Exelegent

Gold Microsoft Partner Microsoft

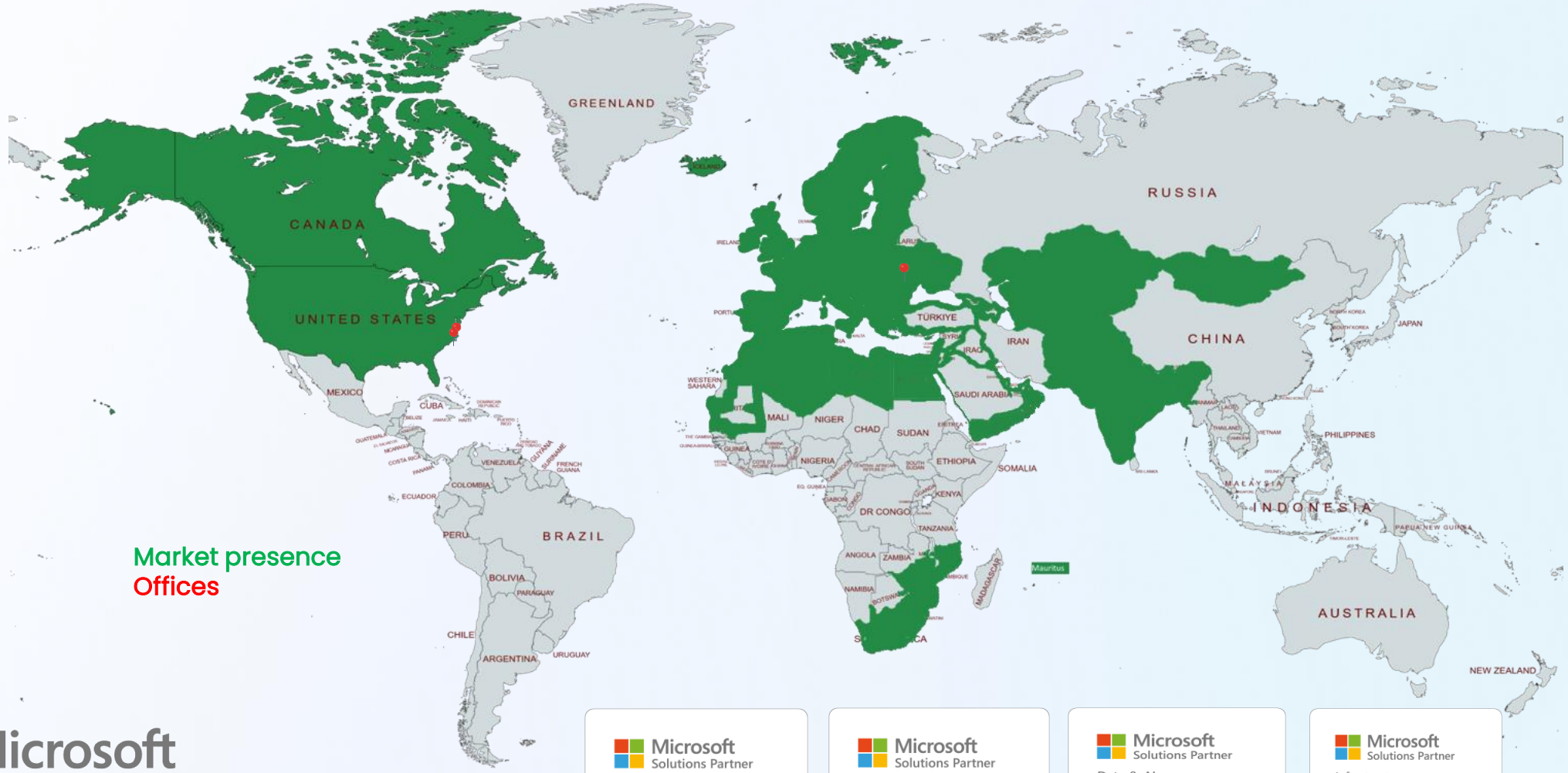
01.

Microsoft Sentinel Migrate & Modernize

By Exelegent & Microsoft

About Exelegent

- Market presence in 45+ countries
- 3 Global Offices with US East Coast HQ
- Workforce presence in 13 countries
- MPN: 2875555



Microsoft Solutions Partner

Microsoft Solutions Partner
Modern Work

Microsoft Solutions Partner
Security

Microsoft Solutions Partner
Data & AI
Azure

Microsoft Solutions Partner
Infrastructure
Azure

BUILD. INTEGRATE. THRIVE.

Exelegent Practices Lead New Era of Computing and Opportunities

Digital Workplace

Aimed at fostering **secure collaboration** and ensuring **seamless operations** in the **modern work** landscape

Security & Compliance

Dedicated to **fortifying organizations** against evolving cyber threats and building business **cyber resilience**

Data & AI

Business Intelligence and **AI** solutions to enhance operations and drive **transformative outcomes**

BPO

Bring **efficiency, innovation,** and **scalability** to organizations seeking streamlined processes and **enhanced productivity**

Value-Added Reseller

Unique and **efficient solutions** to address **business growth** and **technology innovation**

TrustElements.com

Intelligent and Quantified Continuous and Automated **Cyber Risk Management**

Our success is measured by your own

DermOne Dermatology

Bruce Lucarelli, CTO, DermOne

"Switching to Exelegent has been a major contributing factor to the growth of our group. As a company looking to expand, we really value our employees' time and productivity. Exelegent's IT Support has enabled our business to run as efficiently as possible."

Alexey Gololobov, CFO, Columbus Hospital

Exelegent has been with our hospital since we've opened our doors. Their experience in a wide range of projects and solutions, and management of vendors has made a tremendous impact on our efficiency

inflexion point

Kevin Hannigan, President, Inflexion Point

Exelegent has become our trusted business partner and completed migration on time, alleviated hosting responsibilities, and gave us capabilities to enable team productivity and data security.«

CITYMD URGENT CARE

Robert Florescu, CISO, CityMD

Exelegent helped our company migrate from G-Suite to Microsoft Office 365 with zero downtime and zero data loss. During the process, over 3,500 users continued to collaborate and run critical business functions seamlessly

PRISM Vision Group · fastpacehealth · Summit Health · ETS · OceanFirst Bank · CollegeBoard · Sound Physicians · VillageMD

CITYMD URGENT CARE · bai · American Valve · Sentry Management Community Association Management · CENLAR Central Loan Administration & Reporting · Saint Peter's University · opentext · Reid Health

Astrana Health · CentraState Healthcare System Atlantic Health System Partner · Warburg Pincus · Renaissance · WORLD · DermOne Dermatology · inflexion point

Why Enterprises Are Moving Toward a Modern SIEM

Attack surface is expanding due to growing digital estates and hybrid work

Rapid acceleration and increasing sophistication of cybercrime

Rising costs of silos, licenses and staff

Complex set-up and maintenance of on-premises infrastructure

Move faster with simplified threat detection and response

Infrastructure

Devices

Users

Applications

Modernize Security Operations with Microsoft Sentinel

Cloud-native

Powered by AI

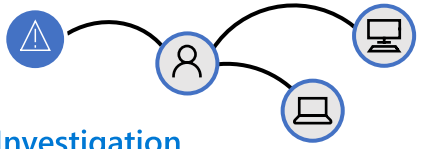
300+ partner integrations

Built-in automation

Across multi-cloud, multiplatform

Powered by community + backed by Microsoft security experts

Detection
Correlate alerts into actionable incidents using machine learning



Investigation
Visualize the full scope of an attack

Response
Act immediately with built-in automation

Threat hunting
Hunt across all data with powerful search and query tools

GOALS

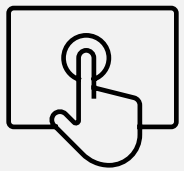
What to Expect

- **Thorough Assessment**
  A deep dive into your current security posture and goals to ensure the engagement is perfectly tailored.
- **Tailored Design & Implementation**
  End-to-end support in architecting and deploying Microsoft Sentinel, complete with data connectors and automation.
- **Ongoing Enablement**
  Hands-on training sessions and best-practice guidance to empower your security team post-migration or modernization.
- **Comprehensive Support**
  Continuous monitoring, fine-tuning, and 24/7 customer service for lasting success and optimal ROI.

Use Case I: Implementing Microsoft Sentinel from the Ground Up

Assessment and Planning

- **Discovery:** Evaluate the current SIEM/SOAR needs, identifying data sources, event volume, and required integrations.
- **Planning:** Define business goals, timelines, and success criteria. Establish an architectural roadmap aligned with your security and compliance requirements.

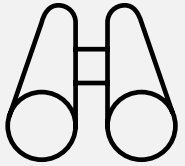


Architecture and Design

- **Cloud Readiness:** Validate infrastructure and assess network requirements for Microsoft Sentinel
- . **Solution Blueprint:** Craft a detailed design covering data connectors, analytics rules, automation scenarios, and role-based access control.

Implementation and Integration

- **Deployment** Set up Microsoft Sentinel in Azure, configure data connectors, ingest logs, and activate security workloads.
- **Integration:** Migrate existing workflows, alert rules, and automation playbooks. Integrate with other Microsoft and third-party security solutions for a unified security posture.



Testing and Validation

- **Functional Testing:** Verify log ingestion, alert rules, and automation routines. Ensure all critical workflows from the previous SIEM are functioning in Sentinel.
- **Security Validation:** Conduct penetration testing or simulated threat scenarios to confirm detection and response effectiveness.

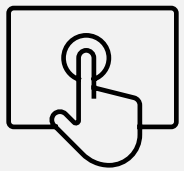
Training and Operational Handoff

- **Knowledge Transfer:** Provide hands-on training for security teams, focusing on Sentinel's incident management, investigation, and response tools.
- **Ongoing Support:** Offer post-migration monitoring, tuning, and best practices to maintain and optimize your new cloud-native SIEM environment.

Use Case II: Modernizing and Enhancing Microsoft Sentinel

Current State Evaluation

- **Review and Gap Analysis:** Examine your existing Microsoft Sentinel setup, identifying performance gaps, compliance issues, or outdated configurations.
- **Prioritization:** Determine key areas for modernization, such as log sources, analytics rules, automation capabilities, or advanced threat intelligence integrations.

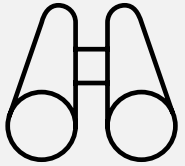


Enhanced Architecture Planning

- **Advanced Features Roadmap:** Identify underutilized Sentinel features (e.g., machine learning analytics, SOAR capabilities) and plan for their introduction or improvement.
- **Scalability Strategy:** Ensure your environment can handle increased data volume, new integrations, and future growth.

Solution Redesign and Upgrades

- **Implementation of Advanced Analytics:** Introduce or update ML-based alerts, custom detections, and enrichment data sources.
- **Automation and Playbooks:** Modernize incident response processes by creating or refining playbooks for faster, automated threat containment.



Integration and Testing

- **Holistic Security Integration:** Connect Sentinel with related Microsoft services (e.g., Defender suite) and third-party security tools for a consolidated threat view.
- **Validation:** Conduct thorough testing—performance checks, alert tuning, and scenario-based tests—to confirm that modernized features operate effectively.

Operational Maturity and Continuous Improvement

- **Ongoing Monitoring and Optimization:** Track key metrics (e.g., Mean Time to Detect/Respond) to gauge effectiveness and ensure continuous refinement.
- **Training and Best Practices:** Equip security analysts with knowledge of new capabilities, ensuring they can manage and expand your modernized SIEM effectively.

What’s in It for You?

1. **Accelerated SIEM Adoption**

Quickly transition to or enhance your cloud-native SIEM & SOAR solution to stay ahead of evolving threats.

2. Cost-Efficient Optimization

Leverage consumption-based pricing and integrated tools to reduce hardware and operational expenses.

3. Advanced Threat Detection

Harness Microsoft’s AI and machine learning capabilities for superior incident detection and automated response.

4. Future-Proof Security Posture

Stay current with continuous innovations and gain a holistic view of your entire security environment.

Maximizing Impact – The Right Audience

- **Security and IT Leaders**
  Professionals responsible for defining security strategy and allocating budget for cybersecurity initiatives.

- **SIEM Administrators and Engineers**
  Technical experts who manage daily operations of SIEM and need insights into advanced threat detection and response.

- **Cloud Architects and Infrastructure Teams**
  Teams tasked with migrating on-premises systems to the cloud and ensuring seamless integration with existing infrastructure.

- **Compliance and Risk Officers**
  Stakeholders who oversee regulatory compliance and want to ensure that security controls and reporting meet organizational and legal requirements.

- **Managed Service Providers (MSPs) and Consultants**
  Third-party security providers who offer or plan to offer Microsoft Sentinel-based services to their clients.

❑Check Your Eligibility

❑Reach out to see if you qualify for a free engagement.

❑If you don’t qualify, let us craft a solution tailored to your unique needs

❑ **Pricing, Terms & Conditions**

- Free for Qualified/Eligible Customers
- Variable Terms for Other Customers & Customized Solutions