



MANAGED XDR

Extended Detection and Response

hbs.net



World-Class Tools Tuned and Managed by Our Experienced SOC Team

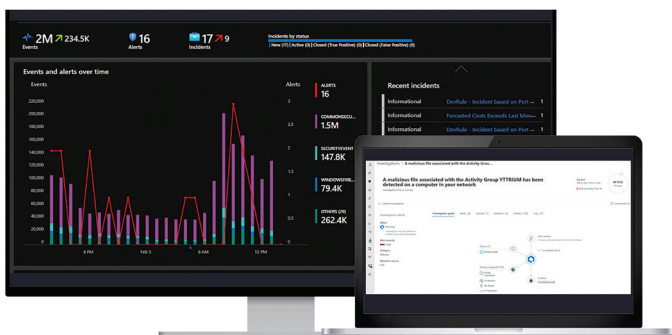
HBS Managed XDR service combines the security expertise of our U.S.-based SOC team with the leading technology of Microsoft Sentinel (SIEM) and Microsoft Defender for Endpoint (EDR). The result is an integrated system that intercepts threats at the earliest stages and constantly adapts to an ever-changing threat landscape.

Customized Experience

Our U.S.-based SOC team onboards each client with a collection of custom workbooks, then continues to tune the system for your unique environment. These proprietary rulesets let our team strengthen your security posture and meet compliance and organizational requirements.

Threat Hunting

Advanced threat hunting analytic rules and built-in algorithms make it possible to automate threat response through security orchestration, automation, and response (SOAR). Additionally, our analysts and forensic investigators can leverage sophisticated run books and machine learning notebooks to perform advanced threat hunting in seconds.



24 x 7 Confidence

Around-the-clock service means that whenever a critical incident occurs, HBS analysts review the situation and notify clients only if they need to respond. You won't have to deal with non-critical alerts during your time off.

Our service protects your extended technology ecosystem, including endpoints; cloud environments; firewalls and network devices; servers; IoT; and email. With machine learning, artificial intelligence and human fine-tuning, HBS Managed XDR constantly adjusts to new threats and limits false positives.

HBS Managed XDR delivers:

The Right TECHNOLOGY

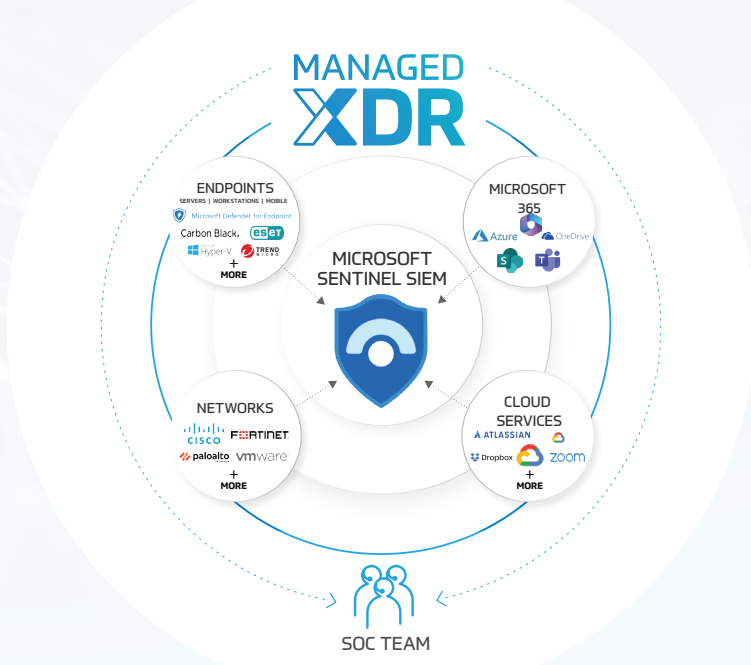
A cloud-native SIEM and enterprise endpoint platform backed by decades of security experience.

The Right SECURITY TEAM


Our SOC analysts work with you to understand your environment and tune the XDR service to fit your needs.

The Right RETURN

We eliminate alert fatigue by reducing millions of monthly events to a handful of alerts that require your attention.



The HBS Difference

FEATURES	EDR	XDR	
Endpoint detection and response	✓	✓	✓
Machine learning	✓	✓	✓
Artificial intelligence	✓	✓	✓
Defense against zero-day threats and fileless malware	✓	✓	✓
Monitoring of cloud workflows, email servers, IoT devices, firewalls, etc.	-	✓	✓
Correlation of events throughout your environment	-	✓	✓
Security Orchestration, Automation and Response (SOAR)	-	✓	✓
Advanced digital forensics	-	✓	✓
Support for proper provisioning and deployment	-	-	✓
SOC team tuning rules to react to emerging threats	-	-	✓
SOC team tuning rules to reduce false positives	-	-	✓
SOC handling alerts on your behalf	-	-	✓
Insights gained from a multitenant environment	-	-	✓
Insights to improve effectiveness of other security tools	-	-	✓

Managed By HBS U.S.-Based SOC

- Onboarding support
- Custom workbook creation
- 24/7/365 incident review/response
- Elimination of false positives
- Recommended actions for alerts forwarded to you

Create a Business Advantage with Managed XDR

Native Integration Mitigates Security Gaps

HBS Managed XDR offers one SOC managing one platform from one vendor. You get native integration of SIEM, endpoint protection, vulnerability scanning, antivirus and more. That means hackers can't find the cracks that weaken most multivendor systems.

Reduced IT Workload

By managing your XDR system, HBS SOC frees up your IT team to complete other business-critical projects. By minimizing false positives, we limit alerts to the critical events you specifically want to monitor.

Dramatically Lower Downtime

Reduce forensics analysis of attacks from days to minutes with 24/7 monitoring of your entire system and advanced threat hunting. We catch and eradicate intruders faster, dropping business interruptions to near zero.

Strategic Guidance

SOC analysts lead provisioning, rule creation and more. We work every day with multiple industries and dozens of clients—and apply the lessons to your XDR setup. Every lesson learned by Microsoft and HBS improves your system.

Better Results From Your Other Tools

Managed XDR monitors the effectiveness of security layers throughout your system. For example, if you have an email filtering solution that isn't stopping spam sufficiently, XDR can let you know. Sometimes, we'll determine that XDR can replace tools altogether, reducing your IT expense.

Actionable Alerts

Our incident alerts provide critical detail and context that let you drill down on specific improvements for your security program.



hbs.net

800.236.7914

inquiry@hbs.net