Grant Thornton

Microsoft Sentinel and Defender

Integration and Managed Services

Grant Thornton Overview – Microsoft Services

Grant Thornton is a security alliance partner with Microsoft. Our managed security services team has executed over 70 different implementation and services engagements working with industry leading security products, helping clients solve complex cyber challenges; which include complex cyber challenges which include cloud SIEM and Log management, endpoint threat detection, email threat prevention and cloud visibility monitoring.

GT Experience

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 experienced engineers who are dedicated to providing implementation and monitoring services support to our client's Microsoft Sentinel & Defender product suite.

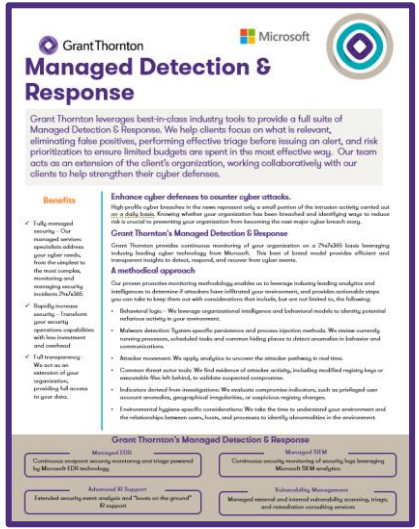
Lessons Learned
Our services and recommendations are based on lessons learned in the field performing this work, not theories. Our integration and monitoring services experience guide success by avoiding items that sound good but don't work and the reason why.

Insight Into Cyber Risks
Purpose built content and models to align implementations to leading risk areas such as ransomware, nation state actors, and cyber operations automation.

GT Services For Microsoft

Deployment Services
Rapidly deploy and integrate your Microsoft security solution

Microsoft SMS
Managed Microsoft Sentinel & Defender engineering support (includes custom content support)



Microsoft MDR
24x7 security monitoring, response, and engineering support

Grant Thornton – Microsoft Offerings

- Overview sessions for Defender modules (Identity, Endpoint, Office 365, Cloud Apps) for technology simplification
  - ✓ **Outcome/benefit:** Determine solution coverage, tool rationalization/reduction

- Sentinel and Defender Readiness Workshop (estimated half day)
  - Data connectors, data element fidelity, applicable analytics alerts
  - Endpoint, Office 365, Cloud Apps, and Identity compatibility
  - Monitoring and response operating models
  - ✓ **Outcome/benefit:** Understanding of prerequisites and dependencies for a successful deployment/migration

- Sentinel and Defender Deployment and Usage Workshops (2-3 weeks)
  - Testing/verifying capabilities and usage for permanent deployment
  - ✓ **Outcome/benefit:** Proven operational capabilities for full scale deployment

GT Managed Detection and Response Services

GT leverages best-in-class industry tools to provide a full suite of managed security services. We help clients focus on what is relevant, eliminating false positives, performing effective triage before issuing an alert, and risk prioritization to ensure limited budgets are spent in the most effective way. Our team acts as an extension of the client's organization, working collaboratively with our clients to help strengthen their cyber defenses.

Where we're located (main hubs)

Our managed security services are operated 24x7 from our Kansas City and Bangalore cyber centers, and backed by advanced engineering and incident response support across the country:

Capability Overview

People

Dedicated team, staffed 24x7x365, based in GT's two cyber centers, supported by seasoned engineering and incident response specialists to support a variety of client scenarios

Technology

Grant Thornton's managed security services are powered by Microsoft, CrowdStrike, and Exabeam, industry leaders in SIEM and EDR technology

Experience

Certified team that has supported over 70 clients across the financial services, healthcare, technology, manufacturing, and retail industry

Managed SIEM

Continuous security monitoring of security logs leveraging Microsoft Sentinel analytics and automation

Managed Defender

Continuous endpoint security, identity monitoring, cloud security, and Office 365 triage powered by Microsoft's Defender technology

Advanced IR Support

Extended security event analysis and "boots on the ground" IR support

Benefits With Grant Thornton

- Engineers that work with you during your business hours as opposed to cold email handoffs from overnight analysts
- GT’s Microsoft managed services are operated out of GT locations in the United States (Kansas City, Washington DC, Chicago, San Francisco), and leverage GT's services center in India
- **In GT's delivery model:**
  - The client owns the Microsoft licensing
  - GT accesses the client’s Microsoft solutions to provide integration and managed services
  - The client maintains the same level of access and visibility in the Microsoft solution as the GT services team
- **Support your team with incident response**
  - Provide recommendations and consultation during incidents
  - Review and assemble supporting data related to an incident
  - Provide “boots on the ground” support via retainer hours with the option for full forensic analysis upon request – Can be built in upon request

Why Grant Thornton?

Our Cybersecurity & Privacy practice encompass focused services for helping our clients assess and improve their information security program. We have technology alliances in all of our service areas to enable us to build and deliver innovative and pragmatic solutions for our clients.

We bring you a diverse team of **100 + security and risk consultants and Cyber SMEs** focused on Cybersecurity & Privacy consulting.

Our credentials:

50+ practitioners have security and privacy certifications

We manage and deliver information security assessment and benchmarking services that give us access to **lessons learned from the trenches**.

In the past year…

30 + information security program or capability assessments

50+ technical security testing

We are more than just consultants. We are **thought leaders and active in the industry**. we have developed many forward-thinking thoughtware to help our clients significantly advance their Cyber programs.

In the past three years…

30 + whitepapers
40 + webcasts/Seminars

We are not only assessors but implementors. Our implementation experience and know-how enable us to provide practical and real-life recommendations for our assessment services.

Our select alliance partners include:

exabeam, servicenow, Microsoft, CROWDSTRIKE, OneTrust Data Privacy Software, SECURITI.ai

Grant Thornton

Cybersecurity & Privacy solution offerings

We utilize a three-pronged approach to assess, implement and manage (AIM) cyber risk processes. This helps our clients make informed decisions about their business strategy, develop an integrated cyber risk strategy and implement comprehensive solutions to manage cyber risks. Our services portfolio include:

Cyber Strategy & Transformation

Assess
- Cyber security risk assessment
- Regulatory and compliance readiness
- Cyber resiliency assessment
- GRC program and strategy review
- Cyber M&A due-diligence review

Implement
- Cyber regulatory change program
- GRC automation, design and implementation
- Cyber risk governance and operating model
- Cyber resiliency strategy and program
- Cyber risk reporting and analytics
- M&A post transaction cyber integration

Manage
- Managed cyber metrics and reporting
- Cyber resiliency plan management and periodic testing
- Ongoing GRC platform and operational support

Cyber Defense Solutions

Assess
- Vulnerability assessment, penetration testing, and adversary emulation assessment (AEA)
- Proactive compromise assessment
- Cyber incident tabletop exercises
- Cloud security assessment
- SOC/Cyber defense capability assessment

Implement
- Cybersecurity analytics & endpoint defense implementation
- Incident Response playbook automation
- Insider threat program design & implementation

Manage
- Managed Security Incident and Event Management (SIEM) services
- Managed Endpoint Detection and Response (EDR) services
- Ongoing vulnerability management

Privacy & Data Protection

Assess
- Privacy program maturity and benchmarking assessment (NIST)
- Privacy regulatory compliance assessment (GDPR, CCPA/CPRA, GLBA, PIPL, etc.)

Implement
- Privacy tool implementation
- Data inventory & discovery
- Consent & preference automation
- Data subject rights automation
- Data retention & disposal program
- Privacy training, awareness, and privacy liaison programs
- Privacy governance and metrics

Manage
- Privacy managed services – data inventory and discovery, Privacy Impact Assessments (PIAs), privacy platform management
- Internal and vendor privacy compliance monitoring

Identity & Access Management

Assess
- IAM program maturity assessment
- IAM vendor evaluation and selection
- IAM strategy, roadmap & business case development

Implement
- Identity & access management solution implementation (cloud & on-prem)
- Identity governance implementation and application onboarding
- Privileged account management implementation
- Role-based access control implementation
- External (customer) identity & access management solution implementation
- Migration from legacy to new IAM platform

Manage
- Managed identity services
- IAM platform upgrade and management

3rd Party Security Risk Mgmt.

Assess
- TPRM program and maturity assessment
- TPRM strategy and roadmap
- Software supply chain security assessment

Implement
- TPRM governance design and implementation
- TPRM tool selection, implementation & optimization
- TPRM process standardization and cost optimization
- Software supply chain security governance and solution implementation

Manage
- Ongoing 3rd party risk assessments
- Software Supply Chain Security / Open-Source code use assessments and planning
- CI/CD pipeline security assessments
- Continuous Open-Source code vulnerability monitoring

Grant Thornton – Organization overview

	Grant Thornton member firms worldwide**	U.S. member firm
Revenue (USD)	$5.76 billion	$1.92 billion
Personnel with Partners & SSC	58,229	8,459*
Partners / Principals	3,708	595
Offices	779	53
Statistics as of:	Sept. 30, 2020	Jul. 31, 2020

*Total personnel includes professionals in the GTUS Shared Services Center (SSC) and GTUS Knowledge and Capability Center (KCC), collectively referred to as INDUS or the India shared services center, which is based out of Bangalore. SSC and KCC are joint ventures with the Grant Thornton U.S. member firm, therefore these professionals are included in U.S. employee data.

**Combined statistics of Grant Thornton International Ltd (GTIL) member firms. GTIL and the member firms are not a worldwide partnership. Services are delivered by the member firms. 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. Please see GT.com for further details.

135+

Grant Thornton member firms operate in 135+ countries.

Thriving since 1924, our U.S. firm is people-focused and purpose-driven. We believe business should be more personal and that the strongest results start with trust.

Who we serve

- 44% Fortune 100 companies served
- 37% Fortune 500 companies served
- 34% Fortune 1000 companies served
- 31% Russell 1000 companies served
- Top 5 auditor of Russell 2000 companies
- Top 5 firm for IPOs (2010 – present)

An award-winning organization, year after year.

Select awards for Grant Thornton International Ltd and Grant Thornton LLP

Grant Thornton

Appendix

Grant Thornton's Integration Approach

Planning

- Conduct initial kickoff meeting and review project plan
- Review data sources, alerts, and workflow requirements
- Provide customer questionnaire
- Conduct log feed engineering and planning for Microsoft Sentinel data sources where required
- Discuss the deployment approach for Microsoft Defender modules for necessary endpoints, cloud, M365, and Identity

Key Outputs:

- Implementation project plan

Integration

- Initiate platform onboarding (system access, current state data sources, and analytics alert configuration review)
- Configure log feeds for data source connection to Microsoft Sentinel
- Deploy Microsoft Defender modules
- Integrate Defender alerts into Sentinel
- Implement customer specified use cases and assist in performing any additional configuration updates

Key Outputs:

- Deployment review with client staff

Review and Training

- Review and tune alert outputs for environment, adjust based on feedback and analysis
- Final reviews of data sources and tuning
- Conduct client training on solution usage and use cases deployed
- Finalize engineering deployment document and review with client staff
- Conduct project close out meeting

Key Outputs:

- Solution turned over to client staff
- Final report delivered

Grant Thornton

GT/Microsoft Workshops

In order to maximize your investment in Microsoft services, GT can conduct the following workshops in partnership with Microsoft on the following topics:

- Microsoft Sentinel Overview
- Microsoft 365 Defender Overview
- Microsoft Defender for Identity Overview
- Microsoft Defender for Cloud Apps Overview
- Microsoft Defender for Endpoint Overview
- Sizing your Environment

Grant Thornton

Microsoft Sentinel Integration Details

GT's Microsoft Sentinel integration empowers organizations to centralize and streamline their security operations, leveraging powerful threat detection, incident response, and automation capabilities. Our integration service provides the following:

- Setup of Microsoft Sentinel Workspace(s)
- Onboarding of Microsoft and non-Microsoft data sources into Microsoft Sentinel
- Setup and configuration of Microsoft Sentinel Workbooks
- Training of how to use Hunting in Microsoft Sentinel via Search and Azure Notebooks
- Training of how to use Automation Playbooks for Analytics triggers

Microsoft Defender Integration Details

GT's Microsoft Defender integration offers organizations a unified approach to securing their digital environments. By combining Microsoft's advanced threat protection capabilities across endpoints, email, identities, and cloud, our integration service provides the following:

- Configuration of Microsoft Defender for Endpoint, Defender for Identity, 365 Defender, and Defender for Cloud
  - Validation that all Defender Endpoints are visible in the Defender GUI with appropriate threat protection and detection policies applied
  - Validation that Defender for Identity sensors are deployed with specific accounts excluded if necessary
  - Setup of automated threat investigation and remediation if desired
  - Integration with Microsoft Sentinel if required
  - Integration of Defender for Cloud with cloud services and setup of detective and preventative policies

Grant Thornton performed this engagement in accordance with American Institute of Certified Public Accountants Statements on Standards for Consulting Services. This was not an attest engagement; accordingly, Grant Thornton did not render any form of opinion or assurance on financial statements nor internal controls over financial reporting.