proarch

ProArch's Managed Detection & Response

The Missing Piece in Your Security Strategy?

proarch

MEET OUR PRESENTERS

Ben Wilcox

Managing Director of Cybersecurity & Compliance
Chief Technology Officer

bwilcox@proarch.com
Linkedin.com/in/ben-wilcox/

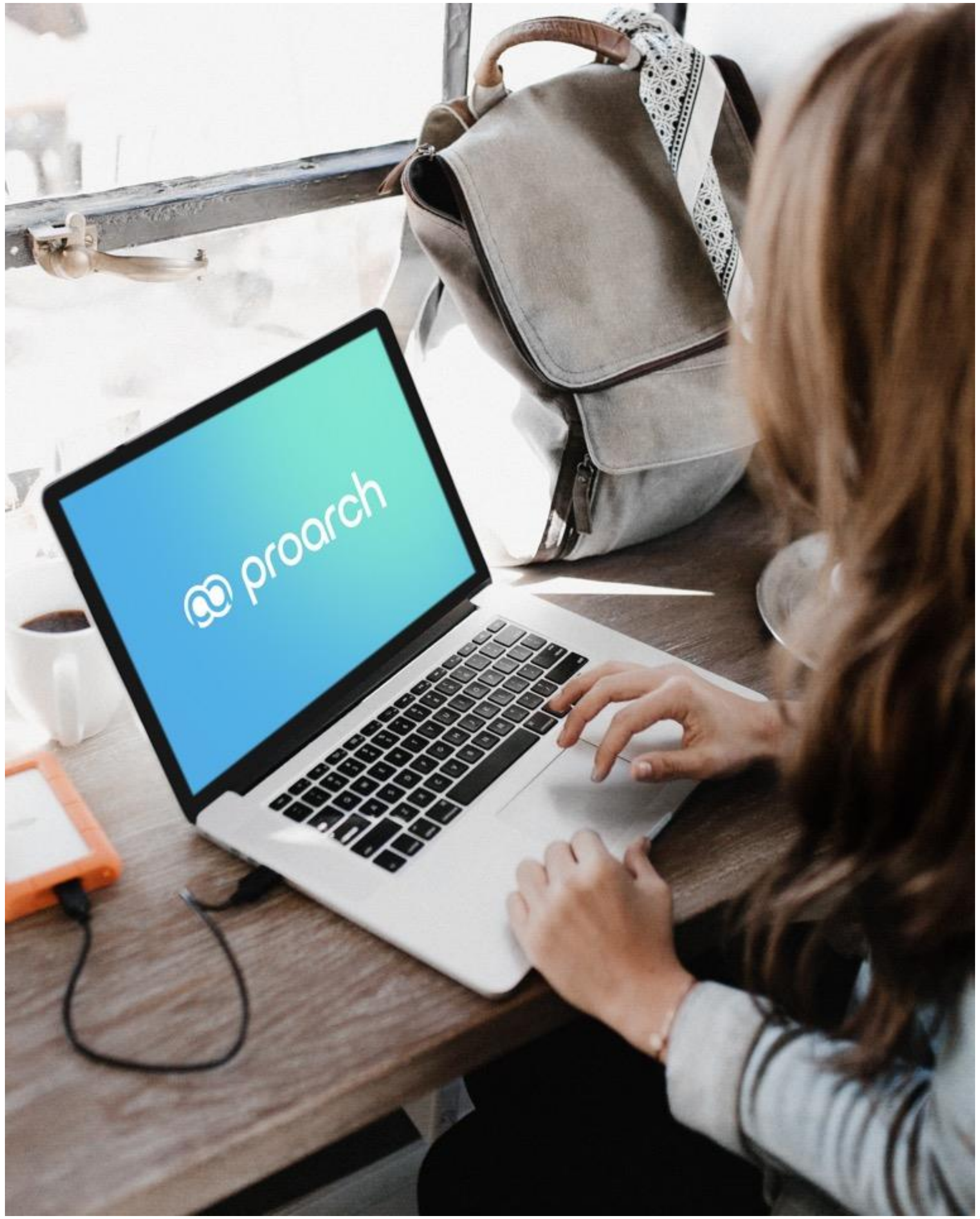
Michael Wurz

VP of Cybersecurity Solutions

mwurz@proarch.com
Linkedin.com/in/mwurz/

Agenda

- Terminology
- LIVE Attack & Response as the:
  - Attacker
  - SOC
  - Client
- Choosing the right MDR vendor
- ProArch MDR takeaways



Making Sense of All the Options

	Managed Security Service Providers (MSSP)	Outsourced SOC	Security Product Vendors (EDR, IDR, XDR)	MDR Provider
Service vs. Tech	Monitors security tools but minimal response.	Handles alerts but requires separate tools.	Provides detection tech but needs internal response.	Combines technology with 24/7 detection and response.
Threat Detection & Response	Alert-driven, basic monitoring.	Triage-focused, no direct remediation.	Strong detection, but teams must respond.	Hands-on investigation, threat containment, and response.
Human Expertise	Have other offerings and capabilities to leverage	Analysts triage alerts but lack strategic input.	Requires in-house security expertise.	Team of security experts with diverse, advanced security skills.
Integration & Customization	Uses specific tools, less flexibility.	Works with existing stacks but limited tuning.	Requires internal integration and consistent tuning.	Integrates with current tools and custom sources

Breaking Down the Costs

	Managed Security Service Providers (MSSP)	Outsourced SOC	Security Product Vendors (EDR, IDR, XDR)	MDR Provider
Cost & Resources	Similar in cost to MDR Providers Requires internal resources for investigation and response.	Mid-range cost Still requires internal staff for strategic security planning.	CapEx upfront and operational costs due to licensing Requires internal staff to manage and respond.	Similar cost to MSSPs Provides complete service, reducing the need for internal security resources.

Managed Detection & Response Criteria

Combines technology and human expertise for 24/7 threat monitoring, detection, and response

Consists of integrated services to deliver a comprehensive security strategy aligned to your business

Leverages highly skilled security experts to effectively utilize your security product solutions

100% prevention of security breaches is not possible.

MDR is about minimizing the time to detect and respond to incidents

proarch

How MDR Works

How MDR Works: Alert → Response

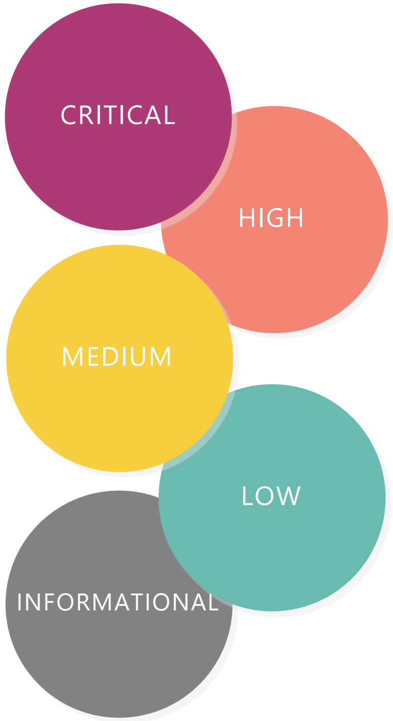
ALERT MONITORING

DATA COLLECTED FROM ACROSS THE ENVIRONMENT

- ENDPOINT
- IDENTITY
- COMMUNICATION
- CLOUD
- NETWORK

ADVANCED DETECTION TOOLS

FIND INDICATORS OF COMPROMISE & PRIORITIZE ALERTS



INVESTIGATION & RESPONSE

THREATS ARE STOPPED QUICKLY & EFFICIENTLY

24/7 Security Operations Center

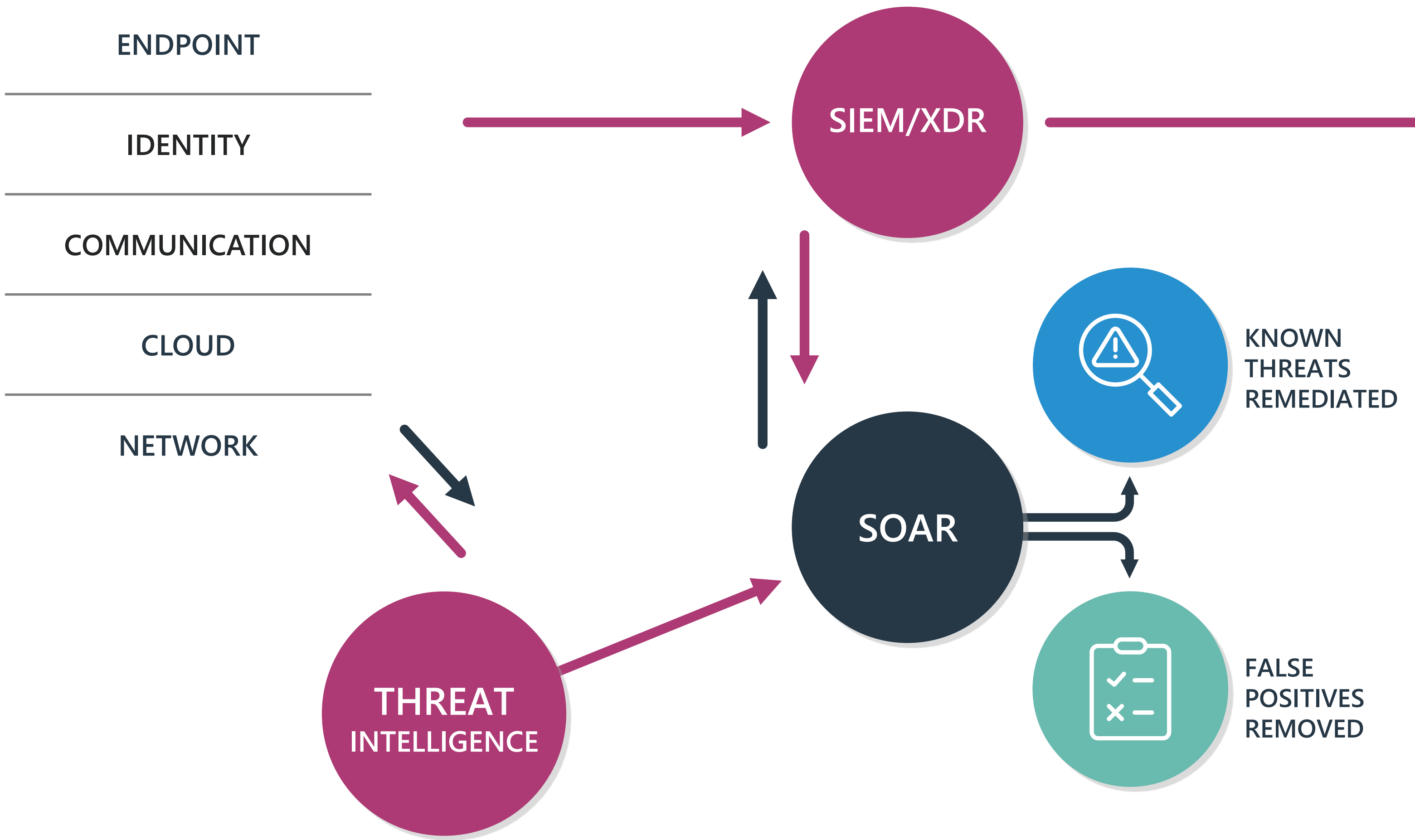
- Alert & Threat Investigation
- Threat Containment & Remediation
- Threat Hunting
- Client Communication & Coordination
- Escalation to Incident Response Team

ALERT MONITORING

DATA COLLECTED FROM ACROSS THE ENVIRONMENT

ADVANCED DETECTION TOOLS

FIND INDICATORS OF COMPROMISE & PRIORITIZE ALERTS



ENDPOINT

IDENTITY

COMMUNICATION

CLOUD

NETWORK

SIEM/XDR

SOAR

THREAT INTELLIGENCE

KNOWN THREATS REMEDIATED

FALSE POSITIVES REMOVED

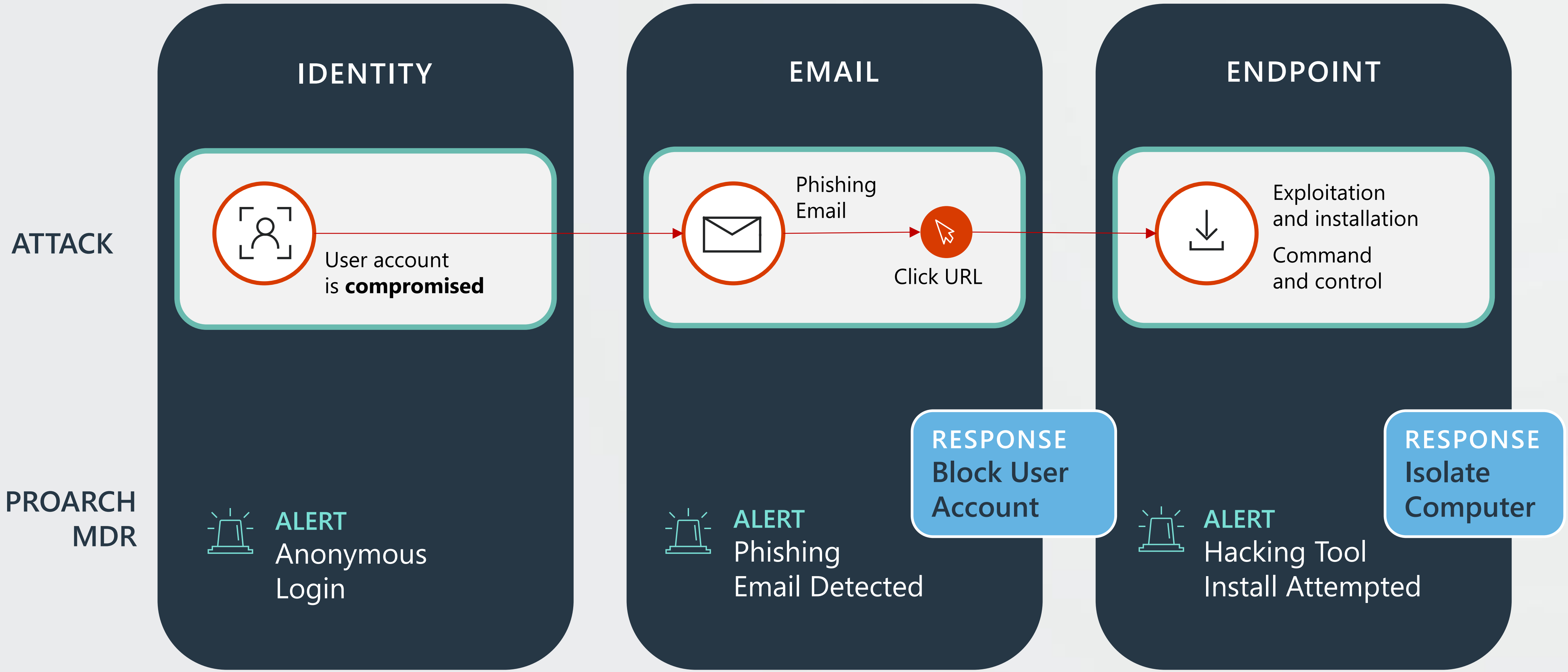
INVESTIGATION & RESPONSE

THREATS ARE STOPPED QUICKLY & EFFICIENTLY

24/7 Security Operations Center

- Alert & Threat Investigation
- Threat Containment & Remediation
- Threat Hunting
- Client Communication & Coordination
- Escalation to Incident Response Team

A Typical Account Compromise Attack



ATTACK

PROARCH MDR

IDENTITY

User account is **compromised**

ALERT

Anonymous Login

EMAIL

Phishing Email

Click URL

ALERT

Phishing Email Detected

RESPONSE

Block User Account

ENDPOINT

Exploitation and installation

Command and control

ALERT

Hacking Tool Install Attempted

RESPONSE

Isolate Computer

LIVE Attack & Response Simulation

proarch

MDR Vendor Evaluation

What to look for in your MDR provider.

Detection, investigation, AND response.

Turnkey offering.

- Compatibility with your technology stack
- Complements your resources.

Support your security vision.

- Flexible and open to change.
- Advise not dictate.
- Will do a Proof of Concept.

No black box.

- Vendor’s actions are visible to you.
- High-Fidelity Detection Management

Clear communication and reporting.

- Ensure prompt communication channels are outlined.
- Ensure quality reporting is done routinely. Ask for a sample report.

Forward-thinking and advanced technology utilization.

- Vendor should safely utilize advanced technologies to improve your experience and enhance MDR functions: SOAR, AI, Automation.

ProArch MDR Takeaways

ProArch MDR Options: Core & Premier

	MDR Core	MDR Premier
24/7/365 SECURITY MONITORING & RESPONSE	Included	Included
ENDPOINTS	Included	Included
IDENTITIES	Included	Included
EMAIL & COLLABORATION	Included	Included
EXTENDED DETECTION & RESPONSE (XDR)	Included	Included
SIEM HOST & NETWORK	-	Included
CLOUD APPS	-	Included
CLOUD PLATFORMS	-	Included
OPERATIONAL TECHNOLOGY (OT)	-	Included
PROACTIVE INCIDENT RESPONSE	Included	Included
STRATEGIC SECURITY ADVISORY SERVICES	-	Included
MONTHLY THREAT HUNTING	-	Included

- Tailored Threat Intelligence Briefings
- Detection & Automation Rule Management
- Automation & Orchestration Playbooks
- Alert & Incident Management Portal
- Monthly Maintenance & Security Health Check Report

What MDR Covers

	ENDPOINT	IDENTITY	COMMUNICATION	CLOUD INFRASTRUCTURE	CLOUD APPS	SIEM	CUSTOM SOURCES	IOT/OT
WHAT'S COVERED	**Servers:** Linux and Windows **Workstations:** Linux, Windows, MacOS **Mobile Devices:** iOS, Android	On-premises Active Directory Azure AD/ Entra ID	Exchange Online Microsoft Teams Microsoft SharePoint Microsoft OneDrive	Microsoft Azure Amazon Web Services Google Cloud Platform	Microsoft 365 Apps Third-party Cloud Apps	**Workstations:** Linux, Windows, **Network Devices:** Firewall, Switches, Routers **Logs:** Web, Cloud, Identity, Security *300+ connectors available.*	Databases Applications AI + Machine Learning Custom Integrations	*Industries we work with.* Manufacturing Health Care Transportation Utilities Energy Retail
TECH STACK	Microsoft Defender for Endpoint Microsoft Defender for Servers CrowdStrike Falcon EDR	Microsoft Defender for Identity Microsoft Entra ID Identity Protection CrowdStrike Falcon Identity	Microsoft Defender for Office 365 Mimecast	Microsoft Defender for Cloud	Microsoft Defender for Cloud Apps	Microsoft Sentinel	Microsoft Sentinel	Microsoft Defender for IOT

Your Next Steps

1. Start with defining your goals
2. Evaluate your current security posture
3. Consider your resources & capabilities
4. Evaluate MDR vendors
5. Craft your security strategy, your MDR vendor should be able to help!
6. Implement your strategy with your MDR vendor
7. Continuous engagement & improvement

proarch

Questions?

proarch

THANK YOU FOR JOINING US | PROARCH.COM