The Unexpected Compliance Benefits of MDR

PONDURANCE

MORE AND MORE, ORGANIZATIONS ARE USING MANAGED DETECTION AND RESPONSE (MDR) SERVICES TO ASSIST THE TALENTED HUMANS AND TECHNOLOGY SOLUTIONS NEEDED TO COMBAT THREATS IN THE CYBER LANDSCAPE.

MDR activities can be classified by the NIST Cybersecurity Framework — organized using five key functions including identify, protect, detect, respond, and recover — as a foundation to manage cybersecurity risk. Additionally, Pondurance MDR services take it further with the dynamicdefense methodology (see page 2).

Protect, detect, and respond are the three benefits that organizations expect from MDR services. But many organizations may not realize the full potential of MDR. By partnering with an MDR provider like Pondurance, your organization also receives the unexpected benefits of identify and recover and the enhanced benefits of protect, detect, and respond. Leveraging the full benefits of all five functions can help your organization better protect your cyber environment and stay in regulatory compliance.

UNEXPECTED BENEFITS

IDENTIFY. Your organization must be able to identify and understand what your infrastructure looks like to adequately protect it. You need to know what your IT inventory includes, what your asset classifications are, what type of data live on those systems, and where your cyber risks lie. As an unexpected benefit, MDR services can help your organization prioritize your assets, such as IT inventory; confidentiality, integrity, and availability (CIA) asset classification; personally identifiable information (PII); protected health information (PHI); IP; and other critical data. Also, using MDR services can help prioritize your risks including risk to safety, mission, revenue, reputation, and regulatory compliance.

RECOVER. Following a cyber threat, your organization needs to understand how to stop the same actions from happening again. Are your vulnerabilities properly patched? Do you need to reduce the number of alerts? As an unexpected benefit, MDR services provide assistance and additional visibility to document lessons learned and reporting, including trend analysis, summary reports, and recommendations. Also, MDR services allow your organization to evolve and improve its overall security maturity with supervised machine learning/artificial intelligence (ML/AI), risk reduction, high-fidelity defense, and security outcomes.

In addition, the unexpected benefits of identify and recover provide data needed for internal audits and gap assessments across your organization and offer the capability to handle a variety of regulatory compliance requirements, such as NIST, HIPAA, and the Payment Card Industry Data Security Standard. With these benefits, your organization can also eliminate silos of compliance by assessing once to address multiple regulations or security controls.

Enhanced Expected Benefits

PONDURANCE

PROTECT. Having extended, enhanced visibility throughout your infrastructure is important. MDR services provide 360-degree visibility for high-fidelity monitoring across endpoints, networks, logs, the cloud, and more.

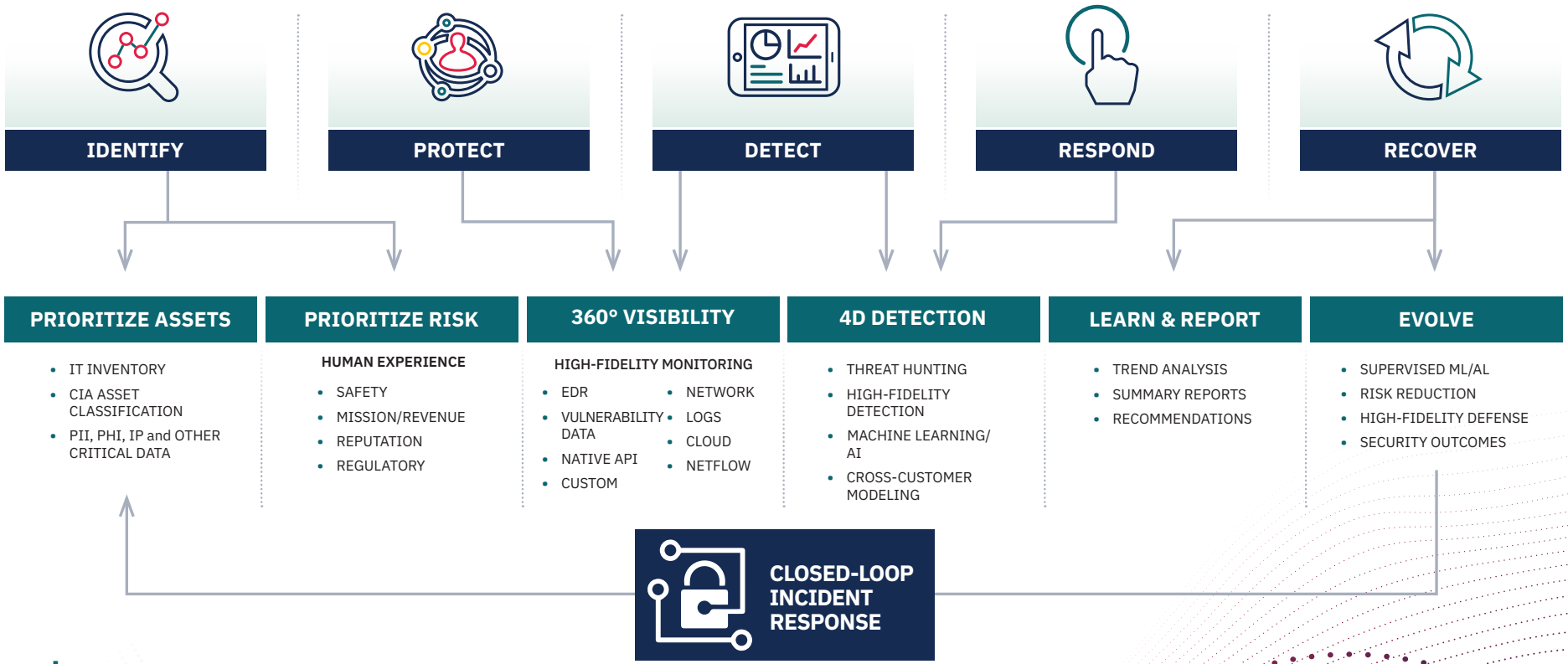
DETECT. MDR services provide enhanced, deeper visibility for a better look at the actual data flow and ingest amounts. This high-fidelity detection — a step beyond standard detection — allows for improved threat hunting, ML/AI, and cross-customer modeling.

RESPOND. The response to a cyber threat must be more than just conveying that something happened. A client wants to know what to do about it and which next steps to take. Respond is enhanced by having an internal digital forensics and incident response team ready to assist in your recovery efforts.

CLOSED-LOOP INCIDENT RESPONSE

Together, Pondurance MDR focusing on the expanded NIST categories, creates a comprehensive solution known as closed-loop incident response — and it should be the cybersecurity goal for every organization. Closed-loop incident response allows your organization to identify your infrastructure and protect it. Then, if a cyber threat occurs, your organization can detect it, appropriately respond, and quickly and fully recover. Let Pondurance implement this comprehensive MDR solution for your organization.

DYNAMIC DEFENSE METHODOLOGY



pondurance.com