cbts | Microsoft Solutions Partner

Managed Microsoft Sentinel XDR

Managed cloud-based security

As IT becomes more strategic, the importance of security grows daily. Security information and event management (SIEM) solutions built for yesterday's environments struggle to keep pace with today's challenges—let alone tomorrow's unimagined risks. Information security leaders are faced with a challenging task: Provide consistent and reliable security in the face of growing complexity, increasingly diverse attack surfaces, growing alert volumes, and increasingly sophisticated and difficult-to-detect cyber-attacks.

That's why CBTS has developed Managed Microsoft Sentinel, a fully cloud-native XDR solution.

Automated threat hunting

Managed Microsoft Sentinel from CBTS delivers intelligent security analytics and threat intelligence across the enterprise, providing a single solution for alert detection, threat visibility, proactive hunting, and threat response. This service is flexible and can be utilized just as a monitoring and alerting service or a full service SOC with automated and orchestrated responses to quickly contain and eliminate threats.

- Gain visibility into threats across e-mail, identity, and data
- Better understand, prioritize, and mitigate potential threat vectors
- Develop joint plans and next steps

Why Managed Microsoft Sentinel

- Identify leaks, threats, and gaps in security by leveraging industry-leading experts
- Reduce alert fatigue and employee time spent researching false positives
- Reduce overhead by outsourcing Security Operations
- Improve your security posture
- Simple per data charges for data monitored
- Get insights to your SOC team, and allow your team to focus on what's important
- Integrated third-party intelligence provides additional context
- Automate responses to mundane or routine incidents or events
- Have a partner who is prepared for remediation if necessary

Remote monitoring

If your organization doesn't have its own security operations center (SOC) or if you want to offload some monitoring tasks, we will demonstrate how CBTS can perform remote monitoring and threat hunting for you.

Joint threat exploration

If your organization is interested in learning how to integrate Microsoft Sentinel in your existing SOC by replacing or augmenting an existing SIEM, we will work with your SecOps team and provide additional readiness to bring them up to speed.

CBTS Security Approach

Analyze your requirements and priorities for a SIEM deployment

Define scope and design automated playbooks and threat hunting criteria

Remote monitoring* and proactive threat hunting to discover attack indicators

*optional component

Discover threats and demonstrate how to automate responses

Recovery processes and procedures are executed to ensure timely restoration of affected systems and assets

Alerting and Monitoring

- Generate analytics for monthly or weekly reports
- Monitoring 24x7x365
- Active threat hunting
- Alert your IT team based on specific criteria or thresholds
- Determine level of response based on SLA
- Run weekly or month vulnerability scans
- Manage connections to customer ITSM system for incident tracking
- Managed playbook and automation to eliminate false positives

Automation and Orchestration

- Automation development, testing, and integrations into other systems
- Develop and orchestrate simple remediation scripts based on customer requirements
- Ongoing script management, patches, and upgrades
- Professional consulting every month

CBTS Security Operations Center

- **Support:** 24x7x365 by SOC analysts
- **Monitoring your environment,** including Network, Cloud, Compute, IAM, and other items that can monitored by Sentinel
- **New rule sets, managed playbooks, and automation** to research, eliminate false positives, and deal with emerging threats
- **Monthly threat hunting:** search Sentinel logs for evidence of compromise
- **Quarterly/monthly** reporting of alarms, incidents, and threats
- **Experience the benefits of a Managed Sentinel** with a true cloud native XDR, managed and monitored by our cybersecurity experts.

Why CBTS?

When it comes to security, you need an experienced partner.

CBTS is a Microsoft Security Solutions Partner with over 20 years experience with managed security solutions. Our experienced team of security professionals has deep knowledge of Microsoft and their security suite of products.

From developing and deploying modern apps and the secure, scalable platforms on which they run, to managing, monitoring, and optimizing their operations, CBTS is the trusted partner businesses need to thrive in the application era.

Contact us today.