SIMFORM

Microsoft

Security Offerings

Microsoft Sentinel SIEM/SOAR Implementation

Contact Us-



Hardik Shah
hardik@simformsolutions.com
Head Of Sales,
Simform



Rajat Bigghe
rajat.bigghe@simformsolutions.com
Director - Microsoft Alliance,
Simform

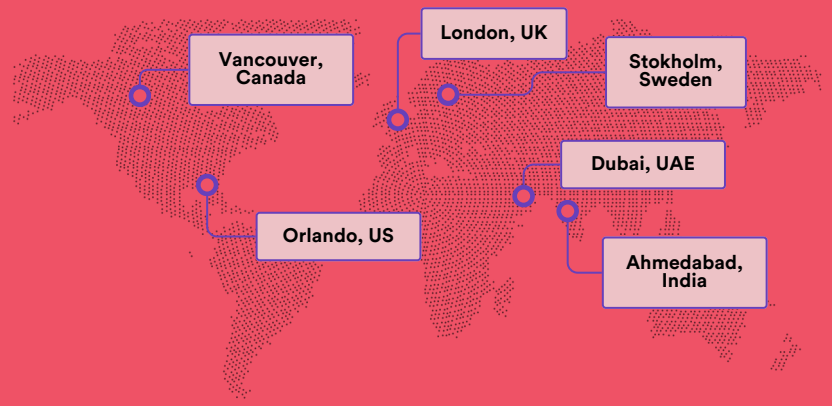
Trusted By Leading Companies, Recognized by Technology Leaders

Red Bull · FUJIFILM · Bank of America · Mitsubishi Electric
Cisco · Hilton · Renesas (Big Ideas for Every Space) · Tryg
UBT Union Bank & Trust · cameo · Hyundai Glovis · Kirloskar (Enriching Lives)

1200+
Employees

2010
Founded

6
Countries



Distinctively Recognized for Engineering Excellence

Microsoft Partner | Azure Expert MSP
Fabric Featured Partner – Microsoft
Microsoft Solutions Partner – Digital & App Innovation – Azure – Specialist: Kubernetes on Azure; Accelerate Developer Productivity with Microsoft Azure
Microsoft Solutions Partner – Data & AI – Azure – Specialist: Build AI Apps on Microsoft Azure; AI Platform on Microsoft Azure
Microsoft Solutions Partner – Infrastructure – Azure – Specialist: Networking Services; Infra and Database Migration
Microsoft Solutions Partner – Security – Specialist: Cloud Security

400+ CERTIFICATIONS **9** ADVANCED SPECIALIZATIONS

aws · Google Cloud · dbt Labs Registered Partner
databricks Consulting Partner Select · IBM Silver Partner · Advanced Datadog Partner

240+
CERTIFICATIONS

CMMI DEV | ML3 Appraised – Appraisal # 64489 | Exp. Apr 28, 2026
AICPA SOC – SOC II Compliant
ISO 27001 Information Security Management

Pushing Boundaries Through Innovation

Innovation Lab
- Lab-As-A-Service

Operational Excellence
- Co-Engineering Framework
- TalentOps Model

Solution Accelerators
- PexAI - Product Engineering Excellence
- ThoughtMesh - GenAI Framework
- +8 more Accelerators
- NeuVantage - App Modernization
- Data360 - Customer Data Platform

Go To Partner for Cloud and AI Excellence

Combining Simform's deep expertise in digital engineering with Azure's robust cloud infrastructure to deliver secure, scalable, and intelligent solutions tailored to client's business goals.



Build Cloud-Native Application And Services

Build cloud-native applications and modernize legacy applications, develop AI-native integrated services on Azure.



Modernize, Optimize and Secure Infrastructure

Build and manage secure, compliant infrastructure ensuring reliability, scalability and optimized performance on Azure.



Drive Innovation in Data and AI

Modernize data platform, Build advanced self-serve analytics, Build agents and enterprise AI platform on Azure.

Advisory & Consulting

Our Advisory and Consulting practices deliver expert guidance on Microsoft Azure, helping businesses optimize their cloud strategies, enhance security, modernize applications, and prepare for innovative technologies like GenAI.

- Migration Assessment
- GenAI Readiness and Data Platform modernization
- WAF Reviews
- App Modernization Strategy
- Cloud Optimization

Engineering & Development

Being primarily a digital engineering company, we have expertise in developing and engineering digital products, AI/ML services, data analytics solutions, application modernization on MACH principles, and QA automation.

- Application/API Engineering and Modernization
- AgenticAI & ML Development
- Data Platform Modernization and Analytics
- DevOps & Automation Implementation
- System Integration

Managed Services

Leveraging our advanced cloud engineering capabilities, we provide forward-looking cloud infrastructure managed services to digital natives and tech-enabled enterprises running more advanced IT and digital workloads on the cloud.

- Cloud Monitoring, Change and Optimization
- DevOps, SecOps, FinOps Automation
- Application Managed Services and Support
- Cloud Billing and Support

Simform Expertise of Azure Services

Expertise 

Security monitoring

- Portal
- Entra
- Multi-Factor Authentication
- Automation
- Key Vault
- Store/ Marketplace
- VM Image Gallery and VM Depot

MACH Backends

- App Service
- Functions
- Container Apps
- Kubernetes Service (AKS)
- API Management

DevOps

- DevOps
- GitHub Actions

Monitoring

- Monitor
- Application Insights
- Service Health
- Advisor

Data and Analytics

- Synapse Analytics
- Data Factory
- Cosmos DB
- Data Lake Storage
- Databricks
- Fabric
- Data Catalog
- Purview

Automation

- Automation
- Logic Apps
- Functions
- Event Grid
- Blueprints
- Resource Manager

Security and Governance

- Entra ID
- Defender
- Sentinel
- Firewall
- Key Vault
- Bastion

AI/ML

- Machine Learning
- Open AI Service
- AI Services
- AI Studio
- Copilot for security
- Open Datasets

Integration and Connectivity

- Azure Service Bus
- Azure IoT Hub
- Azure Data Factory
- Azure Relay

Hybrid Operations

- Azure AD Connect Health
- AD Privileged identity Management
- Backup
- Operational Insight
- Import/Export
- Site Recovery
- StorSimple

Infrastructure and Hybrid

- Cloud
- Virtual Machine
- Virtual Network
- Application Gateway
- VPN Gateway
- Express Routeon
- Backup
- Site Recovery
- Azure Virtual Desktop
- Azure Arc
- Azure Migrate

Security Offerings

SIMFORM

Microsoft Sentinel SIEM/SOAR Implementation

4 Weeks

Offer Description

This offers helps organizations deploy a production Microsoft Sentinel foundation that centralizes priority security telemetry and supports repeatable detection, investigation, and response.

Deliverables:

- Configure one production Microsoft Sentinel workspace with Log Analytics retention, RBAC, and workspace-level security settings.
- Onboard up to 10 Microsoft-native and 3 third-party data connectors with ingestion validation
- Implement and tune up to 20 analytics rules mapped to agreed threat scenarios
- Build up to 5 Logic Apps-based SOAR playbooks for alert enrichment, notification, containment, ticketing, or evidence collection.
- Develop up to 3 workbooks for incidents, detection, connector health, and response metrics.
- Deliver up to 25 reusable KQL hunting queries for identity, endpoint, cloud, and network investigations.
- Conduct production validation and administrator knowledge transfer covering incident triage, rule tuning, playbook operation, and ongoing governance.

Key Azure Services

Sentinel | Azure Monitor | EntraID | Log Analytics | Logic Apps

Commercials $15000

Get this offer at Zero cost by leveraging Microsoft Accelerate Funding Program