



# Microsoft – Threat Protection 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 Threat Protection Engagement helps 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 Threat Protection 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
- (Optional) Provide an overview of Microsoft Sentinel & Defender XDR products
- Provide customer with Threat Protection Engagement questionnaire
- Discuss integration approach for Microsoft Sentinel and Defender XDR

### Key Outputs:

- Kickoff slide deck
- Customer questionnaire



## Implementation

- Deploy engagement trial licenses and subscriptions
- Deploy each Defender XDR platform and apply configuration policies (Defender for Endpoint, Office 365, Cloud Apps, Vulnerability Management & Entra ID Protection)
- Deploy and configure Sentinel in the tenant
- Configure data source ingestion into Sentinel via connectors and the Syslog agent VM
- Configure playbooks, workbooks and automation rules
- Create Sentinel Advanced Hunting queries for threat hunting use cases
- Configure Vulnerability Scanning

### Key Outputs:

- Deployment review with customer staff



## Results & Next Steps

- Review incidents & alerts in Microsoft Sentinel & Defender XDR
- Review results in Defender for Vulnerability Management
- Review risky users in Entra ID Protection
- Remove trial licenses and any engagement configurations from tenant
- Review recommendations to increase Microsoft Secure Score
- Conduct engagement close out meeting

### Key Outputs:

- Deployment document highlighting top threats & 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



"Grant Thornton" refers to the brand under which the Grant Thornton member firms provide assurance, tax and advisory services to their clients and/or refers to one or more member firms, as the context requires. Grant Thornton LLP is a member firm of Grant Thornton International Ltd (GTIL). GTIL and the member firms are not a worldwide partnership. GTIL and each member firm is a separate legal entity. Services are delivered by the member firms. GTIL does not provide services to clients. GTIL and its member firms are not agents of, and do not obligate, one another and are not liable for one another's acts or omissions.

© 2024 Grant Thornton LLP. All rights reserved. U.S. member firm of Grant Thornton International Ltd.