MHEC SECURITY SERVICES SERIES WEBINAR:

Improving Your Cybersecurity Posture

January 26, 2022

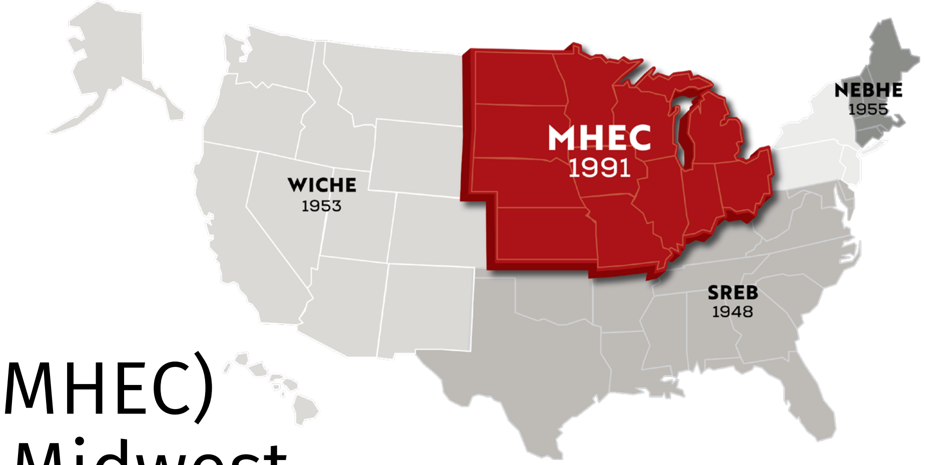
Resources available on the MHEC website post-event.

Submit questions in the Q&A.

Please complete our survey.

MIDWESTERN
HIGHER EDUCATION
COMPACT

About MHEC



- Midwestern Higher Education Compact (MHEC) was legislatively created and serves the Midwest census region (12 states)
- Governed by 60 commissioners plus commissioner alternates
- One of four regional higher education compacts (MHEC, WICHE, SREB, NEBHE)
- MHEC's technologies program includes a community of institutional volunteers offering advice and guidance to MHEC, as well as a technology contracts portfolio designed to meet the community's needs

MIDWESTERN HIGHER EDUCATION COMPACT

MHEC Technologies Community

- The Technologies Community engages IT innovators and specialists from services areas for technology, academia, students, and administration.
- The community provides strategic guidance to MHEC on technology-related topics in support of the mission of higher education institutions and states in the Midwest.
- The community helps identify opportunities for contracts that will serve higher education needs.

Deb Kidwell
MHEC Consultant
Debk@mhec.org

MIDWESTERN HIGHER EDUCATION COMPACT

MHEC Technology Contracts

- Sustain and advance affordable, high-quality educational opportunities through cost-savings initiatives
- MHEC's technology contracts are known and used by higher education IT and procurement offices
- As technology's role in higher education has grown, contracts are needed that might not traditionally be considered 'technology'
- Learn more about MHEC Contracts: MHEC.org/contracts

Contact: Nathan Sorensen
Dir of Govt Contracts
(612) 677-2767
nathans@mhec.org

MIDWESTERN
HIGHER EDUCATION
COMPACT

MHEC SECURITY SERVICES SERIES WEBINARS:

- *January 26, 11:00 a.m. CT, Improving Your Cybersecurity Posture*
- February 15, 11:00 a.m. CT, Educator's Guide to Outsmarting the Puppet Master
- March 16, 11:00 a.m. CT, Ransomware Threat Briefing/ State of the Threat Landscape
- April 12, 11:00 a.m. CT, Building a Culture of Information Security
- May 3, 11:00 a.m. CT, Security Awareness Training

Today's webinar

- Presented in partnership with Pondurance
- MHEC Contract #MHEC-09032021-PO
- Competitively bid solicitation
- Threat Intelligence, SIEM, Managed Security Services, consulting, and training services
- All higher education institutions within the MHEC region, both public and private not-for-profit, are eligible to utilize this contract

PONDURANCE

Improving Your Cybersecurity Posture

Ron Pelletier

Founder & Chief Customer Officer

Today’s Speaker

Ron Pelletier

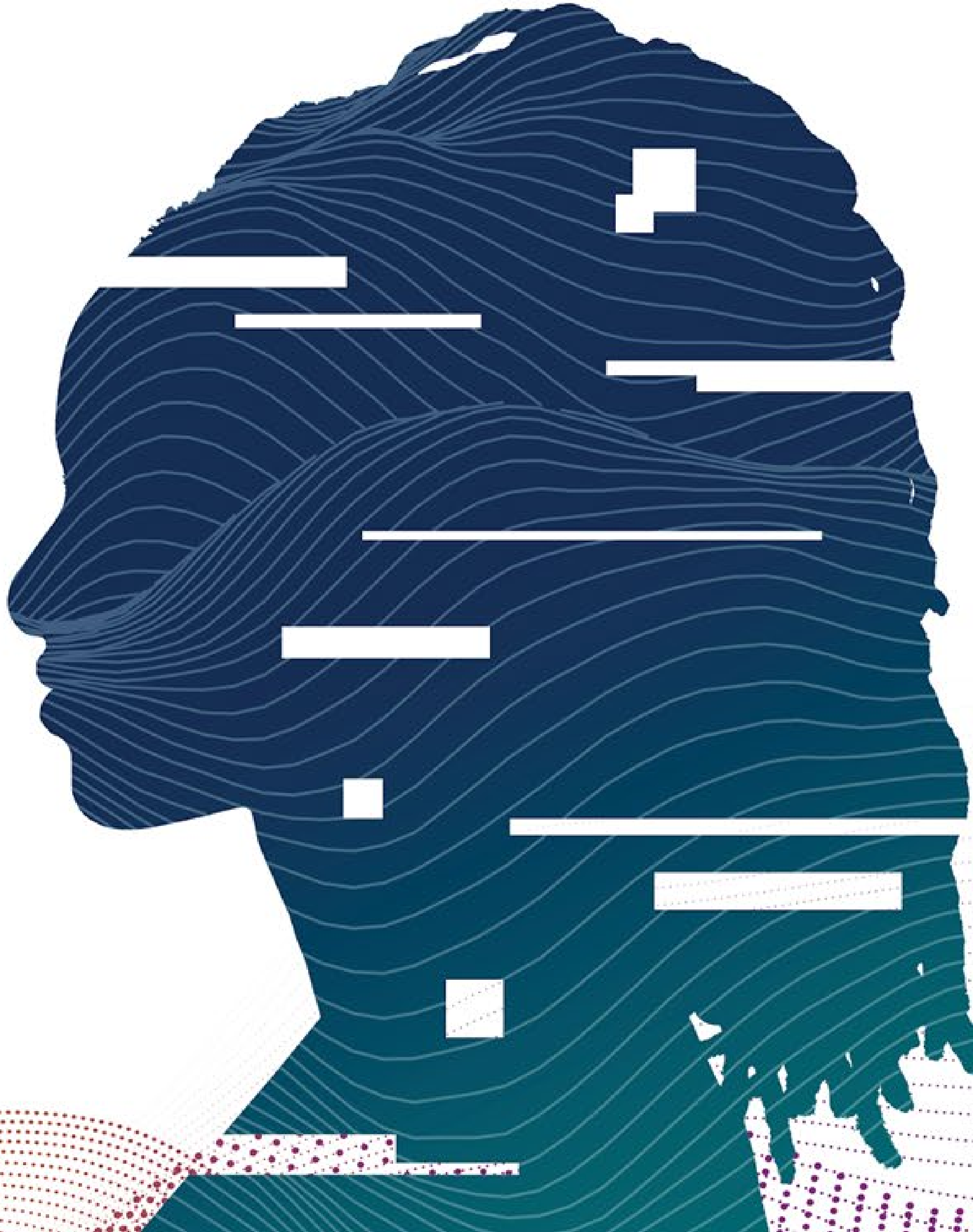
Founder & Chief Customer Officer

PONDURANCE

PONDURANCE

CONTENTS

- Bad Actor Motivations
- Common Cyberattacks
- Formulating Your Program
- Starting with Risk Analysis
- Understanding Common Practices
- Minimum Control Considerations



BAD ACTOR MOTIVATIONS

PONDURANCE

WHAT MOTIVATES BAD ACTORS & WHY SHOULD I BE CONSIDERED A TARGET?*

- **Street Cred** — Proving they can do it for their own ego
- **Hactivism/Denial of Service** — Keeping you from operating
- **Steal & Use Your Data** — Corporate espionage to gain market share
- **Steal & Sell Your Data** — Identities/credit cards sold on the dark web
- **Steal Your CPUs & Bandwidth** — Cryptojacking spikes with cryptocurrency price
- **Steal Your Money** — Propagating fraud puts money directly in their pockets
- **Hold Your Data Hostage** — Ransomware and extortion are now slowing down

Most cyberattacks are

FINANCIALLY MOTIVATED

*This excludes the motivation of state-based cyber warfare.

EXAMPLES/ CASE STUDIES

- **Street Cred** — Capital One (August 2019): Paige Thompson "steals" consumer data ostensibly to draw attention to herself and mental health issues
- **Hactivism/Denial of Service** — Kelloggs (December 2021): Cereal maker Kellogg was temporarily thwarted in its attempt to hire replacements for striking workers by members of the Reddit r/Antiwork board angry about how Kellogg was handling the strike; Reddit hacktivists flooded the hiring site with bogus job apps and a spam campaign
- **Steal & Use Your Data** — Chinese Industrial Espionage (July 2020): 11 years of intellectual property theft (among other malfeasance) attributed to 2 Chinese nationals against multitude of U.S. companies, government agencies
- **Steal & Sell Your Data** — Equifax (2017): The private data of 148 million consumers affected by what is the sixth largest data security breach in history
- **Steal Your CPUs & Bandwidth** — RubyGem (2019): 11 RubyGem language repositories infected, exposing thousands of users to cryptomining code
- **Steal Your Money** — Financial Fraud Through Cybercrime (2021): Federal authorities have arrested hundreds of cybercriminals that are part of an international group conducting cyber financial fraud. This group successfully scams victims through complex schemes involving email, invoice fraud, e-commerce, payroll, and social engineering.
- **Hold Your Data Hostage —** 2014-2020: Over 100 million cases recorded since 2014, averaging an attack every 11 seconds and estimated to cost $20B by 2021

PONDURANCE

COMMON CYBERATTACKS

PONDURANCE

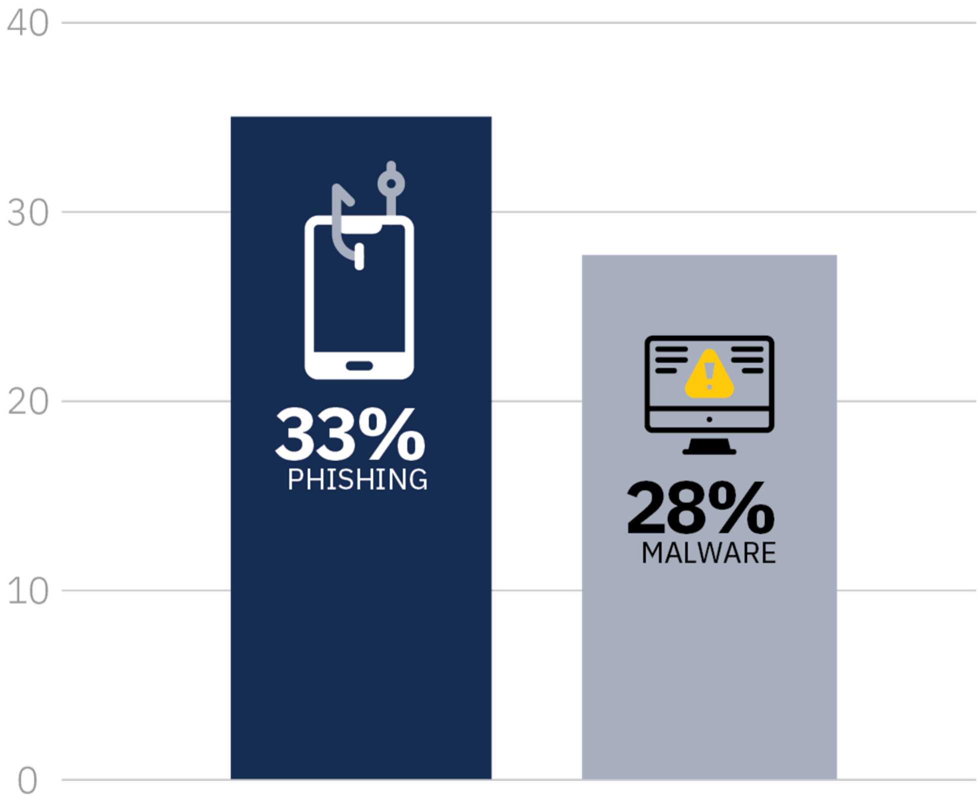
RANSOMWARE

- 100 million ransomware cases have been observed over the last 4 years
- New cases occur every **11 seconds**
- Cost of a data breach is **$3.8m per incident**
- Cyberattacks affect more than just consumer data
  - Business reputation
  - Financial losses associated with paying a ransom, damage to internal systems, and cost to recover
  - Fines

Source: Pondurance Security Operations Report 2021 Q1

PHISHING

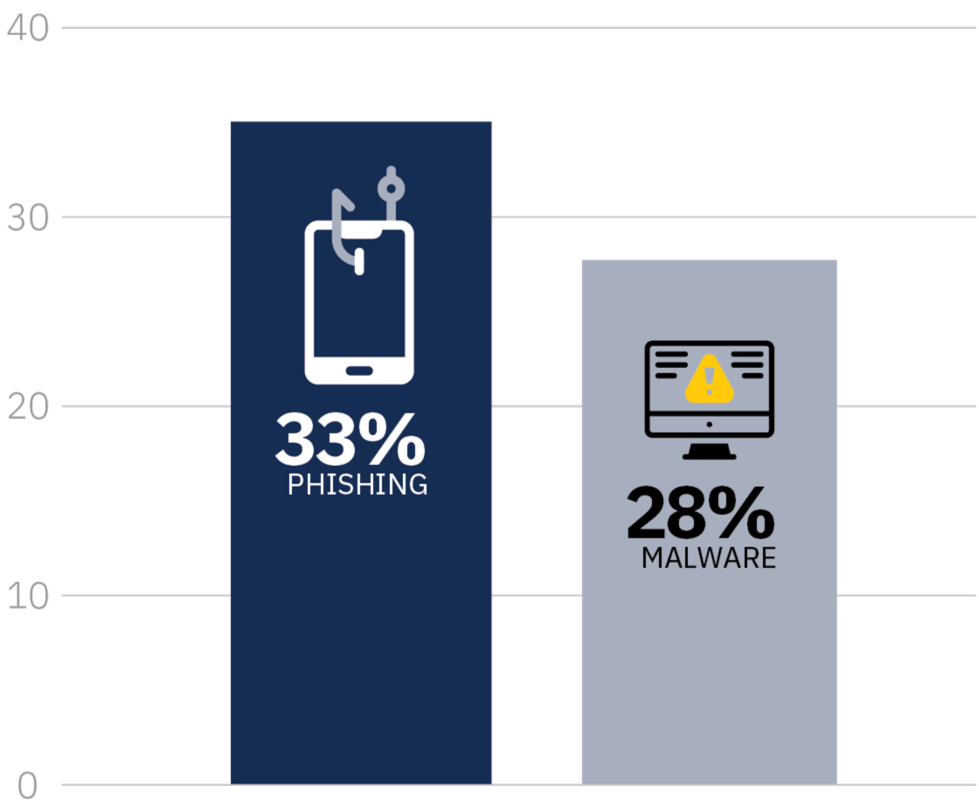
- Phishing attacks continue to be the top attack type seen by our analysts
- 33% of attacks detected were phishing attacks
- Malicious attacks that involve phishing, destructive files, and malware cost an organization upwards of $4.4 m per incident



Source: Pondurance Security Operations Report 2021 Q1

MALWARE

- Malware = Malicious + Software
- Malware is a top attack type that Pondurance has detected
- 28% of attacks detected were malware



Source: Pondurance Security Operations Report 2021 Q1

PONDURANCE

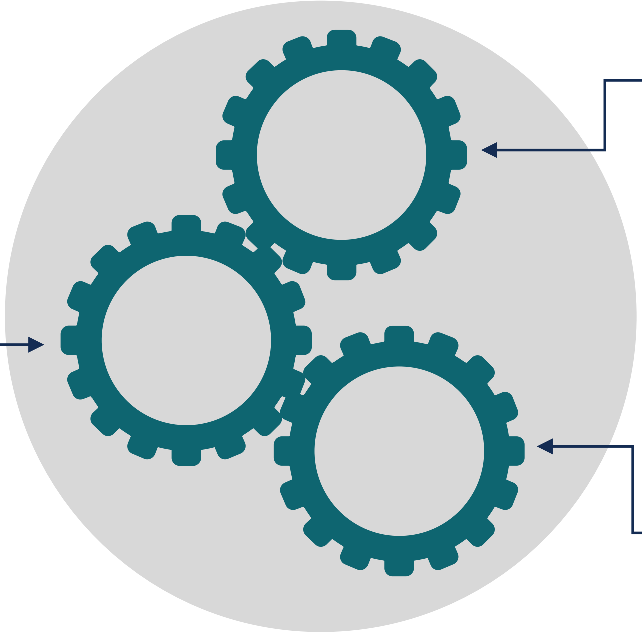
HUMAN ERROR AND MISCONFIGURATIONS

- Leading cause of data breaches are caused by human error and misconfigurations
- 19% Cloud Misconfigurations
- 19% Compromised User Credentials
- 16% Vulnerability in 3rd Party Software
- Third party vendors can be the weakest link when it comes to domain controller compromises

Source: Pondurance Security Operations Report 2021 Q1

FORMULATING YOUR PROGRAM

THE BASIC PRINCIPLES OF SECURITY (THE CIA TRIAD)



INTEGRITY

Assure data or systems cannot be modified in an unauthorized manner

CONFIDENTIALITY

Prevent or limit the unauthorized disclosure of information or access to information systems

AVAILABILITY

Information and systems are readily available for authorized users when needed

WHAT IT MEANS TO FRAME YOUR PROGRAM

- A security framework provides a meaningful basis to **right-size your security investment** using control objectives to mitigate risk (i.e., align your spend with your risk tolerance)
- The Risk Assessment is the **fundamental starting point:** what do you have, who would want it, where does it live, what's the impact if it were lost, unavailable or compromised, and HOW DO I PROTECT IT?
- The controls that achieve security objectives can be **formulated from a mix** of prescriptive and general techniques (allows flexibility and conformity)
- A framework allows the organization to **evaluate and track** its security effectiveness over time, and **make necessary changes** as technology, operations change
- A framework harmonizes organizational effort to achieve **right-sized security** AND **meet compliance requirements**

PONDURANCE

CUSTOMER PAIN POINTS

Shortage of cybersecurity talent

Security professionals that are expensive to hire and hard to retain

Security technology is expensive and hard to maintain

Difficulty managing multiple tools and investigating all alerts

Technology alone can’t deter motivated attackers

New compliance and regulation requirements

Undocumented processes in event of an attack or breach

Lack of visibility across the enterprise

Inability to quickly remediate or reduce attacker dwell time

PONDURANCE

STARTING WITH RISK ANALYSIS

PONDURANCE

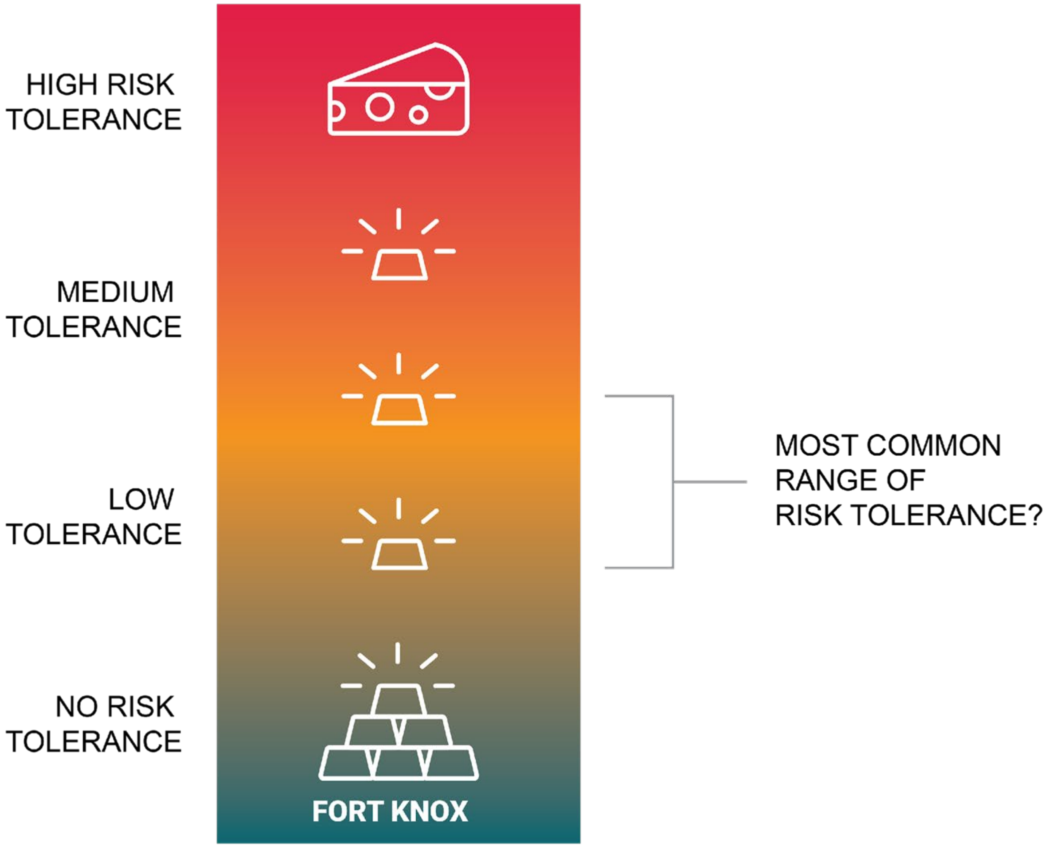
PRECURSORS FOR MEANINGFUL RISK ANALYSIS

- **What do you have?** – Your business industry and operating model generally paints a picture of inherent risk, and the type of data (or criticality of infrastructure) you have in your custody, or that you are ultimately responsible for even if it leaves your environment.
- **Who would want it?** – As covered in the "motivations" slide, you can assume that bad actors are opportunists and will target any org that contributes to their gain. However, certain types of data provide more specific motivation (and commensurate threat) and should be evaluated accordingly, and a likelihood of disruption should be estimated.
- **Where does it live?** – Be sure to take inventory of your digital assets, including the type of data that is processed, stored or transmitted by each in order to provide for a stronger classification scheme and commensurate control set. You should establish a data flow (incoming and outgoing) that includes data that leaves your environment (e.g., to service providers, B2B partners, etc.).
- **What is the impact if lost, unavailable or compromised?** – This will ultimately determine the rigor of control that should be applied to individual or asset sets. The result of impact can then be paired with likelihood to provide evaluation for appropriate mitigation.
- **How do I protect it?** – These are the critical decisions the org needs to make, once a range of inherent risk through residual risk has been identified and classified (i.e., likelihood and impact). This will formulate the prevent and detect controls that should be applied, taking stock of present effectiveness and existing deficiencies.

PONDURANCE

THE CONCEPT OF RISK TOLERANCE

How Much “Security” is Required for the Organization?

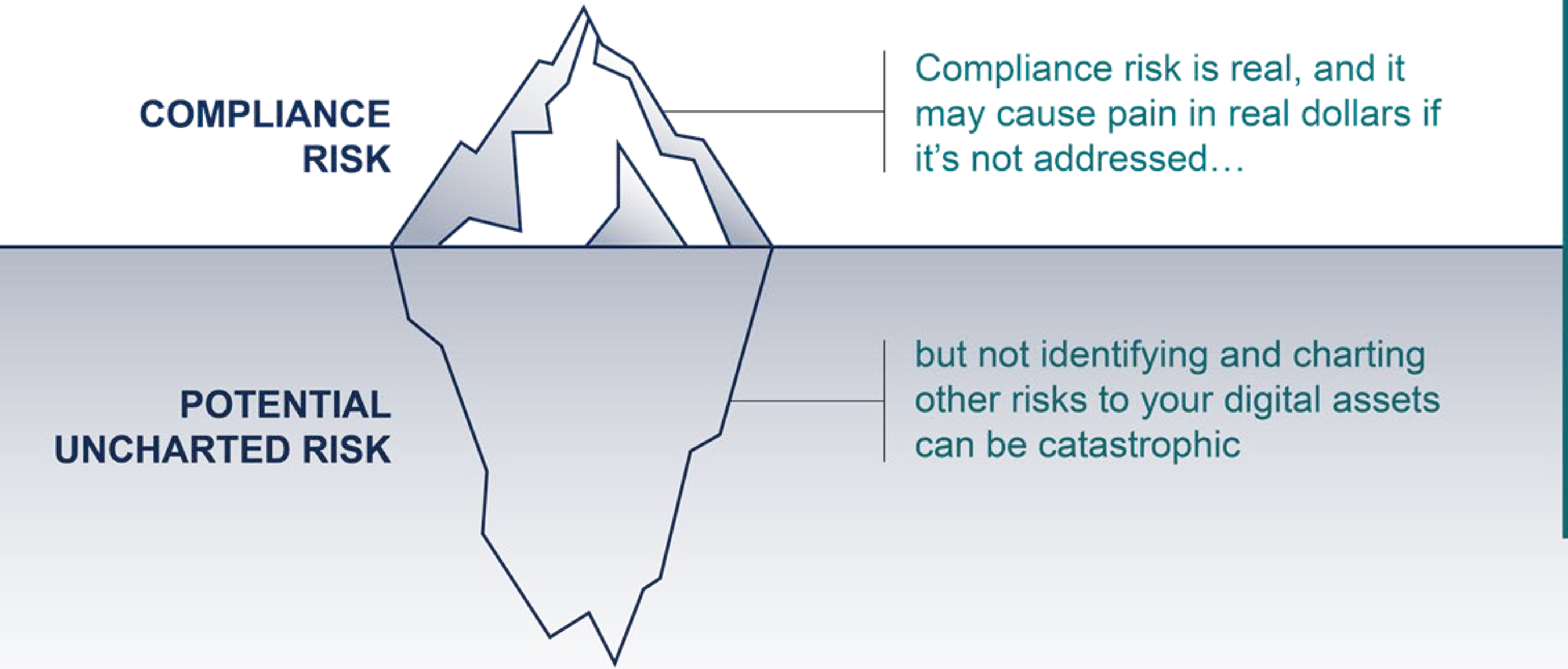


- An integrated, enterprise risk analysis should dictate the level of control and commensurate spend
- The level of “tolerance” becomes management’s definition of risk acceptance following the analysis
- The results of the risk analysis provide greater precision to develop safeguards and processes
- Even the slim range depicted here influences the austerity of those safeguards and processes

PONDURANCE

THE CONCEPT OF RISK TOLERANCE

How Much “Security” is Required for the Organization?



COMPLIANCE RISK

Compliance risk is real, and it may cause pain in real dollars if it’s not addressed…

POTENTIAL UNCHARTED RISK

but not identifying and charting other risks to your digital assets can be catastrophic

An effective Enterprise Security Program addresses risk in all facets, with appropriate measure, where information and information assets are under threat

PONDURANCE

Understanding Common Practices

SUMMARY OF COMMON SECURITY TERMINOLOGY

How Much “Security” is Required for the Organization?

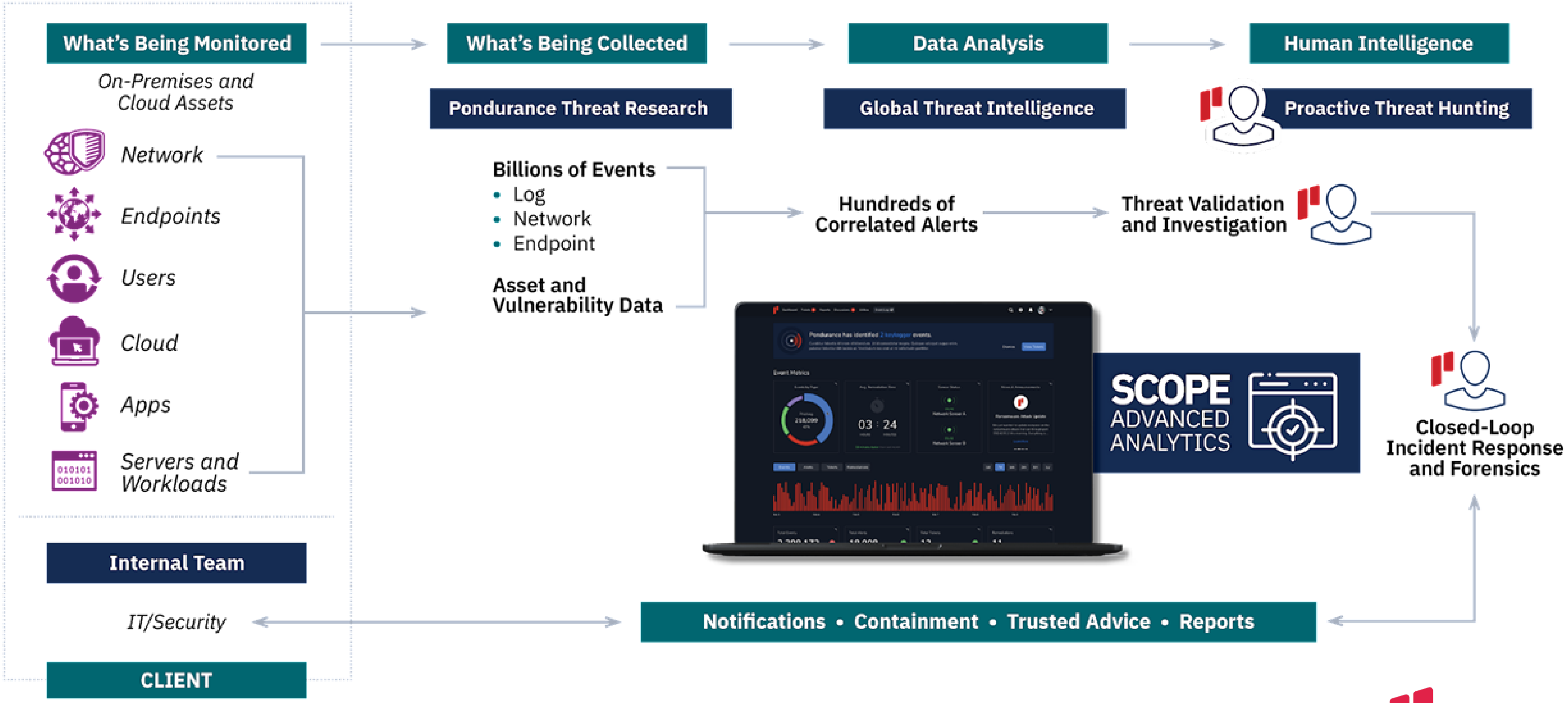
MDR VS **MSSP**

- **MDR vs MSSP –** A traditional Managed Security Services Provider performs an initial triage of system generated security alerts, creates a ticket, and passes the event for confirmation back to the entity. Managed Detection and Response is predicated on dynamic threat detection that involves hunting for indicators of attack and/or compromise rather than waiting for technology alone to find it, and it involves the human analyst in confirming the event to provide appropriate incident response.

MDR Illustrated

Artificial Intelligence and Machine Learning

Meet Human Experience, Intuition, and Unwavering Curiosity



What's Being Monitored

On-Premises and Cloud Assets

Network

Endpoints

Users

Cloud

Apps

Servers and Workloads

Internal Team

IT/Security

CLIENT

What's Being Collected

Pondurance Threat Research

Billions of Events
- Log
- Network
- Endpoint

Asset and Vulnerability Data

Data Analysis

Global Threat Intelligence

Hundreds of Correlated Alerts

Human Intelligence

Proactive Threat Hunting

Threat Validation and Investigation

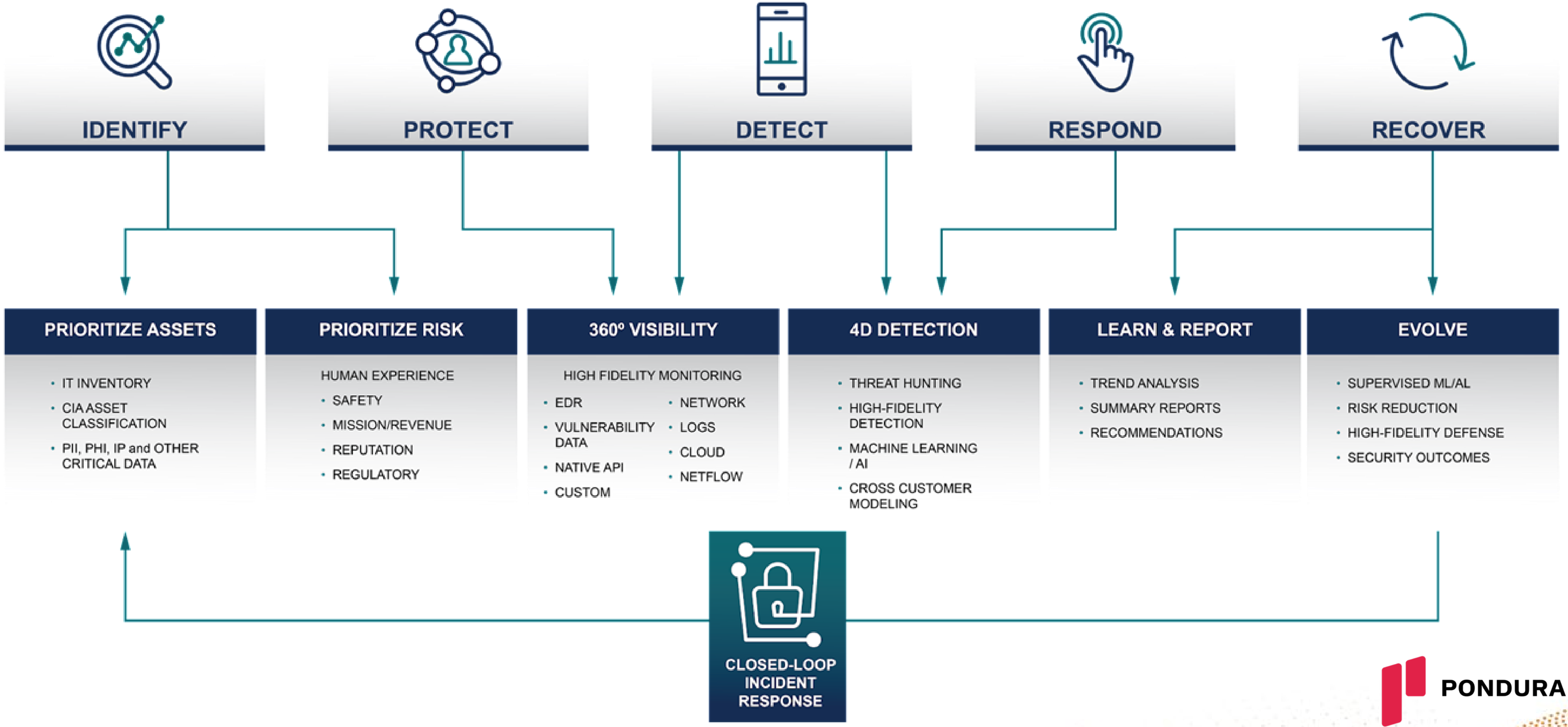
Closed-Loop Incident Response and Forensics

SCOPE ADVANCED ANALYTICS

Notifications • Containment • Trusted Advice • Reports

PONDURANCE

Dynamic Defense Methodology



IDENTIFY

PROTECT

DETECT

RESPOND

RECOVER

PRIORITIZE ASSETS

- IT INVENTORY
- CIA ASSET CLASSIFICATION
- PII, PHI, IP and OTHER CRITICAL DATA

PRIORITIZE RISK

HUMAN EXPERIENCE

- SAFETY
- MISSION/REVENUE
- REPUTATION
- REGULATORY

360º VISIBILITY

HIGH FIDELITY MONITORING

- EDR
- VULNERABILITY DATA
- NATIVE API
- CUSTOM
- NETWORK
- LOGS
- CLOUD
- NETFLOW

4D DETECTION

- THREAT HUNTING
- HIGH-FIDELITY DETECTION
- MACHINE LEARNING / AI
- CROSS CUSTOMER MODELING

LEARN & REPORT

- TREND ANALYSIS
- SUMMARY REPORTS
- RECOMMENDATIONS

EVOLVE

- SUPERVISED ML/AL
- RISK REDUCTION
- HIGH-FIDELITY DEFENSE
- SECURITY OUTCOMES

CLOSED-LOOP INCIDENT RESPONSE

PONDURANCE

MINIMUM CONTROL CONSIDERATIONS

SUMMARIZE BENEFITS OF USING A PROGRAM

- **Right-Size Your Program** – Evaluating risk and establishing a commensurate set of controls for mitigation (on the basis of risk tolerance) provides the greatest opportunity for increased ROI, and appropriately allocating security investment.
- **Evaluate and Evolve** – A program allows you to measure the effectiveness and success of your security posture, and ensures that mitigation requirements shift with the business to maintain effective and sustained security.
- **Facilitates Balanced Control Set** – While technical prevent controls are strong and necessary to mitigate some threats, an over-reliance on technology creates gaps that can be exploited…a program helps balance technical and operational controls that contain both prevent and detective controls
- **Plan to Avoid, Prepare to Response** – While low hanging risk can be effectively mitigated (assuming control discipline is maintained), a security program provides for a strong Incident Response process that is predicated on known risk scenarios, yet can be applied should the unknown occur.
- **YOU DON'T HAVE TO BE FORT KNOX** – In re-emphasizing the first point above, you cannot prevent all forms of threat occurrence, nor should you try, as it will likely impinge the flow of business and data. Sometimes being just good enough is acceptable

PONDURANCE

YOU DON’T NEED TO OUTRUN THE BEAR

While targeted attacks can and do occur, the majority of cyberattacks are based on opportunity, and bad actors are staunch opportunists. If you can eliminate your low hanging fruit…

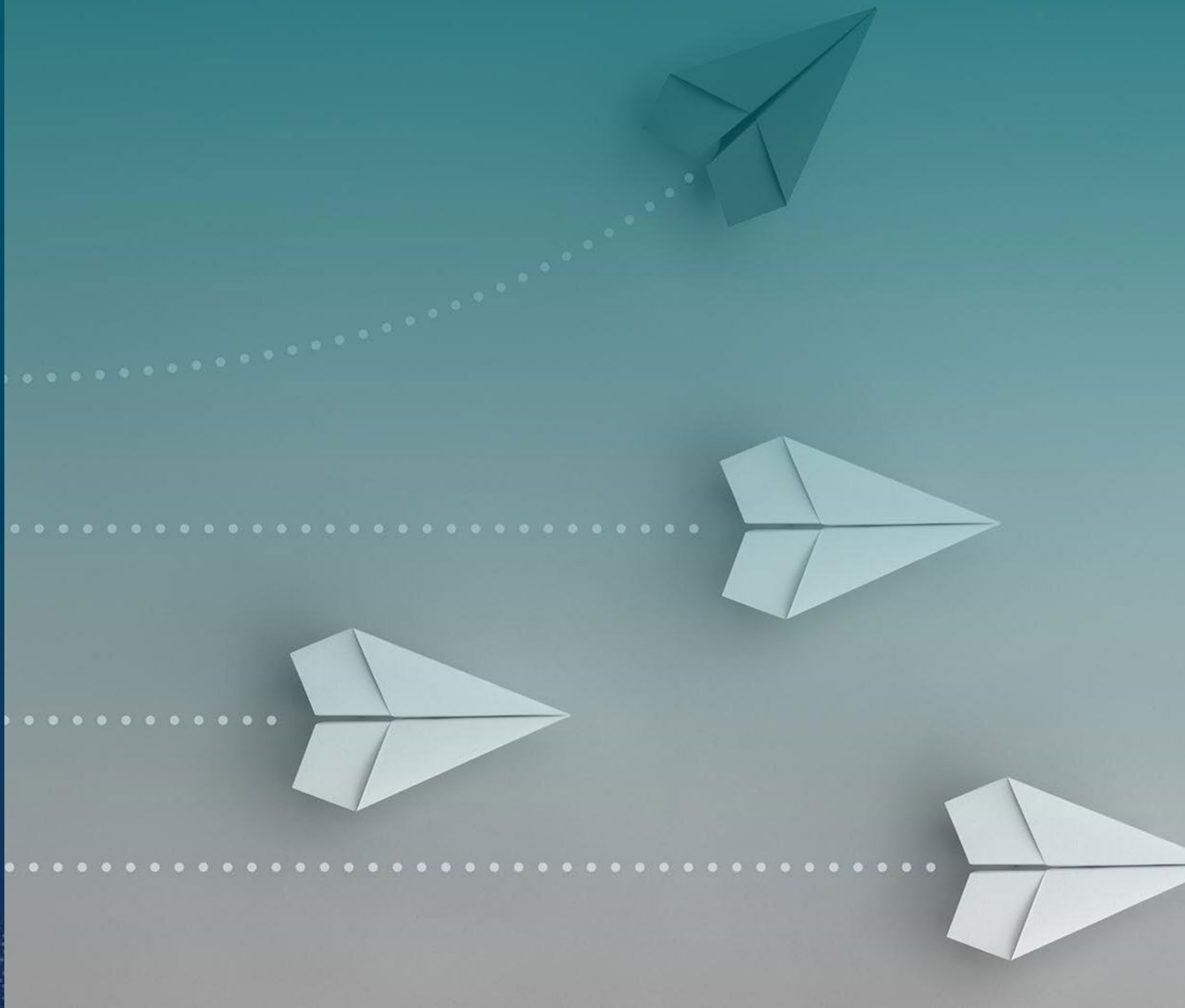
…then that allows you to outpace other orgs and be less of a target (i.e., a concept known as “limiting your attack surface,” or more flippantly… “just run faster than the other guy!”)

MINIMUM CONTROL CONSIDERATIONS

- **Protect the Domain Controller** – If an attacker gains domain administration, they are free to effectuate any number of attacks that affect Confidentiality, Integrity and/or Availability
- **Mobile Disk Encryption** – If the data on a mobile device is encrypted properly, and that device is lost, your loss it mitigated to the cost of replacing the asset
- **Vulnerability Management** – New system vulnerabilities are discovered daily and coupled with weak system configurations, can create tempting fruit for bad actors
- **Multi-Factor Authentication** – A password as a single factor of authentication provides a strong breach opportunity when it is compromised…and it's likely to happen
- **Next-Gen Antivirus** - Legacy antivirus programs work using signatures, which can be easily circumvented. The next-gen products (Endgame, Cylance) work using algorithms and are 90-94% effective against all malware
- **Managed Detection and Response** – You need people to counter people, and an over-reliance on technology alone is a big risk
- **User Awareness Training** – People need to be trained, and trained, and trained to recognize cyber security risk

PONDURANCE

QUESTIONS?



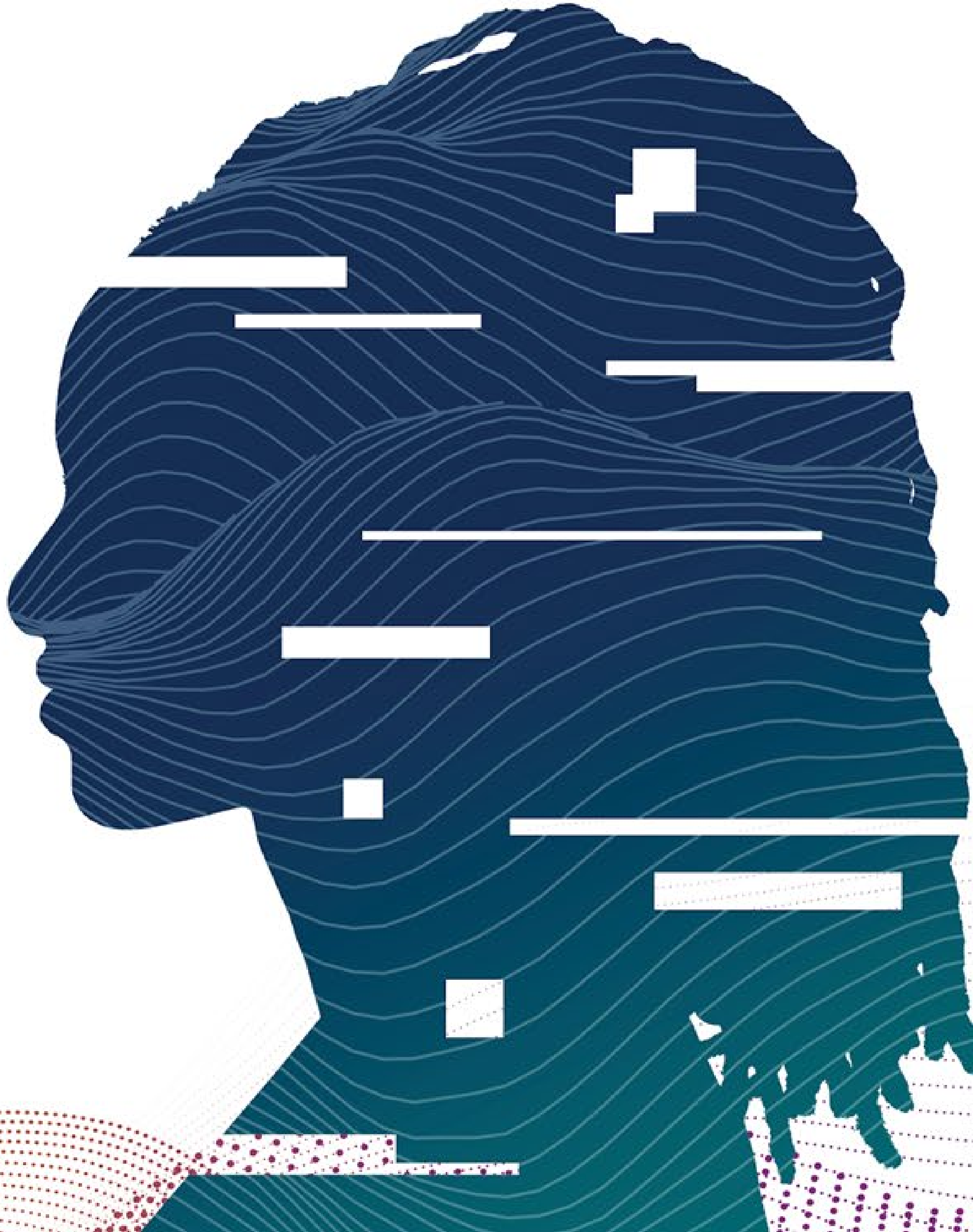
PONDURANCE

About Pondurance

Pondurance delivers world-class **MDR** services to industries facing today's most pressing and dynamic cybersecurity challenges including ransomware, complex compliance requirements, and digital transformation accelerated by a distributed workforce. By combining our advanced platform with our experienced team of analysts, we continuously hunt, investigate, validate, and contain threats so your own team can focus on what matters most.

Pondurance experts include seasoned security operations analysts, digital forensics and incident response professionals, and compliance and security strategists who provide always-on services to customers seeking broader visibility, faster response and containment, and more unified risk management for their organizations.

Visit **www.pondurance.com** for more information.



pondurance.com

500 N. Meridian St., STE. 500
Indianapolis, IN 46204