PONDURANCE

The Unexpected Compliance Benefits of Managed Detection and Response (MDR)

Maximize the use of MDR to meet regulatory compliance requirements



Dustin Hutchison, Ph.D.
Vice President of Services and Chief Information Security Officer

PONDURANCE

Agenda

Introduction

Defining Managed Detection and Response

Reviewing the Expected Benefits

Understanding Unexpected Benefits

Finding the Unexpected Benefits



Why MDR?

Reactive response

- A struggle to keep up with the latest threats and attack vectors
- Too many alerts (from too many tools) to review and investigate
- Failed MSSP/SIEM initiatives
- Limited ability to proactively hunt for threats

Insufficient resources

- Limited funding for security operations to focus on large security strategy
- SIEM and other security tools are labor-intensive
- Difficulty attracting and retaining security talent
- Not enough time to cover the basics

Evolving regulations

- Industry-specific compliance requirements
- Complex digital regulatory requirements for data, privacy, and breaches
- Inability to dynamically mitigate compliance risk

PONDURANCE

Traditional Managed Detection and Response (MDR) Services



Traditional MDR is a ***managed service*** that provides cybersecurity experts to organizations with limited resources or lack the expertise to monitor their attack surface 24/7, typically across telemetry only from:

- Networks
- Endpoints

Extended Detection and Response (XDR) Platform



XDR is a ***software technology*** that broadens the scope of conventional endpoint detection and response (EDR) tools to include telemetry from:

- Networks
- Endpoints
- Logs (e.g., from a SIEM tool)
- Clouds (e.g., AWS, Azure, GCP)

Something Something Something Detection and Response

The acronyms will continue to evolve, but the needs and expectations of organizations at a base level have been consistent, especially based on the speed of regulatory compliance framework changes.

PONDURANCE

PONDURANCE

Expected Benefits







NIST – SI, System and Information Integrity, AU – Audit and Accountability, MP – Media Protection

HIPAA – Security management process, security incident procedures, contingency plan, and audit controls

PCI - Maintain a vulnerability management program, regularly monitor, and test networks

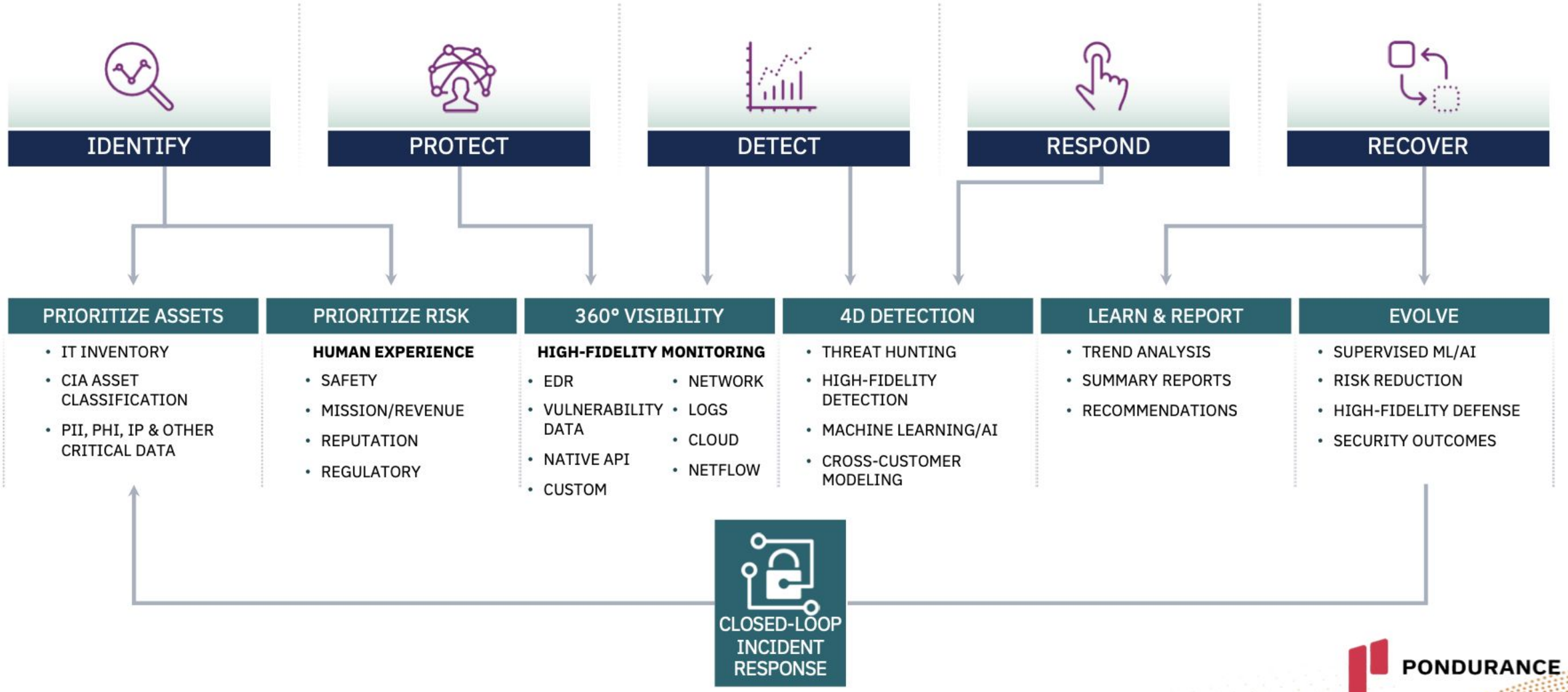
Unexpected Benefits

Positive, unexpected outcome from an action (that may require a little bit of deliberate work in this case).



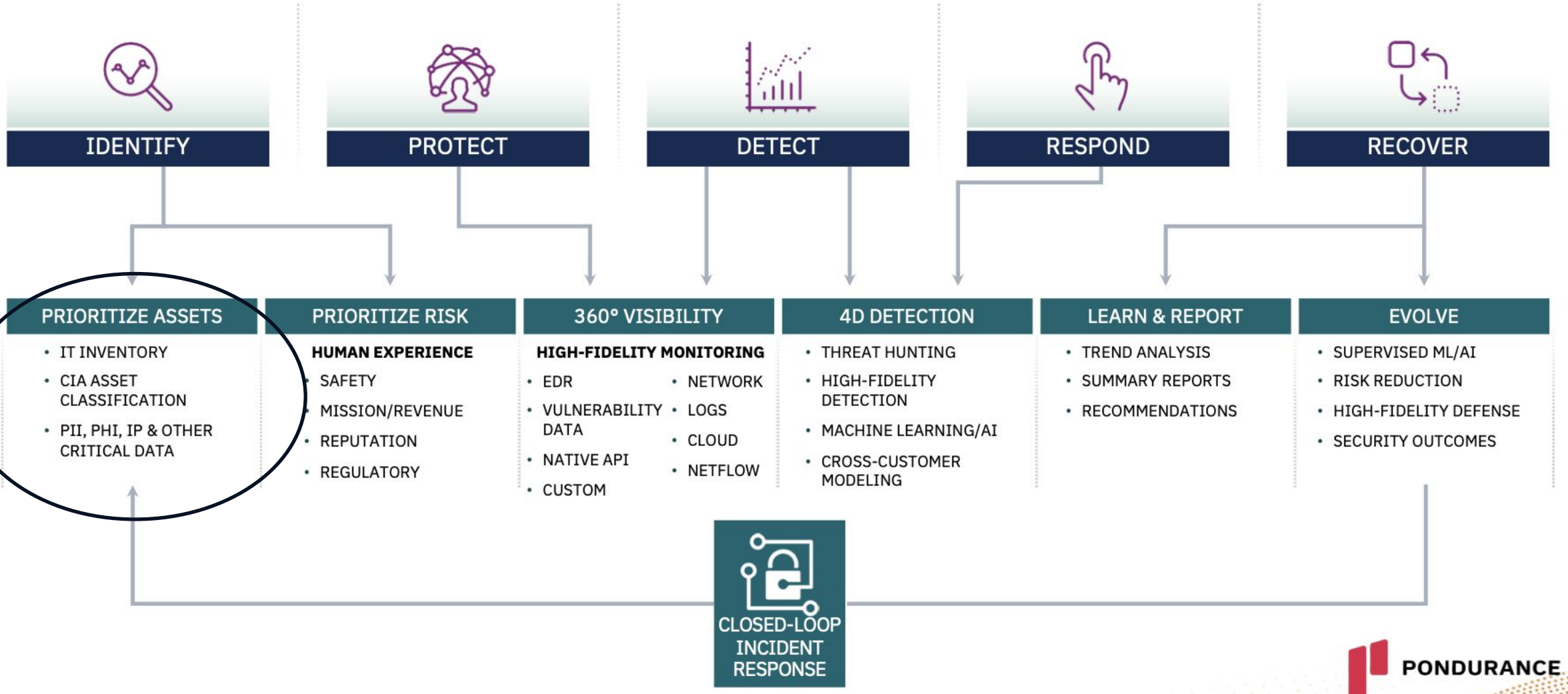
PONDURANCE

DYNAMIC DEFENSE METHODOLOGY



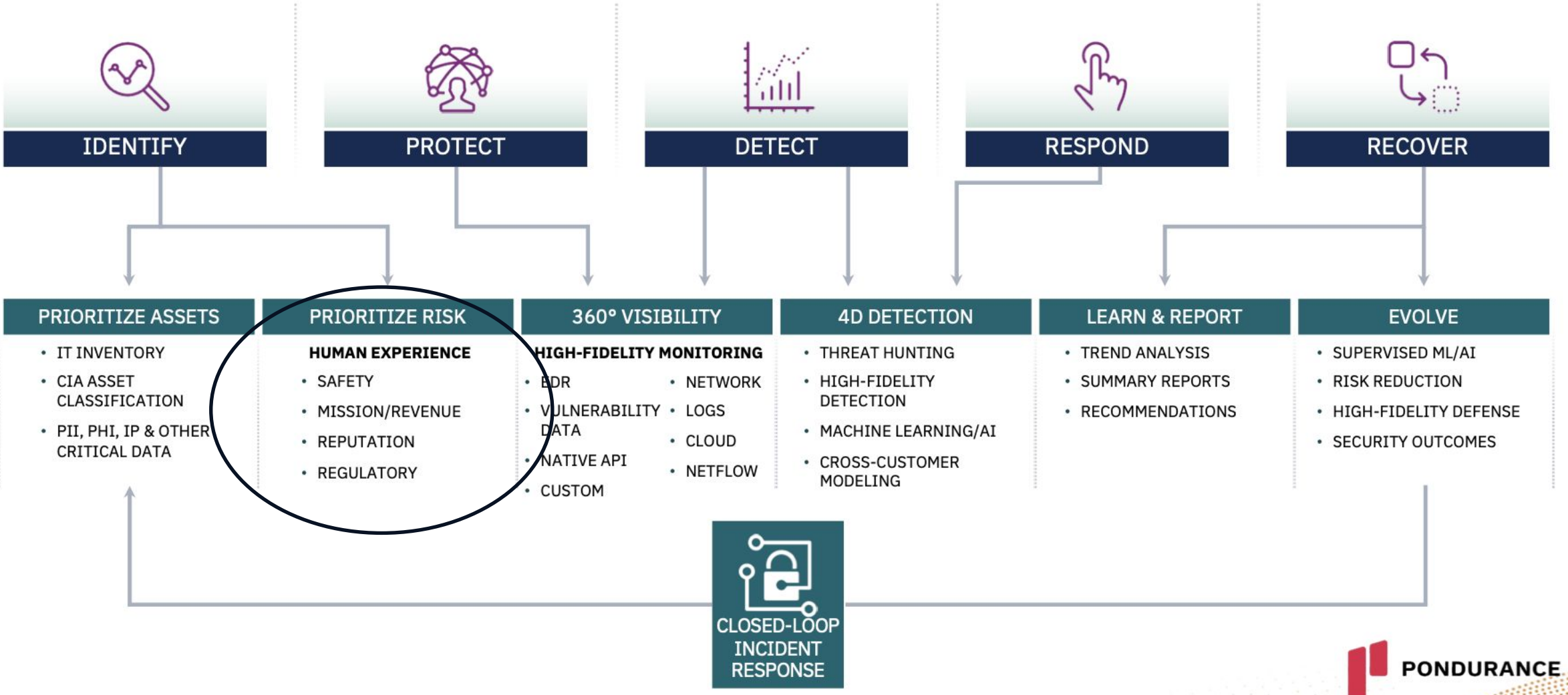
PONDURANCE

DYNAMIC DEFENSE METHODOLOGY



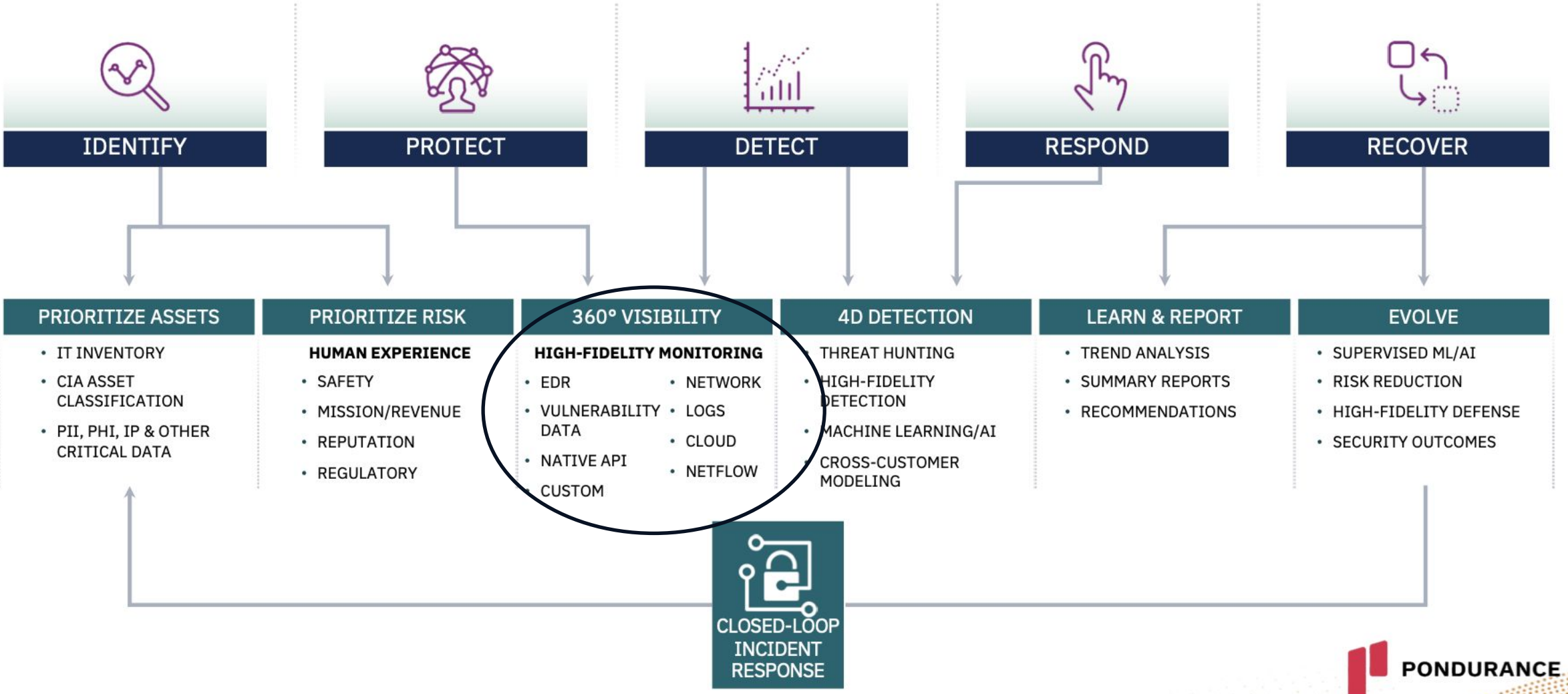
PONDURANCE

DYNAMIC DEFENSE METHODOLOGY



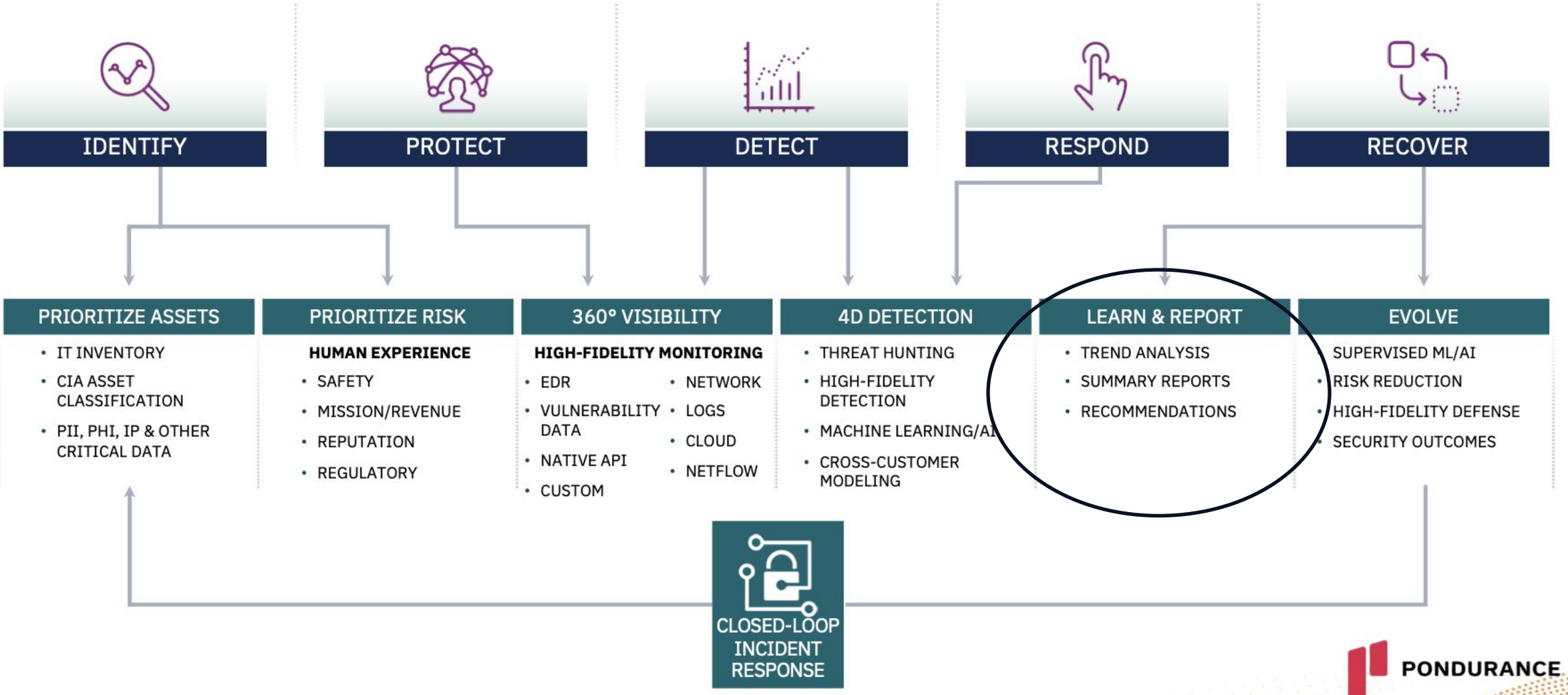
PONDURANCE

DYNAMIC DEFENSE METHODOLOGY



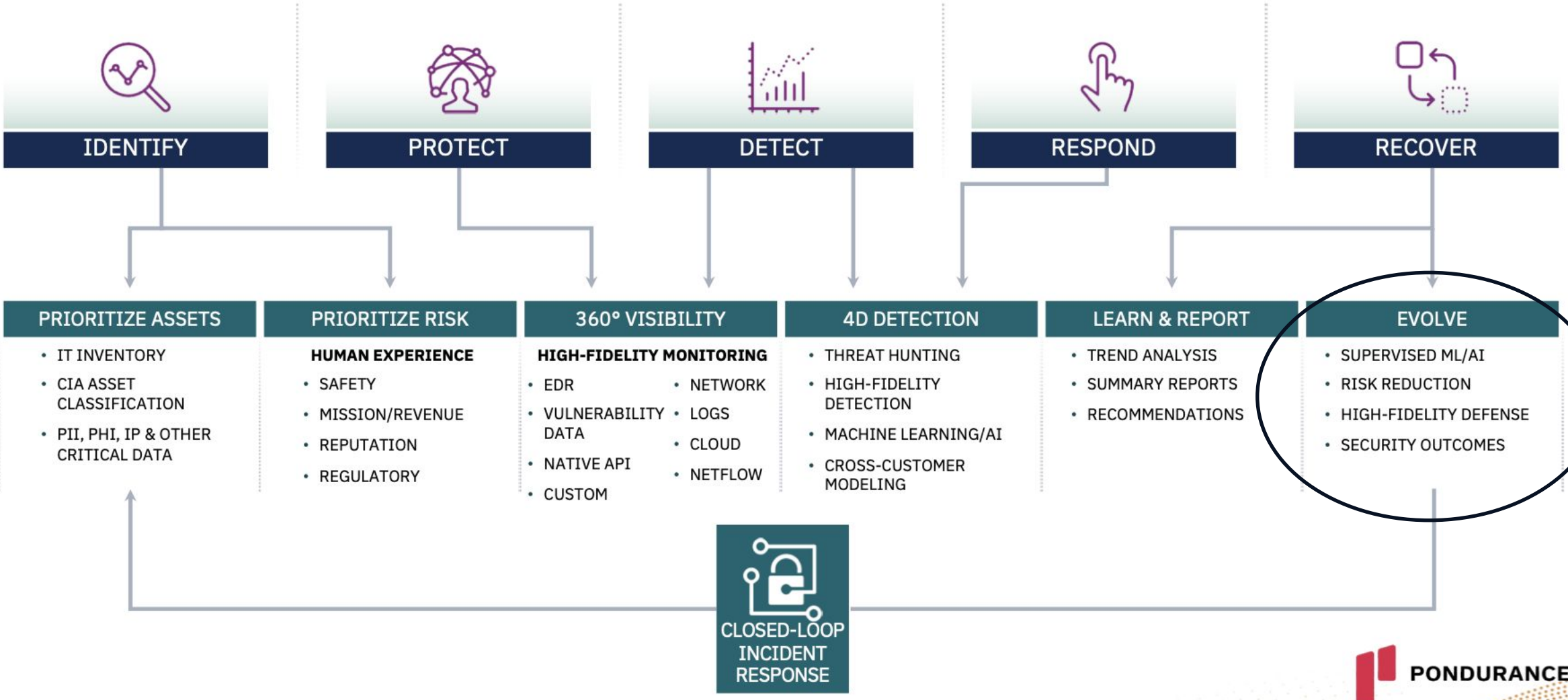
PONDURANCE

DYNAMIC DEFENSE METHODOLOGY



PONDURANCE

DYNAMIC DEFENSE METHODOLOGY



PONDURANCE

MyCyberScoreCard (MCSC) Control Mapping



		Question Count	MyCyber Score		Percent Score
MyCyberScorecard		294	864		
MDR	Managed EDR	49	168	16.7%	19.4%
	Managed Logs	6	9.5	2.0%	1.1%
	Managed Network	7	13	2.4%	1.5%
Other Services	Vulnerability Plan/Scanning	15	29.5	5.1%	3.4%
	Pen Testing	5	5	1.7%	0.6%
	DFIR	5	13	1.7%	1.5%
	Tabletop	4	17	1.4%	2.0%
	IR Plan	4	16	1.4%	1.9%
	AST	2	8	0.7%	0.9%
	Awareness Training	8	22	2.7%	2.5%
	Assessments	3	13	1.0%	1.5%
	Total	108	314	36.7%	36.3%

PONDURANCE

MDR Control Focus (ID, PR)

Category Name	SubCategory Code	SubCategory Name
Asset Management	ID.AM-2	Software platforms and applications within the organization are inventoried
Asset Management	ID.AM-2	Software platforms and applications within the organization are inventoried
Asset Management	ID.AM-3	Organizational communication and data flows are mapped
Business Environment	ID.BE-3	Priorities for organizational mission, objectives, and activities are established and communicated
Risk Assessment	ID.RA-1	Asset vulnerabilities are identified and documented
Risk Assessment	ID.RA-1	Asset vulnerabilities are identified and documented
Risk Assessment	ID.RA-2	Cyber threat intelligence, and vulnerability information is received from information sharing forums and sources
Risk Assessment	ID.RA-3	Threats, both internal and external, are identified and documented
Risk Assessment	ID.RA-3	Threats, both internal and external, are identified and documented
Risk Management Strategy	ID.RM-2	Organizational risk tolerance is determined and clearly expressed
Data Security	PR.DS-4	Adequate capacity to ensure availability is maintained
Data Security	PR.DS-5	Protections against data leaks are implemented
Data Security	PR.DS-5	Protections against data leaks are implemented
Data Security	PR.DS-5	Protections against data leaks are implemented
Data Security	PR.DS-8	Integrity checking mechanisms are used to verify hardware integrity
Data Security	PR.DS-8	Integrity checking mechanisms are used to verify hardware integrity
Information Protection Processes and Procedures	PR.IP-8	Effectiveness of protection technologies is shared with appropriate parties
Information Protection Processes and Procedures	PR.IP-8	Effectiveness of protection technologies is shared with appropriate parties
Information Protection Processes and Procedures	PR.IP-8	Effectiveness of protection technologies is shared with appropriate parties
Protective Technology	PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy
Protective Technology	PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy
Protective Technology	PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy
Protective Technology	PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy

PONDURANCE

MDR Control Focus (ID, PR)

Category Name	SubCategory Code	SubCategory Name
Asset Management	ID.AM-2	Software platforms and applications within the organization are inventoried
Asset Management	ID.AM-2	Software platforms and applications within the organization are inventoried
Asset Management	ID.AM-3	Organizational communication and data flows are mapped
Business Environment	ID.BE-3	Priorities for organizational mission, objectives, and activities are established and communicated
Risk Assessment	ID.RA-1	Asset vulnerabilities are identified and documented
Risk Assessment	ID.RA-1	Asset vulnerabilities are identified and documented
Risk Assessment	ID.RA-2	Cyber threat intelligence, and vulnerability information is received from information sharing forums and sources
Risk Assessment	ID.RA-3	Threats, both internal and external, are identified and documented
Risk Assessment	ID.RA-3	Threats, both internal and external, are identified and documented
Risk Management Strategy	ID.RM-2	Organizational risk tolerance is determined and clearly expressed
Data Security	PR.DS-4	Adequate capacity to ensure availability is maintained
Data Security	PR.DS-5	Protections against data leaks are implemented
Data Security	PR.DS-5	Protections against data leaks are implemented
Data Security	PR.DS-5	Protections against data leaks are implemented
Data Security	PR.DS-8	Integrity checking mechanisms are used to verify hardware integrity
Data Security	PR.DS-8	Integrity checking mechanisms are used to verify hardware integrity
Information Protection Processes and Procedures	PR.IP-8	Effectiveness of protection technologies is shared with appropriate parties
Information Protection Processes and Procedures	PR.IP-8	Effectiveness of protection technologies is shared with appropriate parties
Information Protection Processes and Procedures	PR.IP-8	Effectiveness of protection technologies is shared with appropriate parties
Protective Technology	PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy
Protective Technology	PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy
Protective Technology	PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy
Protective Technology	PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy

PONDURANCE

MDR Control Focus (ID, PR)

Category Name	SubCategory Code	SubCategory Name
Asset Management	ID.AM-2	Software platforms and applications within the organization are inventoried
Asset Management	ID.AM-2	Software platforms and applications within the organization are inventoried
Asset Management	ID.AM-3	Organizational communication and data flows are mapped
Business Environment	ID.BE-3	Priorities for organizational mission, objectives, and activities are established and communicated
Risk Assessment	ID.RA-1	Asset vulnerabilities are identified and documented
Risk Assessment	ID.RA-1	Asset vulnerabilities are identified and documented
Risk Assessment	ID.RA-2	Cyber threat intelligence, and vulnerability information is received from information sharing forums and sources
Risk Assessment	ID.RA-3	Threats, both internal and external, are identified and documented
Risk Assessment	ID.RA-3	Threats, both internal and external, are identified and documented
Risk Management Strategy	ID.RM-2	Organizational risk tolerance is determined and clearly expressed
Data Security	PR.DS-4	Adequate capacity to ensure availability is maintained
Data Security	PR.DS-5	Protections against data leaks are implemented
Data Security	PR.DS-5	Protections against data leaks are implemented
Data Security	PR.DS-5	Protections against data leaks are implemented
Data Security	PR.DS-8	Integrity checking mechanisms are used to verify hardware integrity
Data Security	PR.DS-8	Integrity checking mechanisms are used to verify hardware integrity
Information Protection Processes and Procedures	PR.IP-8	Effectiveness of protection technologies is shared with appropriate parties
Information Protection Processes and Procedures	PR.IP-8	Effectiveness of protection technologies is shared with appropriate parties
Information Protection Processes and Procedures	PR.IP-8	Effectiveness of protection technologies is shared with appropriate parties
Protective Technology	PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy
Protective Technology	PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy
Protective Technology	PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy
Protective Technology	PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy

PONDURANCE

MDR Control Focus (ID, PR)

Category Name	SubCategory Code	SubCategory Name
Asset Management	ID.AM-2	Software platforms and applications within the organization are inventoried
Asset Management	ID.AM-2	Software platforms and applications within the organization are inventoried
Asset Management	ID.AM-3	Organizational communication and data flows are mapped
Business Environment	ID.BE-3	Priorities for organizational mission, objectives, and activities are established and communicated
Risk Assessment	ID.RA-1	Asset vulnerabilities are identified and documented
Risk Assessment	ID.RA-1	Asset vulnerabilities are identified and documented
Risk Assessment	ID.RA-2	Cyber threat intelligence, and vulnerability information is received from information sharing forums and sources
Risk Assessment	ID.RA-3	Threats, both internal and external, are identified and documented
Risk Assessment	ID.RA-3	Threats, both internal and external, are identified and documented
Risk Management Strategy	ID.RM-2	Organizational risk tolerance is determined and clearly expressed
Data Security	PR.DS-4	Adequate capacity to ensure availability is maintained
Data Security	PR.DS-5	Protections against data leaks are implemented
Data Security	PR.DS-5	Protections against data leaks are implemented
Data Security	PR.DS-5	Protections against data leaks are implemented
Data Security	PR.DS-8	Integrity checking mechanisms are used to verify hardware integrity
Data Security	PR.DS-8	Integrity checking mechanisms are used to verify hardware integrity
Information Protection Processes and Procedures	PR.IP-8	Effectiveness of protection technologies is shared with appropriate parties
Information Protection Processes and Procedures	PR.IP-8	Effectiveness of protection technologies is shared with appropriate parties
Information Protection Processes and Procedures	PR.IP-8	Effectiveness of protection technologies is shared with appropriate parties
Protective Technology	PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy
Protective Technology	PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy
Protective Technology	PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy
Protective Technology	PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy

PONDURANCE

MDR Control Focus (ID, PR)

Category Name	SubCategory Code	SubCategory Name
Asset Management	ID.AM-2	Software platforms and applications within the organization are inventoried
Asset Management	ID.AM-2	Software platforms and applications within the organization are inventoried
Asset Management	ID.AM-3	Organizational communication and data flows are mapped
Business Environment	ID.BE-3	Priorities for organizational mission, objectives, and activities are established and communicated
Risk Assessment	ID.RA-1	Asset vulnerabilities are identified and documented
Risk Assessment	ID.RA-1	Asset vulnerabilities are identified and documented
Risk Assessment	ID.RA-2	Cyber threat intelligence, and vulnerability information is received from information sharing forums and sources
Risk Assessment	ID.RA-3	Threats, both internal and external, are identified and documented
Risk Assessment	ID.RA-3	Threats, both internal and external, are identified and documented
Risk Management Strategy	ID.RM-2	Organizational risk tolerance is determined and clearly expressed
Data Security	PR.DS-4	Adequate capacity to ensure availability is maintained
Data Security	PR.DS-5	Protections against data leaks are implemented
Data Security	PR.DS-5	Protections against data leaks are implemented
Data Security	PR.DS-5	Protections against data leaks are implemented
Data Security	PR.DS-8	Integrity checking mechanisms are used to verify hardware integrity
Data Security	PR.DS-8	Integrity checking mechanisms are used to verify hardware integrity
Information Protection Processes and Procedures	PR.IP-8	Effectiveness of protection technologies is shared with appropriate parties
Information Protection Processes and Procedures	PR.IP-8	Effectiveness of protection technologies is shared with appropriate parties
Information Protection Processes and Procedures	PR.IP-8	Effectiveness of protection technologies is shared with appropriate parties
Protective Technology	PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy
Protective Technology	PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy
Protective Technology	PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy
Protective Technology	PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy

PONDURANCE

MDR Control Focus (ID, PR)

Category Name	SubCategory Code	SubCategory Name
Asset Management	ID.AM-2	Software platforms and applications within the organization are inventoried
Asset Management	ID.AM-2	Software platforms and applications within the organization are inventoried
Asset Management	ID.AM-3	Organizational communication and data flows are mapped
Business Environment	ID.BE-3	Priorities for organizational mission, objectives, and activities are established and communicated
Risk Assessment	ID.RA-1	Asset vulnerabilities are identified and documented
Risk Assessment	ID.RA-1	Asset vulnerabilities are identified and documented
Risk Assessment	ID.RA-2	Cyber threat intelligence, and vulnerability information is received from information sharing forums and sources
Risk Assessment	ID.RA-3	Threats, both internal and external, are identified and documented
Risk Assessment	ID.RA-3	Threats, both internal and external, are identified and documented
Risk Management Strategy	ID.RM-2	Organizational risk tolerance is determined and clearly expressed
Data Security	PR.DS-4	Adequate capacity to ensure availability is maintained
Data Security	PR.DS-5	Protections against data leaks are implemented
Data Security	PR.DS-5	Protections against data leaks are implemented
Data Security	PR.DS-5	Protections against data leaks are implemented
Data Security	PR.DS-8	Integrity checking mechanisms are used to verify hardware integrity
Data Security	PR.DS-8	Integrity checking mechanisms are used to verify hardware integrity
Information Protection Processes and Procedures	PR.IP-8	Effectiveness of protection technologies is shared with appropriate parties
Information Protection Processes and Procedures	PR.IP-8	Effectiveness of protection technologies is shared with appropriate parties
Information Protection Processes and Procedures	PR.IP-8	Effectiveness of protection technologies is shared with appropriate parties
Protective Technology	PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy
Protective Technology	PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy
Protective Technology	PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy
Protective Technology	PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy

PONDURANCE

MDR Control Focus (DE)

Category Name	SubCategory Code	SubCategory Name
Anomalies and Events	DE.AE-1	A baseline of network operations and expected data flows for users and systems is established and managed.
Anomalies and Events	DE.AE-2	Detected events are analyzed to understand attack targets and methods
Anomalies and Events	DE.AE-2	Detected events are analyzed to understand attack targets and methods
Anomalies and Events	DE.AE-2	Detected events are analyzed to understand attack targets and methods
Anomalies and Events	DE.AE-2	Detected events are analyzed to understand attack targets and methods
Anomalies and Events	DE.AE-3	Event data are aggregated and correlated from multiple sources and sensors
Anomalies and Events	DE.AE-5	Incident alert thresholds are established
Security Continuous Monitoring	DE.CM-1	The network is monitored to detect potential cybersecurity events
Security Continuous Monitoring	DE.CM-1	The network is monitored to detect potential cybersecurity events
Security Continuous Monitoring	DE.CM-1	The network is monitored to detect potential cybersecurity events
Security Continuous Monitoring	DE.CM-4	Malicious code is detected
Security Continuous Monitoring	DE.CM-4	Malicious code is detected
Security Continuous Monitoring	DE.CM-5	Unauthorized mobile code is detected
Security Continuous Monitoring	DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed
Detection Processes	DE.DP-1	Roles and responsibilities for detection are well defined to ensure accountability
Detection Processes	DE.DP-1	Roles and responsibilities for detection are well defined to ensure accountability
Detection Processes	DE.DP-2	Detection activities comply with all applicable requirements
Detection Processes	DE.DP-3	Detection processes are tested
Detection Processes	DE.DP-3	Detection processes are tested
Detection Processes	DE.DP-4	Event detection information is communicated to appropriate parties
Detection Processes	DE.DP-4	Event detection information is communicated to appropriate parties
Detection Processes	DE.DP-4	Event detection information is communicated to appropriate parties
Detection Processes	DE.DP-5	Detection processes are continuously improved
Detection Processes	DE.DP-5	Detection processes are continuously improved

PONDURANCE

MDR Control Focus (DE)

Category Name	SubCategory Code	SubCategory Name
Anomalies and Events	DE.AE-1	A baseline of network operations and expected data flows for users and systems is established and managed.
Anomalies and Events	DE.AE-2	Detected events are analyzed to understand attack targets and methods
Anomalies and Events	DE.AE-2	Detected events are analyzed to understand attack targets and methods
Anomalies and Events	DE.AE-2	Detected events are analyzed to understand attack targets and methods
Anomalies and Events	DE.AE-2	Detected events are analyzed to understand attack targets and methods
Anomalies and Events	DE.AE-3	Event data are aggregated and correlated from multiple sources and sensors
Anomalies and Events	DE.AE-5	Incident alert thresholds are established
Security Continuous Monitoring	DE.CM-1	The network is monitored to detect potential cybersecurity events
Security Continuous Monitoring	DE.CM-1	The network is monitored to detect potential cybersecurity events
Security Continuous Monitoring	DE.CM-1	The network is monitored to detect potential cybersecurity events
Security Continuous Monitoring	DE.CM-4	Malicious code is detected
Security Continuous Monitoring	DE.CM-4	Malicious code is detected
Security Continuous Monitoring	DE.CM-5	Unauthorized mobile code is detected
Security Continuous Monitoring	DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed
Detection Processes	DE.DP-1	Roles and responsibilities for detection are well defined to ensure accountability
Detection Processes	DE.DP-1	Roles and responsibilities for detection are well defined to ensure accountability
Detection Processes	DE.DP-2	Detection activities comply with all applicable requirements
Detection Processes	DE.DP-3	Detection processes are tested
Detection Processes	DE.DP-3	Detection processes are tested
Detection Processes	DE.DP-4	Event detection information is communicated to appropriate parties
Detection Processes	DE.DP-4	Event detection information is communicated to appropriate parties
Detection Processes	DE.DP-4	Event detection information is communicated to appropriate parties
Detection Processes	DE.DP-5	Detection processes are continuously improved
Detection Processes	DE.DP-5	Detection processes are continuously improved

PONDURANCE

MDR Control Focus (DE)

Category Name	SubCategory Code	SubCategory Name
Anomalies and Events	DE.AE-1	A baseline of network operations and expected data flows for users and systems is established and managed
Anomalies and Events	DE.AE-2	Detected events are analyzed to understand attack targets and methods
Anomalies and Events	DE.AE-2	Detected events are analyzed to understand attack targets and methods
Anomalies and Events	DE.AE-2	Detected events are analyzed to understand attack targets and methods
Anomalies and Events	DE.AE-2	Detected events are analyzed to understand attack targets and methods
Anomalies and Events	DE.AE-3	Event data are aggregated and correlated from multiple sources and sensors
Anomalies and Events	DE.AE-5	Incident alert thresholds are established
Security Continuous Monitoring	DE.CM-1	The network is monitored to detect potential cybersecurity events
Security Continuous Monitoring	DE.CM-1	The network is monitored to detect potential cybersecurity events
Security Continuous Monitoring	DE.CM-1	The network is monitored to detect potential cybersecurity events
Security Continuous Monitoring	DE.CM-4	Malicious code is detected
Security Continuous Monitoring	DE.CM-4	Malicious code is detected
Security Continuous Monitoring	DE.CM-5	Unauthorized mobile code is detected
Security Continuous Monitoring	DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed
Detection Processes	DE.DP-1	Roles and responsibilities for detection are well defined to ensure accountability
Detection Processes	DE.DP-1	Roles and responsibilities for detection are well defined to ensure accountability
Detection Processes	DE.DP-2	Detection activities comply with all applicable requirements
Detection Processes	DE.DP-3	Detection processes are tested
Detection Processes	DE.DP-3	Detection processes are tested
Detection Processes	DE.DP-4	Event detection information is communicated to appropriate parties
Detection Processes	DE.DP-4	Event detection information is communicated to appropriate parties
Detection Processes	DE.DP-4	Event detection information is communicated to appropriate parties
Detection Processes	DE.DP-5	Detection processes are continuously improved
Detection Processes	DE.DP-5	Detection processes are continuously improved

PONDURANCE

MDR Control Focus (DE)

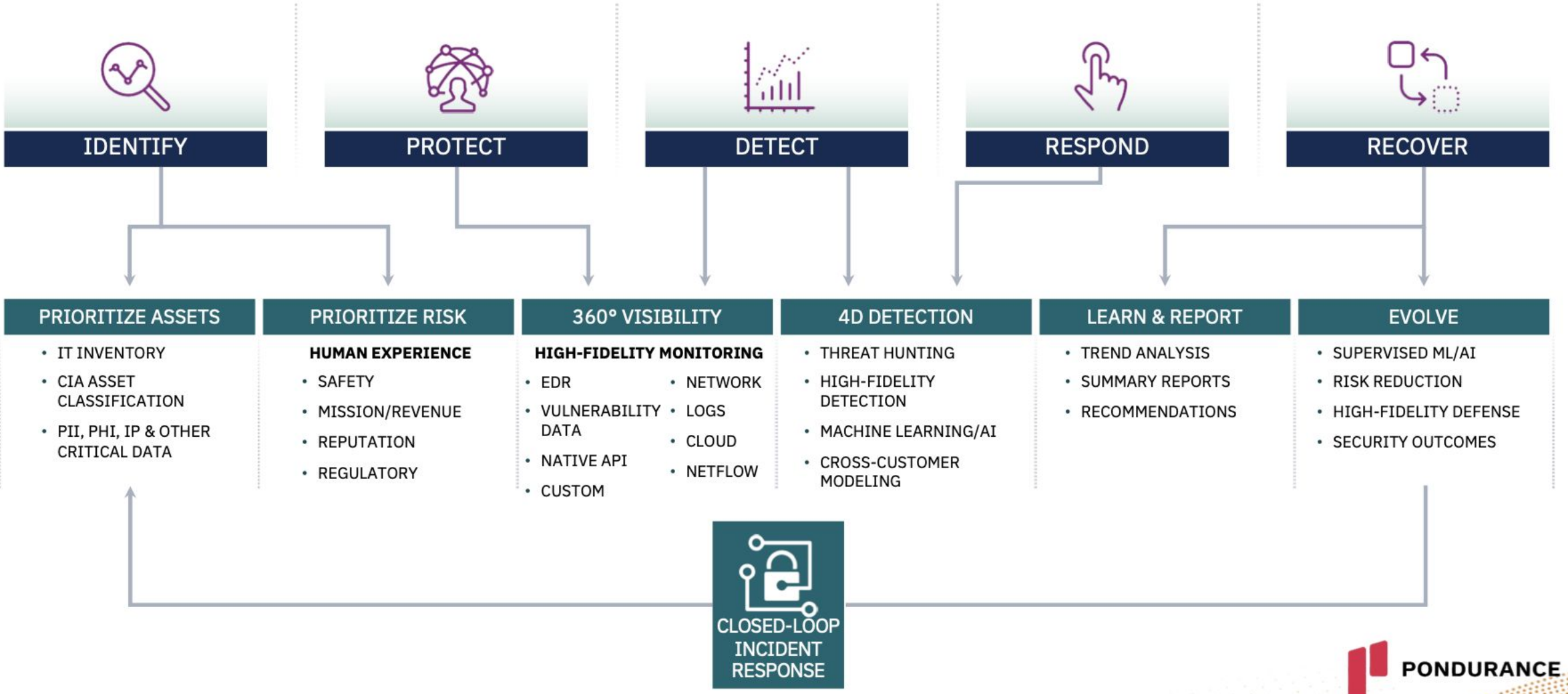
Category Name	SubCategory Code	SubCategory Name
Anomalies and Events	DE.AE-1	A baseline of network operations and expected data flows for users and systems is established and managed.
Anomalies and Events	DE.AE-2	Detected events are analyzed to understand attack targets and methods
Anomalies and Events	DE.AE-2	Detected events are analyzed to understand attack targets and methods
Anomalies and Events	DE.AE-2	Detected events are analyzed to understand attack targets and methods
Anomalies and Events	DE.AE-2	Detected events are analyzed to understand attack targets and methods
Anomalies and Events	DE.AE-3	Event data are aggregated and correlated from multiple sources and sensors
Anomalies and Events	DE.AE-5	Incident alert thresholds are established
Security Continuous Monitoring	DE.CM-1	The network is monitored to detect potential cybersecurity events
Security Continuous Monitoring	DE.CM-1	The network is monitored to detect potential cybersecurity events
Security Continuous Monitoring	DE.CM-1	The network is monitored to detect potential cybersecurity events
Security Continuous Monitoring	DE.CM-4	Malicious code is detected
Security Continuous Monitoring	DE.CM-4	Malicious code is detected
Security Continuous Monitoring	DE.CM-5	Unauthorized mobile code is detected
Security Continuous Monitoring	DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed
Detection Processes	DE.DP-1	Roles and responsibilities for detection are well defined to ensure accountability
Detection Processes	DE.DP-1	Roles and responsibilities for detection are well defined to ensure accountability
Detection Processes	DE.DP-2	Detection activities comply with all applicable requirements
Detection Processes	DE.DP-3	Detection processes are tested
Detection Processes	DE.DP-3	Detection processes are tested
Detection Processes	DE.DP-4	Event detection information is communicated to appropriate parties
Detection Processes	DE.DP-4	Event detection information is communicated to appropriate parties
Detection Processes	DE.DP-4	Event detection information is communicated to appropriate parties
Detection Processes	DE.DP-5	Detection processes are continuously improved
Detection Processes	DE.DP-5	Detection processes are continuously improved

PONDURANCE

MDR Control Focus (RS)

Category Name	SubCategory Code	SubCategory Name
Analysis	RS.AN-1	Notifications from detection systems are investigated
Analysis	RS.AN-1	Notifications from detection systems are investigated
Analysis	RS.AN-1	Notifications from detection systems are investigated
Analysis	RS.AN-3	Forensics are performed
Analysis	RS.AN-5	Vulnerability processes and procedures are established
Communications	RS.CO-2	Events are reported consistent with established criteria
Communications	RS.CO-2	Events are reported consistent with established criteria
Communications	RS.CO-3	Information is shared consistent with response plans
Communications	RS.CO-3	Information is shared consistent with response plans
Communications	RS.CO-3	Information is shared consistent with response plans
Communications	RS.CO-3	Information is shared consistent with response plans
Communications	RS.CO-4	Coordination with stakeholders occurs consistent with response plans
Communications	RS.CO-5	Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness
Mitigation	RS.MI-1	Incidents are contained
Mitigation	RS.MI-2	Incidents are mitigated

DYNAMIC DEFENSE METHODOLOGY



PONDURANCE

PONDURANCE

Questions?

Reach out to info@pondurance.com



PONDURANCE

Thank You

pondurance.com

