Extended Detection and Response (XDR)

24/7/365 network monitoring by cybersecurity experts.

Who's Watching Your Network?

A good cybersecurity defense includes implementing tools like SIEM, UTM firewalls, and advanced endpoint security technology. However, without the human component—someone to actively utilize the data coming from these tools—you are essentially still at square one. That's because it's not only how good your tools are, but who's leveraging those tools to keep watch over your environment.

The PDI XDR Team Stands Guard

We perform Extended Detection and Response (XDR) specifically for organizations that don't have the internal expertise and/or bandwidth to keep a vigilant watch over the security of their IT environment. We employ the right people and the right processes to efficiently supplement your organization's security threat management efforts.

Our experts take care of it all—threat monitoring, detection, and targeted response activities to prevent and deflect any inconsistencies.

Our team identifies intrusions as they are happening, before any damage is done:

- Defining, implementing, and updating security rules
- Running targeted threat hunting sequences to trace anomalies
- Examining alerts to separate true concerns from false positives
- Addressing and appropriately escalating threats in real time
- Applying patches to fix operating system security vulnerabilities
- Employing advanced content filtering to better meet compliance and security needs

Removing the Burden of Log Management

A single network device can generate thousands of logs each day, and an organization may have hundreds of network devices and servers. The overwhelming amount of log messages can obscure network visibility, overtax internal resources, and increase operational costs.

As part of the PDI XDR service, we collect, aggregate, and normalize your organization's log data from servers, endpoints, applications, and security devices for compliance and infrastructure management. Our expert security analysts monitor and analyze your log events, freeing up your IT resources to focus on growing your business:

- More than one trillion events ingested each day
- Myriad log types ingested, including Microsoft, Cisco, Meraki, Palo Alto, Checkpoint, Solaris, Linux, Cylance, Crowdstrike, Carbon Black, Fidelis, Dark Trace, and more

Security Operations Center (SOC)

PDI's SOC captures and compiles data from both physical and digital sources to develop a level of decision support not possible in a standard monitoring environment. This process combines our people, processes, and technology to analyze and act on robust data sets, allowing us to see the whole picture of an enterprise. We keep your business optimized and running no matter what challenges arise.

PDI utilizes two SOC locations that operate 24/7/365 and are staffed by highly trained SecOps personnel. Located in Hunt Valley, MD, and Lexington, KY, these secure facilities feature video surveillance, redundant fiber-optic Internet connectivity, and battery and diesel redundant power.

To learn how PDI can protect your organization from cyberthreats, contact us today.

Contact Us Today

PDI

www.pdisoftware.com