

# ALFA Connections Managed Security Operations Center





Singapore

Personal information of parents, staff at 127 schools accessed in data security breach

4 months ago



Business

Live Nation confirms Ticketmaster hack amid user data leak concerns

2 months ago



Singapore

Poh Heng Jewellery hit by data breach, customers' personal information may have been compromised

4 months ago

Downtime, lost productivity, and damage to customer trust

Business Continuity

Strain IT and security teams

Internal threats or unintentional mishandling of data



Singapore

Carousell fined S\$58,000 over data leaks that affected more than 2.6 million users

6 months ago

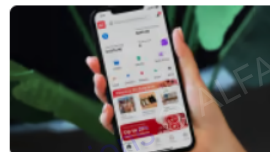
Delayed responses and increased damage



Singapore

Personal data of 128,000 customers of moneylenders stolen after IT vendor hacked

16 days ago



Singapore

ShopBack fined S\$74,400 over leak of more than 1.4 million customers' personal data

12 months ago

**\*SG Data breaches surged 319% in last two years. Q4 2023 – 86,317 cases. 38<sup>th</sup> among 250 countries worldwide**

## Customer Pain Points

### 1. Security Threats and Data Breaches:

Enterprises face constant threats from cyberattacks, unauthorized access, and data breaches.

### 2. Compliance Requirements:

Many industries are subject to strict regulatory requirements (e.g., GDPR, HIPAA, SOX) that mandate detailed record-keeping of user activities.

### 3. User Activity Visibility:

In large organizations, it's challenging to keep track of what users are doing across the Microsoft 365 environment

### 4. Incident Response Time:

Security teams may not be aware of a security incident until it's too late

### 5. Operational Efficiency and Resource Allocation:

Manually monitoring logs and ensuring compliance can be time-consuming and resource-intensive

### 6. Unauthorized Access and Account Compromise:

Risk of unauthorized access and account compromise has grown, especially through tactics like phishing or brute-force attacks.

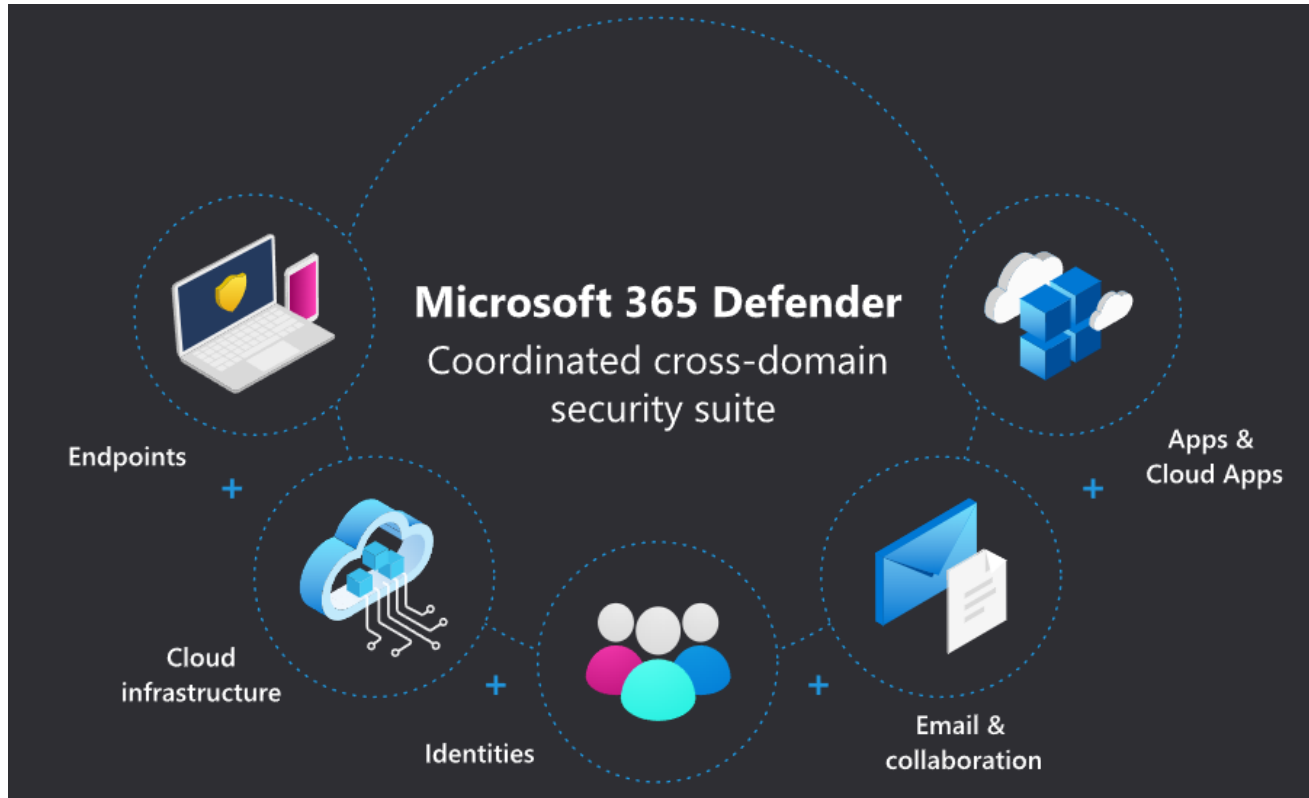




# Managed Security Operations Center

## Proactive Protection and Real-Time Threat Response

The Managed Security Operations Center (SOC) utilizes the advanced capabilities of Microsoft 365 Defender Extended Detection and Response (XDR) and Microsoft Sentinel (SIEM & SOAR) to deliver a robust and proactive security posture for organizations. This service integrates seamlessly with existing infrastructure, ensuring optimal threat detection, response, and prevention to safeguard digital assets around the clock.



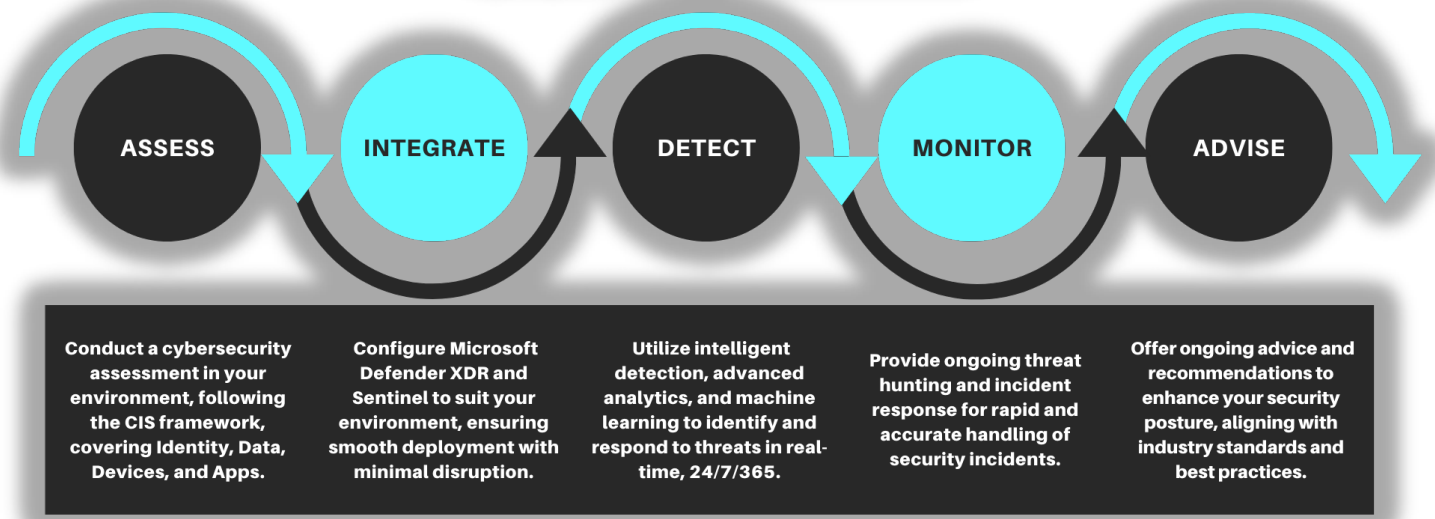
## Target Audience

- ❖ Enterprises with significant investments in Microsoft technologies
- ❖ Companies operating in highly regulated industries
- ❖ Businesses seeking to enhance their security posture with minimal disruption
- ❖ Organizations facing sophisticated cyber threats and seeking expert guidance

## Benefits

- ❖ **Enhanced Security:** Reduces cyber threat risks with real-time protection.
- ❖ **Cost Efficiency:** Lowers operational costs through a transparent subscription model.
- ❖ **Expert Support:** Provides certified professionals for technical and strategic advice.
- ❖ **Scalability:** Adapts to your security needs as your business grows.
- ❖ **Compliance:** Ensures adherence to ISO27001 and other standards.

## MULTI-TIERED APPROACH



## Eligible Workloads

- Microsoft Entra ID
- Microsoft Purview
- Microsoft Intune
- Microsoft Sentinel
- Microsoft 365 Defender XDR
  - Microsoft Defender for Endpoint
  - Microsoft Defender for Office
  - Microsoft Defender for Identity
  - Microsoft Defender for Cloud Apps
  - Microsoft Defender for Vulnerability Management
- Microsoft Defender for Cloud

## SOC Team Levels Roles and Responsibilities

SOC Analyst I	SOC Analyst II	SOC Analyst III	SOC Manager
<ul style="list-style-type: none"> <li><input type="checkbox"/> Monitoring and Initial Alert Triage</li> <li><input type="checkbox"/> Incident Documentation and Escalation</li> <li><input type="checkbox"/> Leveraging Microsoft Defender XDR</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Deep Dive Analysis and Threat Hunting</li> <li><input type="checkbox"/> Fine-Tuning Detection Systems and Automation</li> <li><input type="checkbox"/> Leveraging SIEM, EDR, XDR, and Threat Intelligence</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Overseeing Incident Management and Response</li> <li><input type="checkbox"/> Mentoring and Developing SOC Procedures</li> <li><input type="checkbox"/> Managing Audits and Compliance Reviews</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Strategic Oversight and SOC Operations Management</li> <li><input type="checkbox"/> Policy Development, Compliance, and Technology Integration</li> <li><input type="checkbox"/> Leading Auditing and Regulatory Compliance Efforts</li> </ul>

Summary of Incidents

Recommendation steps


Option to activate managed service for remediation

## ALFA Managed Security Operations Center

Microsoft Sentinel Monthly Incident Report

AA ALFA Demo Admin <demo.admin@alfa-iaas-ad.com>  
 To: Thin Thin Ei; ALFA Demo Admin; Soe Minn Win

High importance

 **alfaconnections**

**Your Monthly Incident Report for Company Name**

Thank you for using Alfa Connections Managed Service. This Monthly Report provides a summary of the incident alerts detected during this month:

**Security Alerts by Severity**

Total Alerts 809	High 0
Medium 805	Low 4

**Top Four Entities in Security Alerts**

Target	Entity Type	Count
thinthin.ei@alfa-iaas-ad.com	account	193
2001:fb1:56:ce42:2472:a64d:ba19:785c	ip	115
demo.admin@alfa-iaas-ad.com	account	50
49.245.87.248	ip	50

**Most Common Alerts**

Alert Title	Alert Count	Recommendation
TestCustomEntities	376	<a href="https://learn.microsoft.com/en-us/defender-for-identity/remediation-actions">https://learn.microsoft.com/en-us/defender-for-identity/remediation-actions</a>
Detect Creation of Anonymous Link and access from uncommon user agents	194	<a href="https://learn.microsoft.com/en-us/defender-cloud-apps/anomaly-detection-policy">https://learn.microsoft.com/en-us/defender-cloud-apps/anomaly-detection-policy</a>
User Sign-In from Asia During Off-Hours (Alfa)	182	<a href="https://learn.microsoft.com/en-us/defender-for-identity/remediation-actions">https://learn.microsoft.com/en-us/defender-for-identity/remediation-actions</a>
Detect changes in SPO External sharing settings	84	<a href="https://learn.microsoft.com/en-us/sharepoint/turn-external-sharing-on-or-off">https://learn.microsoft.com/en-us/sharepoint/turn-external-sharing-on-or-off</a>

[Check more Incident alert details in Microsoft Sentinel](#)



## Managed Security Operations Center Sample SOW

- Phase 1** **Project kick-off**
- Phase 2** **Assessment**
- Phase 3** **Planning**
- Phase 4** **Integration**
  - Microsoft Entra ID Protection
  - Defender for Office 365
  - Defender for Endpoint
  - Defender for Cloud App
  - Defender for Identity
  - Microsoft Intune
  - Microsoft Purview
  - Microsoft Sentinel
  - Microsoft Defender for Cloud
- Phase 5** **User Acceptance Test (UAT)**
- Phase 6** **Documentation**
- Phase 7** **Knowledge Transfer**
- Phase 8** **Go-live & Monitor**
- Phase 9** **Hunt, Triage, Investigate, and respond with Monthly incident report**

Thank You