MICROSOFT AZURE SENTINEL-BASED MANAGED THREAT, DETECTION AND RESPONSE (SOC SERVICES)

Overview

Cloud computing is an enterprise reality today as it offers flexible, cost-effective and a proven delivery platform to enable digitization of business. Due to the wide adaptation of cloud services, there is an added level of risk as some of the most essential services such as compute, network and storage is provided by the cloud provider, which makes it harder to maintain data security, privacy, and compliance.

A recent survey by CSA (March 2021)* based on inputs from C-level, security architects, security professionals and security engineers has highlighted the following top cloud security challenges faced during cloud adoption

- Lack of cloud security architecture and strategy
- Data breaches
- Misconfigurations and inadequate change control
- Insufficient identity, credential, access, and key management
- Insecure interfaces and APIs
- Limited cloud usage visibility

As industries continues to exponentially adopt cloud services, SaaS and API's based services, security threats become more advanced and sophisticated, and as a result, companies are struggling to keep up with the rapid pace of change and complexity in cyber security.

Security Information and Event Management (SIEM) solutions built for traditional environments are struggling to keep pace with today's challenges and risks.

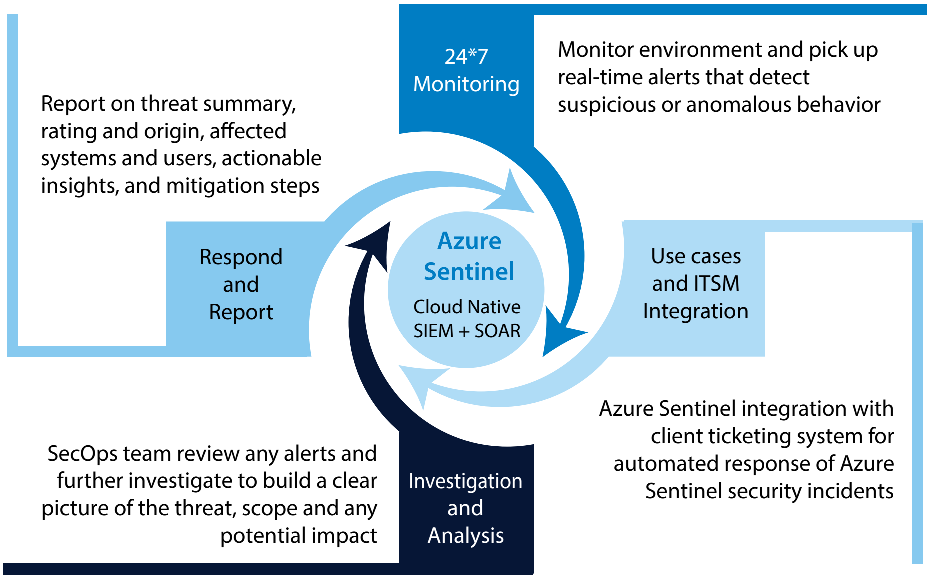
Microsoft has developed **Azure Sentinel** - a scalable, cloud-native, SIEM and Security Orchestration, Automation and Response (SOAR) solution, with in-built AI and machine learning features, enabling organizations to predict and prevent threats before they cause harm.

Azure Sentinel delivers intelligent security analytics and threat intelligence across enterprises by providing a single solution for alert detection, threat visibility, proactive hunting, and threat response.

Infosys Cloud Security Services, part of Infosys Cobalt offers cloud security advisory, cloud infrastructure protection, cloud security posture & compliance management, cloud infrastructure entitlements management, cloud managed detection & response, cloud data protection, cloud automation.

With a strong strategic and technical partnership with Microsoft, Infosys Cyber Security offers a full spectrum of security service for the Azure environment. Our services provide security and maturity assessment, security architecture design, implementation of security controls, monitoring, management, and operations of not only the Azure environment but also the hybrid cloud and O365 platforms.

Infosys + Microsoft Value Chain



Monitor environment and pick up real-time alerts that detect suspicious or anomalous behavior

Report on threat summary, rating and origin, affected systems and users, actionable insights, and mitigation steps

Azure Sentinel integration with client ticketing system for automated response of Azure Sentinel security incidents

SecOps team review any alerts and further investigate to build a clear picture of the threat, scope and any potential impact

With Infosys, Manage your Microsoft Sentinel based Security Operations

The Infosys and Microsoft Azure partnership provides Azure security capabilities that helps customers to not only accelerate their digitization and cloud journey but also manage their cyber security risks and improve the overall security posture of the environment.

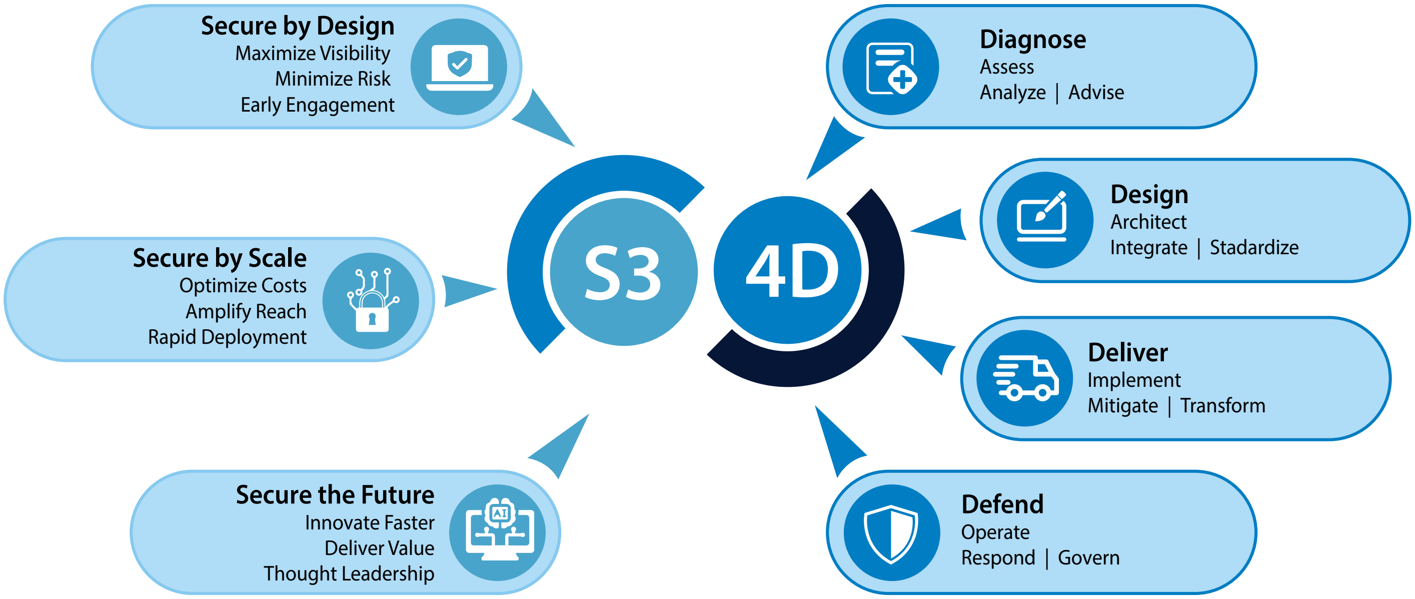
Infosys Security Operations Center (SOC) services leveraging Sentinel will enable you to deliver intelligent security analytics and threat intelligence, providing a single solution for alert detection, threat visibility, proactive hunting and threat response. Sentinel will help you have overall efficiency metrics and see incident operations over time by many different criteria, like severity, MITRE tactics, mean time to triage, mean time to resolve, and more. Azure Sentinel makes this data available to you with the new security incident table and schema in log analytics and the accompanying security operations efficiency workbook.

Services Offered

- Security monitoring and architecture design
- SIEM solution implementation using Microsoft Sentinel
- Integration with Infosys shared security monitoring infrastructure
- Custom data source integrations
- Custom threat scenario monitoring
- Custom log data retention solution

Infosys S3-4D Approach and Methodology to Deliver Enterprise Security

Infosys' approach to secure solution scope is based on our S34D model built on decades of experience, industry best practices and partnership with technology & knowledge partners.



Infosys Cyber Security instills trust into the business of our clients by enabling and enhancing their digital ambitions. Our philosophy, Digital–trust. Assured. is categorically based on the nexus of our S3-4D principle that helps enterprises navigate towards a secure future.

Guided by our S3 principles, we are committed towards building a holistic security program with our suite of service offerings, that follows a 4D approach of Diagnose-Design-Deliver-Defend

- Program guidance and requirements mapping
- Map business risks to program requirements
- Threat profiling and security baseline
- SOC operating model
- Roadmaps and integrations

DIAGNOSE

- Design and build Sentinel platform (greenfield, brownfield)
- Flexible, agile, scalable
- Multiple delivery models including private cloud, public cloud, and hybrid configurations
- Log volumes managed, use cases and playbooks

DESIGN

- 24x7 SIEM system monitoring and capacity management
- Source data feed monitoring
- Implement use cases, integrate Azure DevOps, playbooks
- Vendor mediation, upgrade and patch management

DELIVER

- Monthly and quarterly management reporting
- Enriched, SIEM ready threat feeds
- Client specific threat intelligence reporting and use cases
- Service SLAs
- Automate

DEFEND

24x7x365 Threat Monitoring

Remediation & investigation support

SIEM Health Monitoring

Infrastructure management tasks and enable effective security monitoring

SIEM Content Development

Mature & refine security intelligence

Threat Intelligence and Analytics

Actionable threat awareness

Managed Threat Service Reporting

Measure program effectiveness

Infosys' dedicated Security Operations team leverages cutting-edge Microsoft detection technology and artificial cyber intelligence, to offer an unparalleled outsourced SOC service, to ensure your cloud and on-premise environments follow cyber security best practice recommendations and crucial security policies to proactively prevent potential threats.

Business Benefits

Infosys Security Operations team provides a flexible and agile service operations model to suit your organization’s need that will help you to meet your business objective and to safeguard your data with our holistic, business service driven, SOC operations.

Comprehensive SOC operations

Triage, analysis and response integrated into a comprehensive SOC operating model reducing time and improving effectiveness. Integrated threat and risk modelling with security analysis and reporting for private cloud, public cloud, and hybrid configurations.

Respond quickly and effectively

To any security incidents to protect your data, staff and organization. Removes the noise of event logs and time-consuming task of event analysis, allowing your IT team to better focus their time. Ensures any security incidents are thoroughly investigated and can be quickly acted upon to mitigate damage and remove threats

Visibility and compliance

Provide holistic visibility into your complete asset and environment through collaboration, automation and tools with business partners and IT stakeholders within the organization. This will help in identifying threats and provide a complete view of vulnerabilities in real time, correlate and analyze them.

Optimize

Delivering flexible and adaptive security solution for securing the Azure environment through a simple engagement model with commercial flexibility to streamline the cost of Managed Security Threat Detection, Response and SoC services.

Manage risk

Single holistic view of risk and threat across the enterprise including private and public clouds with centralized integrated security knowledge repository with enhanced anomaly detection

For more information, contact askus@infosys.com

Navigate your next