



Managed Threat Detection and Response

What you don't know can hurt you

Visibility provides knowledge—the vital context concerning risk of exposure and exploitation of your data and assets.

Security is challenging and complex, and few organizations have the experts or infrastructure needed to properly protect their data. Hiring experienced security practitioners is an expensive endeavor and maintaining a modern security stack can be complicated and expensive. So, what do you need to know?

- Not all data is created equally. A clear understanding of the types of data and the acceptable level of risk involved with each type of data is necessary.
- When moving to a cloud model, the dynamics of security change significantly. By combining visibility, identification of sensitive data, and automation to enforce policies, your defensive posture improves.
- A strong combination of security tools and security experts are required 24x7x365 to monitor, analyze, and report on the ever-changing threat environment.

The CBTS Managed Threat Detection and Response Service actively monitors your network to identify threats across an organization. When suspicious activity occurs, we immediately notify you and work with you to contain and investigate the malicious behavior.

Managed Threat Detection and Response

Early detection and faster response

The constant changes in IT practices and the threat landscape place an exorbitant amount of pressure on IT staff. Partnering with CBTS will help your organization with:

- Underlying technologies.
- Alert fatigue.
- Network monitoring.
- Investigation and verification.
- Threat awareness.
- Incident response.
- Compliance reporting.
- Access to security specialists.

Given the modern threat landscape, every organization must be prepared to detect and respond to a security breach. Whether developing your incident response plan, improving your visibility through security monitoring, adopting stronger security controls, or formalizing a security and risk program, businesses should turn to the experts where gaps exist.

Managed Threat Detection and Response options

	MDR Professional	MDR Enterprise
	Essentials + Threat Detection and Incident Management. Get all the capabilities of our Essentials option plus these additional capabilities.	Professional + Managed WAF and assigned SOC analyst options. Step up to our enterprise level to provide your customers with our premium WAF capabilities and proactive security service partnership.
Security Platform	<ul style="list-style-type: none"> • Threat monitoring and visibility. • Intrusion detection. • Security analytics. • Log collection and monitoring. • Extensive log search capabilities. • AV & Cloud security integrations. 	<ul style="list-style-type: none"> • Always-on WAF defense against web attacks (for example, OWASP Top 10, emerging threats, zero-day vulnerabilities). • Protection from SQL injection, DOS attacks, URL tampering, cross-site scripting attacks, and more.
Threat Intelligence	<ul style="list-style-type: none"> • Event insights and analysis. • Threat frequency, severity, and status intelligence. • Attack prevention capabilities. 	<ul style="list-style-type: none"> • Verified testing against more than 2.1 million web application attacks. • Advanced detection capabilities to spot and block malicious activity. • Dark Web scanning.
Expert Defenders	ActiveWatch Professional 24/7 SOC with incident management, escalation, and response support.	ActiveWatch Enterprise <ul style="list-style-type: none"> • Security posture review. • Incident response assistance. • Threat hunting. • Help with tuning strategies, customized policies, and best practices.



Speak to a security expert today at cbts.com