Microsoft Sentinel Services

SecureSky

Who We Are

SecureSky delivers a complete portfolio of cloud security solutions to help organizations protect their cloud applications, services and infrastructure.

SecureSky Microsoft Sentinel solutions includes Sentinel deployment and enablement and managed eXtended Detection and Response services, which provides Sentinel threat escalation and investigation, tuning and optimization, ongoing development threat hunting, and continuous enhancements to protective controls.

SecureSky Managed eXtended Detection and Response Team

Microsoft Sentinel Overview

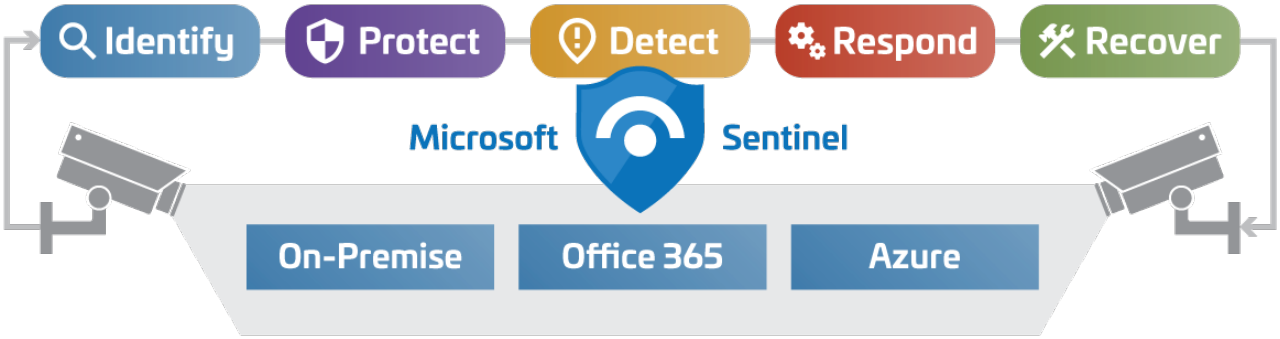
Microsoft Sentinel is a cloud-native, Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) platform that aggregates data from multiple sources, including users, applications, servers and devices running on-premises or in any cloud, letting you analyze millions of records in a few seconds.

Microsoft Sentinel includes built-in connectors for easy onboarding of popular security solutions and can collect data from any source using open standards like CEF and Syslog.

Microsoft Sentinel is your view across the enterprise and SecureSky's team of cloud security experts will be there each step of the way to design, configure and optimize Sentinel for your environment. Sentinel has no upfront cost, with pricing based on usage.

Sentinel Security Features and Interface with Other Azure Modules

The Microsoft Sentinel application is built on Azure infrastructure, allowing high-scale, flexible security while reducing security infrastructure setup and maintenance. Together with the functionality of Azure Log Analytics, this enables rapid connection to data sources, pre-built functionality, visibility to multi-cloud and hybrid environments, and powerful analytics.



Microsoft Sentinel Services

SecureSky

Continuous Optimization of Protection and Detection

Organizations today constantly find themselves reacting to threats and, with a growing cybersecurity skills shortage, are challenged to find resources capable of advanced detection, investigation and response.

SecureSky's managed detection and response focus is to evaluate lessons learned from detection and response activities, and deploy protective measures to stop that threat from recurring.

Over time, as protective controls and detection policies are strengthened and unneeded "noise" is tuned out, threat volumes will decrease, allowing detection and response resources to focus on true threats to the environment.

Microsoft Sentinel Deployment and Enablement Overview

- SIEM use case assessment and identification of key technologies for effective detection
- Build and configuration of Sentinel cloud instance
- Sentinel agent deployment (if required)
- Onboarding of log data, using SecureSky proprietary and native Sentinel connectors
- Creation of client dashboards
- Development of threat hunting templates
- Building and tuning of alerting scenarios for investigative case generation
- Setup of playbooks to execute automatically when an alert is triggered
- Client security team detection and response training

Microsoft Sentinel Managed XDR Services include:

- Tier 3 and 4 threat escalation and investigation provided by SecureSky skilled and trained intrusion analysts, forensic investigators and engineers
- Tuning and optimization of your Microsoft Sentinel environment
- Ongoing building and maintenance of detection policies, threat hunting queries and playbooks/ response actions
- Scenario-based, threat intelligence-based and free form threat hunting
- Expert analysis of your risk and threat landscape to identify and deploy protective hardening recommendations, providing continuous improvement to your security posture

Contact us

For more information, please contact us | e: info@securesky.com | p: +1 833.473.2759 | w: securesky.com