Microsoft – Sentinel Migration & Modernization Engagement

Leverage Grant Thornton's dedicated team of Microsoft certified engineers & analysts to maximize your Microsoft investment.

Solution Benefits

- ✓ **Lessons learned from the field. Our expertise and knowledge base can be used as accelerators to streamline the implementation process.**
- ✓ **Our deep understanding of the Microsoft platform will allow us to advise you on leading practices to follow and common misconfigurations to avoid for a successful implementation.**
- ✓ **Integration experience to guide success by avoiding items that sound good but don't work and the reason why.**

Grant Thornton's Microsoft Sentinel Migration & Modernization Engagement help customers solve complex cyber challenges; which include creation of efficient cyber threat monitoring solutions for security operations, bolstering insider threat programs, and building unique cyber fraud detection capabilities. Our deeply qualified teams bring the right mix of technical expertise and operational acumen to align your Microsoft investment with your overall program goals and objectives.

Experienced Staff - Our team members are comprised exclusively of Microsoft certified Engineers & Analysts dedicated to providing deployment and implementation services for Microsoft's entire product suite.

Lessons Learned - Our services and recommendations are based on lessons learned in the field performing this work, not theories. Our deployment and integration services experience guide success by avoiding items that sound good but don't work and knowing the reason why.

Insight Into Cyber Risks - Our purpose-built content and models align implementations to leading risk areas such as insider threat, cyber fraud, and cyber operations automation.

When Grant Thornton implements Microsoft suite product(s) for your organization, our team of specialists will prepare for the various aspects of the Microsoft solution to ensure details and dependencies for your environment are identified and addressed. From planning out data source quality, use cases analysis, and training of your staff, our team will leverage their expertise to provide a solution that your team is ready to operate day 1 to support your environment.

Grant Thornton's Microsoft Services

Deployment and Integration
Deployment and integration of data sources into Microsoft Sentinel & Defender products for your organization

Managed Cyber Analytics
Continuous managed detection and response services leveraging your Microsoft Sentinel & Defender solutions

Solution Management Service
Managed engineering and custom content support for your Microsoft Defender XDR and Sentinel SIEM solution

Custom Engineering and Integration
Bespoke use cases and content engineering services for your Microsoft Defender XDR and Sentinel SIEM solution

Grant Thornton's Sentinel Migration & Modernization Engagement Approach

Planning

- Conduct initial kickoff meeting and review project plan
- Review roles and responsibilities between Grant Thornton & Customer staff
- Review process for change control
- Review data sources in scope, use cases, and workflow requirements
- Conduct log feed engineering and planning
- Review the deployment planning for endpoint agents, where required

Key Outputs:

- Kickoff slide deck
- Customer questionnaire

Implementation

- Deploy and configure Sentinel in the tenant
- Configure Microsoft feeds ingestion in Microsoft Sentinel
- Configure log feeds for data source ingestion in Microsoft Sentinel via 'Content Hub'
- Review data parsing and modify data source ingest as required
- Configure playbooks, workbooks and automation rules
- (Optional) Create Sentinel Advanced Hunting queries for threat hunting use cases
- (Optional modules) Endpoint Protection & Hybrid Identity Protection

Key Outputs:

- Deployment review with customer staff

Results & Next Steps

- Review Sentinel incidents and tune alerts to reduce false positives
- Review data ingestion per log source
- Recommendations for enhancing security log ingestion & monitoring
- Remove trial licenses and any engagement configurations from tenant
- Conduct Engagement close out meeting

Key Outputs:

- Deployment document highlighting Engagement results & recommendation

Why Grant Thornton?

- ✓ Microsoft certified services partner with direct access to Microsoft's engineering, product development and customer support teams
- ✓ Experience and expertise with the implementation and operation of Microsoft technologies for numerous programs including, but not limited to Microsoft Defender, Sentinel, Entra ID, Purview, and Intune
- ✓ Specific risk models and workflows built for Microsoft to support cybersecurity programs
- ✓ Backed by a national team of cybersecurity and privacy professionals to meet the needs of your cyber program

Contact

John Pearce
Principal
T +1 703 637 4071
E John.Pearce@us.gt.com

Don Sheehan
Managing Director
T +1 703 847 7642
E Don.Sheehan@us.gt.com

Microsoft Solutions Partner
Security
Specialist
Cloud Security
Threat Protection

Grant Thornton