboard Data	Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Inter-Process Communication (2)	Browser Extensions	Create or Modify System Process (4)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Dashboard	Remote Services (6)	Data from Cloud Storage Object	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (2)	Deploy Container	Input Capture (4)	Cloud Service Discovery	Replication Through Removable Media	Data from Configuration Repository (2)	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Stage Capabilities (5)	Supply Chain Compromise (3)	Scheduled Task/Job (7)	Create Account (3)	Escape to Host	Direct Volume Access	Man-in-the-Middle (2)	Container and Resource Discovery	Software Deployment Tools	Data from Information Repositories (2)	Fallback Channels	Exfiltration Over Web Service (2)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)		Trusted Relationship	Shared Modules	Create or Modify System Process (4)	Event Triggered Execution (15)	Domain Policy Modification (2)	Modify Authentication Process (4)	Domain Trust Discovery	Taint Shared Content	Data from Local System	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Search Open Websites/Domains (2)		Valid Accounts (4)	Software Deployment Tools	Event Triggered Execution (15)	Exploitation for Privilege Escalation	Execution Guardrails (1)	Network Sniffing	File and Directory Discovery	Use Alternate Authentication Material (4)	Data from Network Shared Drive	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Search Victim-Owned Websites			System Services (2)	External Remote Services	Hijack Execution Flow (11)	Exploitation for Defense Evasion	OS Credential Dumping (8)	Network Service Scanning		Data from Removable Media	Non-Application Layer Protocol		Network Denial of Service (2)
			User Execution (3)	Hijack Execution Flow (11)	Process Injection (11)	File and Directory Permissions Modification (2)	Steal Application Access Token	Network Share Discovery		Data Staged (2)	Non-Standard Port		Resource Hijacking
			Windows Management Instrumentation	Implant Internal Image	Scheduled Task/Job (7)	Hide Artifacts (7)	Steal or Forge Kerberos Tickets (4)	Network Sniffing		Email Collection (3)	Protocol Tunneling		Service Stop
				Modify Authentication Process (4)	Valid Accounts (4)	Hijack Execution Flow (11)	Steal Web Session Cookie	Password Policy Discovery		Input Capture (4)	Proxy (4)		System Shutdown/Reboot
				Office Application Startup (6)		Impair Defenses (7)	Two-Factor Authentication Interception	Peripheral Device Discovery		Man in the Browser	Remote Access Software		
				Pre-OS Boot (5)		Indicator Removal on Host (6)	Unsecured Credentials (7)	Permission Groups Discovery (3)		Man-in-the-Middle (2)	Traffic Signaling (1)		
				Scheduled Task/Job (7)		Indirect Command Execution		Process Discovery		Screen Capture	Web Service (3)		
				Server Software Component (3)		Masquerading (6)		Query Registry		Video Capture			
				Traffic Signaling (1)		Modify Authentication Process (4)		Remote System Discovery					
				Valid Accounts (4)		Modify Cloud Compute Infrastructure (4)		Software Discovery (1)					
						Modify Registry		System Information Discovery					
						Modify System Image (2)		System Location Discovery					
						Network Boundary Bridging (1)		System Network Configuration Discovery (1)					
						Obfuscated Files or Information (4)		System Network Connections Discovery					
						Pre-OS Boot (5)		System Owner/User Discovery					
						Process Injection (11)		System Service Discovery					
						Rogue Domain Controller		System Time Discovery					
						Rootkit		Virtualization/Sandbox Evasion (3)					
						Signed Binary Proxy Execution (11)							
						Signed Script Proxy Execution (1)							
						Subvert Trust Controls (6)							
						Template Injection							
						Traffic Signaling (1)							
						Trusted Developer Utilities Proxy Execution (1)							
						Unused/Unsupported Cloud Regions							
						Use Alternate Authentication Material (4)							
						Valid Accounts (4)							
						Virtualization/Sandbox Evasion (3)							
						Weaken Encryption (2)							
						XSL Script Processing							

Office 365 Breach Tactics

proarch

Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Impact
2 techniques	4 techniques	1 techniques	3 techniques	5 techniques	5 techniques	2 techniques	2 techniques	2 techniques
Phishing (1)	Account Manipulation (2)	Valid Accounts (2)	Impair Defenses	Brute Force (4)	Account Discovery (2)	Internal Spearphishing	Data from Information Repositories (1)	Endpoint Denial of Service (3)
Spearphishing Link	Exchange Email Delegate Permissions	Default Accounts	Use Alternate Authentication Material (2)	Password Guessing	Email Account	Use Alternate Authentication Material (2)	Sharepoint	Service Exhaustion Flood
Valid Accounts (2)	Add Office 365 Global Administrator Role	Cloud Accounts	Application Access Token	Password Cracking	Cloud Account	Application Access Token	Email Collection (2)	Application Exhaustion Flood
Default Accounts	Create Account (1)		Web Session Cookie	Password Spraying	Cloud Service Dashboard	Web Session Cookie	Remote Email Collection	Application or System Exploitation
Cloud Accounts	Cloud Account		Valid Accounts (2)	Credential Stuffing	Cloud Service Discovery		Email Forwarding Rule	Network Denial of Service (2)
	Office Application Startup (6)		Default Accounts	Forge Web Credentials (1)	Permission Groups Discovery (1)			Direct Network Flood
	Add-ins		Cloud Accounts	SAML Tokens	Cloud Groups			Reflection Amplification
	Office Template Macros			Steal Application Access Token	Software Discovery (1)			
	Outlook Forms			Steal Web Session Cookie	Security Software Discovery			
	Outlook Rules			Unsecured Credentials				
	Outlook Home Page							
	Office Test							
	Valid Accounts (2)							
	Default Accounts							
	Cloud Accounts							

More difficult to remediate once at this stage

More accounts and systems are compromised.

Attackers own your data.

Detection and response happens during these stages. In just minutes.

Where attacks need to be stopped

Matrices

Windows
macOS
Linux
Network
Containers
Mobile
ICS

Cloud
- Office 365
- Azure AD
- Google Workspace
- SaaS
- IaaS

Real World Attack

ProArch response to successful ransomware attack

- Production down across locations
- Lost revenue
- Fine and penalties

ProArch performed

- End-to-end Incident Response
- Deployed XDR capabilities in under 4 hours

MDR prevented second attack attempt 14 days later

Client Initial Breach Notification

Containment
XDR toolkit deployed and integrated in under 4 hours. (SIEM, EDR, 24x7 SOC)

Eradication
Countermeasures deployed to mitigate the attack.

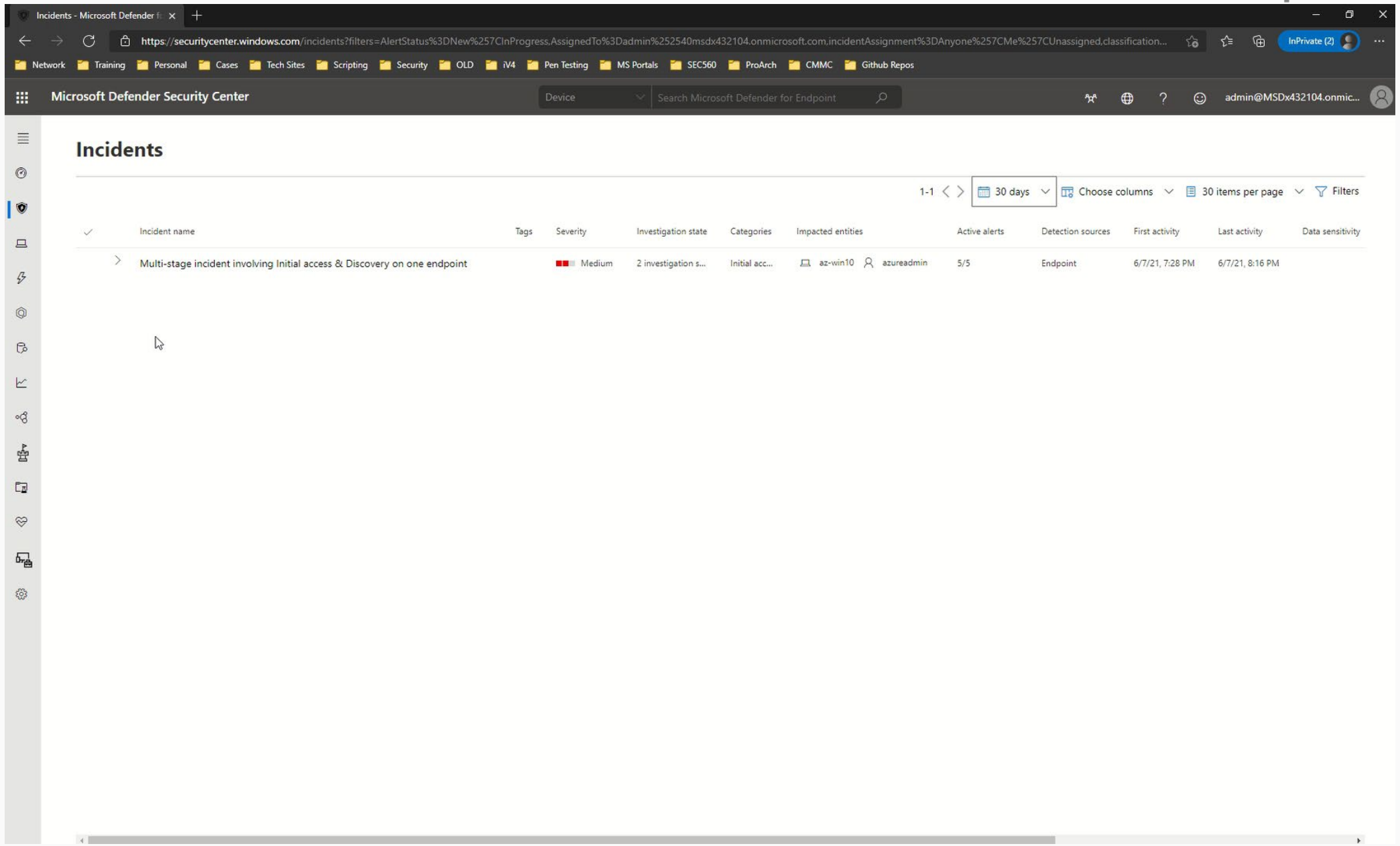
Recovery
IR Team provided 60% of production restoration within the first 72 hours.

Cleanup & Reporting
Delivery of IR report, post-incident actions, and next steps.

Hardening
Client continues with ProArch MDR Services.

Prevented Second Attack
Two weeks after recovery wrapped the MDR solution prevented a second attack.

How Threats are Responded To



Threat Intelligence: By Design

- Method by which data and insights are collected, analyzed, and automated to accelerate distinct security systems and functions
- It's a mindset; a philosophy for how intelligence drives every security initiative and strategic decision
- Brings automation and insight to the forefront of every facet of security, including strategic planning, technical design and architecture, and implementation and execution

Security Intelligence:

An outcomes-centric approach to reducing risk that fuses external and internal threat, security, and business insights across an entire organization.

Source: Recorded Future

Threat Intelligence: SecOps

A Global View of Risks to Accelerate SecOps Response

Alert Triage

50% more alerts reviewed

Prioritize and resolve alerts confidently

Threat Detection

Threats identified 10x faster

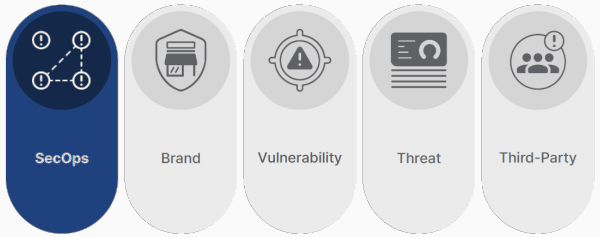
Detect previously undetected threats

Threat Prevention

22% more threats identified before impact

Block threats with less business disruption

Allows ProArch Analysts to simplify workflows with contextualized SecOps intelligence



Threat Intelligence: Threat

A Comprehensive View of Your Threat Landscape

Advanced Threat Research and Reporting

Reduce time spent compiling reports by 34%

Access the broadest set of sources in one platform

Advanced Detection and Validation

Threats identified 10x faster

Simplify threat detection and response workflows

Monitoring for Threats to Your Tech Stack

11 days faster than the NVD

Learn about product vulnerabilities before they're published

Dark Web Investigation

22% more threats identified before impact

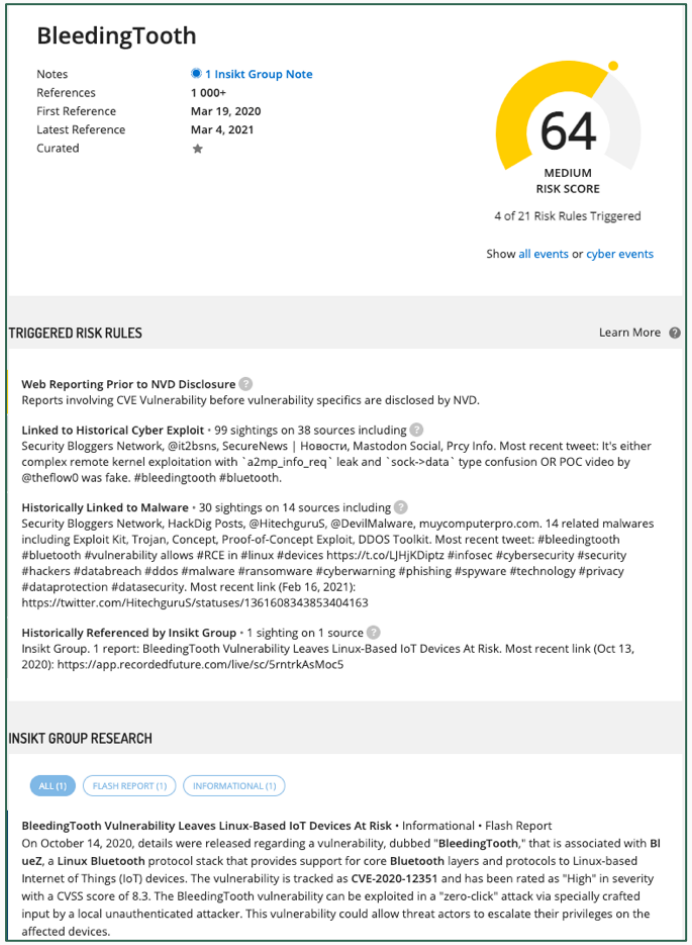
Expand your visibility of the threat landscape

Threat Intelligence: Vulnerability

A Truly Risk-Centered Approach

- Relevant, threat-based risk scores, updated in real time for fast prioritization of vulnerabilities
- Real-time alerting on vulnerabilities days before they're published in the NIST Vulnerability Database (~11 days faster)
- Detailed risk evidence and context for transparent and fast analysis by ProArch's SecOps team
- Integration into Microsoft Sentinel

86% reduction in unplanned downtime



BleedingTooth

Notes	1 Insikt Group Note
References	1 000+
First Reference	Mar 19, 2020
Latest Reference	Mar 4, 2021
Curated	★

64
MEDIUM
RISK SCORE

4 of 21 Risk Rules Triggered

Show all events or cyber events

TRIGGERED RISK RULES — Learn More

Web Reporting Prior to NVD Disclosure
Reports involving CVE Vulnerability before vulnerability specifics are disclosed by NVD.

Linked to Historical Cyber Exploit • 99 sightings on 38 sources including
Security Bloggers Network, @it2bsns, SecureNews | Новости, Mastodon Social, Prcy Info. Most recent tweet: It's either complex remote kernel exploitation with `a2mp_info_req` leak and `sock->data` type confusion OR POC video by @theflow0 was fake. #bleedingtooth #bluetooth.

Historically Linked to Malware • 30 sightings on 14 sources including
Security Bloggers Network, HackDig Posts, @HitechguruS, @DevilMalware, muycomputerpro.com. 14 related malwares including Exploit Kit, Trojan, Concept, Proof-of-Concept Exploit, DDOS Toolkit. Most recent tweet: #bleedingtooth #bluetooth #vulnerability allows #RCE in #linux #devices https://t.co/LJHjKDiptz #infosec #cybersecurity #security #hackers #databreach #ddos #malware #ransomware #cyberwarning #phishing #spyware #technology #privacy #dataprotection #datasecurity. Most recent link (Feb 16, 2021): https://twitter.com/HitechguruS/statuses/1361608343853404163

Historically Referenced by Insikt Group • 1 sighting on 1 source
Insikt Group. 1 report: BleedingTooth Vulnerability Leaves Linux-Based IoT Devices At Risk. Most recent link (Oct 13, 2020): https://app.recordedfuture.com/live/sc/5rntrkAsMocS

INSIKT GROUP RESEARCH

ALL (1) | FLASH REPORT (1) | INFORMATIONAL (1)

BleedingTooth Vulnerability Leaves Linux-Based IoT Devices At Risk • Informational • Flash Report
On October 14, 2020, details were released regarding a vulnerability, dubbed "**BleedingTooth**," that is associated with **BlueZ**, a **Linux Bluetooth** protocol stack that provides support for core **Bluetooth** layers and protocols to Linux-based Internet of Things (IoT) devices. The vulnerability is tracked as **CVE-2020-12351** and has been rated as "High" in severity with a CVSS score of 8.3. The BleedingTooth vulnerability can be exploited in a "zero-click" attack via specially crafted input by a local unauthenticated attacker. This vulnerability could allow threat actors to escalate their privileges on the affected devices.

MDR vs. MSSP

MDR vs. MSSP Comparison Chart

MDR: Services that proactively search out, validate and alert organizations of detected, current or incoming threats.

MSSP: Services that reactively respond to security events and focus primarily on defending vulnerabilities through passive technologies like firewalls. MSSPs send out alerts to IT teams when anomalies are detected but do not investigate them.

	MDR	MSSP
Alert Monitoring	✓	✓
Threat Investigation	✓	
Threat Containment	✓	
24x7 Security Operations Center	✓	
Security Information Event Management (SIEM)	✓	
Incident Response	✓	Yes (varies by provider)

Who Needs MDR?

Invested in security tools but have not fully integrated them and are not getting full value

Must adhere to compliance and/or regulatory requirements

Want to use their monetary resources for initiatives other than staffing a security team and managing a SOC

Everyone. Every company has something to lose, and attackers always have something to gain.

What MDR Isn't…

MDR is not 'all encompassing'

Foundational Attack Surface Reduction elements not included

- vulnerability management
- security awareness training
- system and infrastructure hardening
- web content filtering
- antivirus and boundary defense
- risk management
- pen testing

MDR is not a guarantee against a breach. Other risk mitigation, such as, cyber-insurance, should be considered.

MDR is not a replacement for an **incident response** or **disaster recovery plans**

Security Architecture tied to Enterprise Architecture: **Zero Trust Architect**

Regulatory Compliance: Compliance frameworks are the floor, not the ceiling.

The Investment

What to Look for in an MDR Vendor

Gartner Recommendations

Use MDR services to **add remotely delivered modern 24/7 security operations center functions in a turnkey approach** when there are no existing internal capabilities, or when the organization needs to accelerate or augment existing capabilities.

Embrace **containment actions as an incident response capability of MDR** service providers when there are no internal 24/7 operations to respond to threats that require immediate attention.

Assess how the MDR provider's **containment approach can integrate with your organization's policies and procedures.**

Ensure the MDR providers **technology stack fits well with your existing security controls** and IT environment, from on-premises to cloud.

Use MDR providers that **have experience with use cases appropriate to your organization's size, location and industry vertical**. Use any unique challenges in your industry vertical to differentiate potential providers.

Gartner Source: Gartner-Marketing Guide for Managed Detection and Response Services

MDR Service Attributes according to Gartner

24x7 SOC Attributes	ProArch MDR
Applicable technologies to detect, investigate and respond to threats.	✓
Staff that have skills and expertise in threat monitoring, detection and hunting, threat intelligence (TI), and incident response.	✓
Processes that include a standard playbook of workflows and procedures.	✓

MDR Delivery Attributes	ProArch MDR
A focus on high-fidelity threat detection and validation, geared toward attacks that have bypassed preventative security controls.	✓
Remote incident response investigation and containment activities beyond alerting and notification. Threats move too fast for most organization these days. Depending on the type of threat and the environment targeted, this could have an impact on data confidentiality, availability to operations, an impact on privacy, or even an impact on physical safety.	✓
Selective use of technologies and a turnkey model to enable the MDR provider's team to quickly implement and deliver services.	4-Hour Deployment

Justifying the Investment

Getting buy-in from the c-suite

Identification of critical business information

- Understanding what critical assets need to be protected is the first step.

Knowledge of threats and attack vectors

- The specific nature of threats needs to be examined
- Which "threat communities" pose the most risk to your organization?

Forecasting loss magnitude and loss frequency

- Losses may be categorized as theft of intellectual property, fines from compliance violations, ransomware payments, lost revenues, reputational loss, etc., and are used to estimate loss magnitude. The estimated loss frequency (more than "this may happen," but within what time period) needs to be estimated.

ROSI (Return on Security Investment) Model

$$\text{ROSI} = \frac{(\text{Risk Exposure x \%Risk Migtigated}) - \textit{Solution cost}}{\text{Solution Cost}}$$

Risk Exposure: $25,000, 4x per year = $100,000
Risk Mitigated: 75%
Solution Cost: $25,000

$$\text{ROSI} = \frac{(\$100{,}000 \text{ x } 75\%) - \$25{,}000}{\$25{,}000} = 200\%$$

In the United States, security budgets typically run at about 10.6% of the IT budget as part of total revenue.

The fact is that over the 12 years 2005 until 2019, security budgets increased by 60%, while cybersecurity risks increased by 309%.

proarch

Thank You!

Recording and slide deck will be sent out this afternoon.