DEFEND

A guide to SOC/SIEM.

What's right for your organisation?

created in partnership with DEFEND

Tertiary Education Commission
Te Amorangi Mātauranga Matua

As criminals get smarter and more aggressive with their attacks, it's becoming harder for organisations to stay safe. Increasingly, more businesses are looking at specialty security solutions to help them monitor threats and respond to these quickly.

This guide has been developed to help unravel the complexities of one of these solutions, a SOC/SIEM. It will help you to consider factors like prerequisites and type of organisation, while providing a clear overview of what costs to expect without requiring you to go through a lengthy procurement and discovery phase.

The guide was developed by the Tertiary Education Commission (TEC) in partnership with DEFEND. It has been validated by a SOC/SIEM implementation at TEC and Te Wānanga o Aotearoa.

What is a SOC/SIEM?

A SOC (Security Operations Center) is a dedicated team that uses a SIEM for monitoring, analysing, and responding to cybersecurity incidents.

A SIEM (Security Information and Event Management) is a technological solution that collects and analyses security data from various sources, such as firewalls, antivirus software, and log files, to detect potential threats.

Together, a SOC/SIEM solution is like having a high-tech security guard that keeps a watchful eye on your systems and networks. It can spot suspicious activities or signs of an attack, and quickly raise an alarm so that you can take action.

Why do I need it?

All organisations are at risk from threats such as account compromise, phishing scams, and ransomware/malware, as well as threats to supply chain and denial of service attacks. Having a function dedicated to detecting, investigating, and responding to these events is critical to ensure your organisation can minimise the impact of a cyber event.

Why a Managed SOC/SIEM?

Delivering 24/7 security operations requires a dedicated team of security specialists, which can be expensive and hard to resource. Outsourcing to a specialist partner may allow you to achieve the benefits in a more cost-effective manner.

This guide is focused on a Managed SOC/SIEM solution based on Microsoft technologies, because for many organisations this is the most widely used and cost-effective solution. However, a section on alternative solutions is also included.

What you’ll find in this guide

Service overview

An overview of the service, key threats covered, and technology integration components.

Security data sources

Review the technical configuration of Microsoft Sentinel and gain an understanding of data sources, ingestion and retention.

Cost calculator

Use the calculator to estimate the expected monthly costs.

Implementation activity

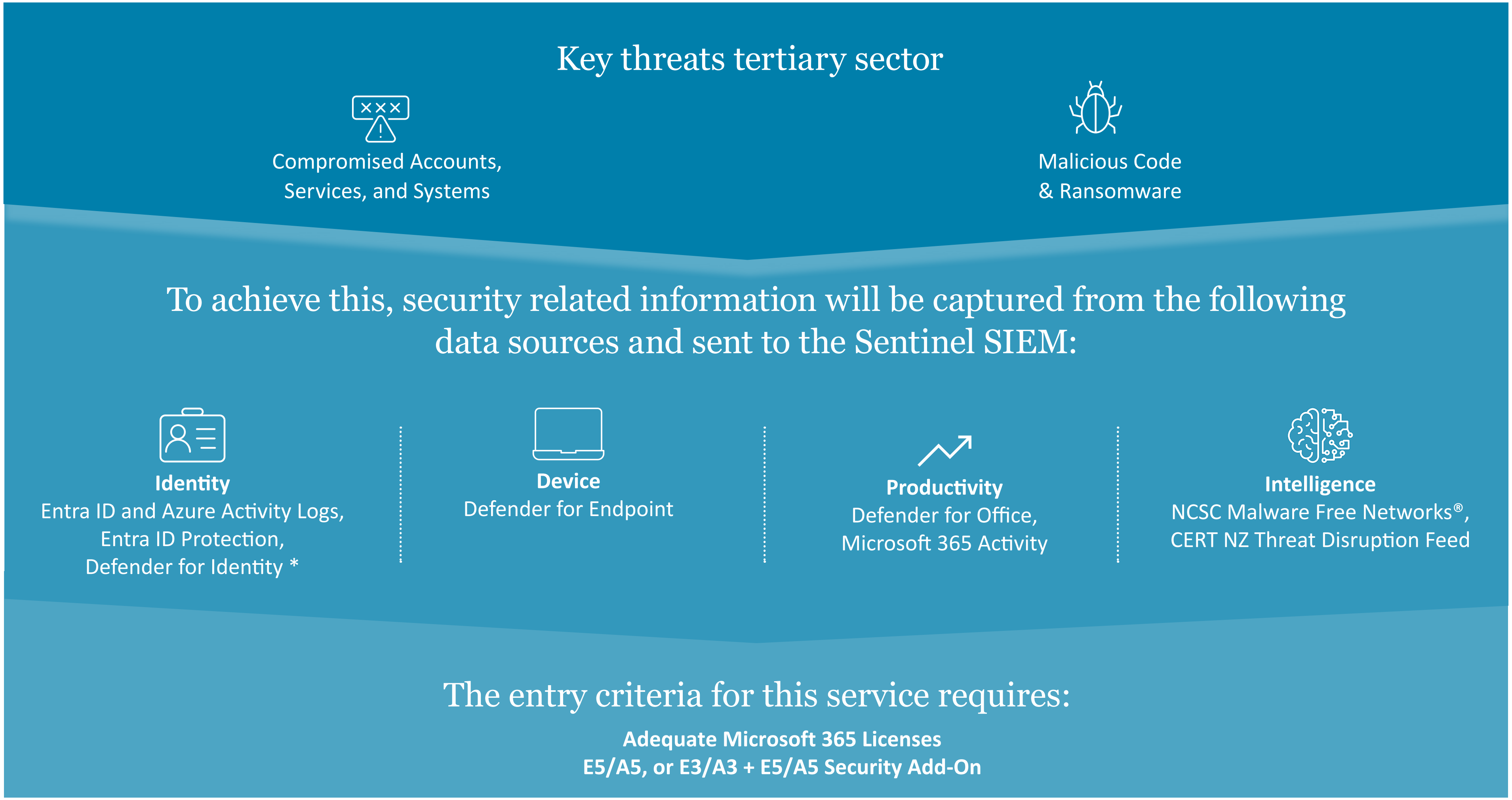
Review the list of capabilities which need to exist or be deployed as part of service onboarding, as well as dependencies or potential effort required by your organisation.

Total Cost of Ownership

Determine the estimated total costs of a Managed SOC/SIEM service.

Managed SOC/SIEM - overview

This service consists of a SIEM (Microsoft Sentinel) and a Managed Security Operations Centre (SOC). By ingesting security related information from identified **data sources** within your environment, the service addresses **key threats** identified from across the sector.



Key threats tertiary sector

Compromised Accounts,
Services, and Systems

Malicious Code
& Ransomware

To achieve this, security related information will be captured from the following data sources and sent to the Sentinel SIEM:

Identity
Entra ID and Azure Activity Logs,
Entra ID Protection,
Defender for Identity *

Device
Defender for Endpoint

Productivity
Defender for Office,
Microsoft 365 Activity

Intelligence
NCSC Malware Free Networks®,
CERT NZ Threat Disruption Feed

The entry criteria for this service requires:

Adequate Microsoft 365 Licenses
E5/A5, or E3/A3 + E5/A5 Security Add-On

*Required for hybrid IT environments (Entra ID & On-Premises Active Directory)

Security data sources

Microsoft Sentinel

We've chosen the following data sources from the Microsoft 365 and Defender XDR services as the most appropriate to provide key security information to address the threats identified to the sector. The information and retention of this data directly impacts the Azure Sentinel consumption costs.

Data Sources

High-Fidelity Alerts

- Entra ID Protection
- Defender for Endpoint
- Defender for Office
- Defender for Identity

General Telemetry

- Azure Activity
- Entra ID
- Microsoft 365

Threat Intelligence

- NCSC MFN®
- CERT NZ PDS

Data Ingestion

Analytic Logs

- Majority of data ingested as 'Analytic Logs'
- Data Collection Rules (DCRs) utilised to filter high-volume telemetry (such as EntraID data)

Basic Logs

- Supplementary Defender for Endpoint logs ingested as 'Basic Logs' to enable cost savings

Data Retention

Interactive

- Ingested data is 'interactive' within Sentinel for first 90 days (analytic-tier retention within Sentinel)

Archive

- Beyond initial 90 days, data is 'archived' for next 9 months (archive-tier retention within Sentinel)

Cost Calculator

Please answer the following questions. Answering these questions will help to calculate the expected managed service cost and Microsoft Azure consumption costs (see the next page for more information on how these costs are calculated).

Cost Factor

1	How many staff are in your organisation?	Small (0–300 staff)	□	Medium (300–800 staff)	□	Large (800–1500 staff)	□
2	How would you describe the complexity of interactions between your IT, Security, and Faculty departments?	Simple	□	Moderate	□	Complex	□
3	What are your governance, change control, and reporting requirements?	Light	□	Moderate	□	Heavy	□
4	How effective are your security controls?	Strong	□	Standard	□	Baseline	□

SIEM cost calculations

The table below explains how your SIEM Azure consumption costs were calculated using the average number of staff within the range that you selected in the cost calculator. These calculations have been validated by Microsoft as of May 2024.

	Small	Medium	Large
	150 Users	550 Users	1,150 Users
Analytic Log Ingest (GB/day)	1	2.5	5
Basic Log Ingest (GB/day)	5	7.5	10
A5 Benefit (zero rated GB/day)	0.75GB /day	2.75GB /day	5.75GB /day
Cost/month	$465	$800	$1,220
Cost/year	$5,580	$9,600	$14,640

- Pricing based on deployment to Australia East region as of May 2024
- Sizing based on analysis of in-scope data connectors, tables and data
- A5 benefit (5MB/day/license zero-rated ingest) assumes that the included benefit will apply to 75% of ingested Analytic Logs
- Analytic log ingest volume based on sending MDE logs to Basic tables
- Basic log ingest volume based on sending MDE logs to Basic tables
- No data restore or search queries/jobs processing included in calculations
- Assumes a single Entra ID tenancy / M365 environment

Implementation Activity

The Managed SOC/SIEM service requires the configurations below. If these configurations are not in place yet, they will be part of the implementation. We've also provided an effort estimate to guide in assessing any internal costs.

Required configurations	Implementation criteria	Implementation costs	Internal effort	Notes
Conditional Access (CA)	CA policies required to enforce: › MFA required for Microsoft Admin Portals › MFA required for risky activity	$20k	Low — Medium	› MFA must be operational prior to CA setup › Deployment of MFA across all users performed by organisation
Defender for Office (MDO)	Minimum configuration requirements: › Balanced actions for malicious and bulk email content › Safe Links and Safe Attachments enabled		Low	
Defender for Endpoint (MDE)	› Defender for Endpoint configured to 'Block Mode'		Low — Medium	› MDE agents deployed to EUC devices by organisation › Deployment state, supported Operating Systems, organisation size & complexity will impact enablement effort
Defender for Identity (MDI)	› Configuration of MDI Cloud Portal		Low — Medium	› Domain controller count will impact enablement effort › Deployment of MDI sensor on Domain Controllers & configuration of logging settings as per Microsoft documentation performed by organisation

Total Cost of Ownership

This page summarises the cost calculations so you can build a view of the overall total cost of ownership for a managed SOC/SIEM service.

Cost components	Cost
Managed service costs (per year)	
SIEM Azure costs (per year)	
Service implementation costs (one-off)	
Total	

Please note, there are some costs for internal implementation activities and support of the SOC/SIEM service (e.g. responding to incidents the managed SOC can't deal with).

Because each organisation is different it's not possible to definitively calculate these costs. However, on the previous page you'll find guidance on implementation activities. Support of the SOC/SIEM service is expected to be minimal (allow around 0.2 FTE).

DISCLAIMER

The costs provided in this model are intended to serve as estimates and should not be considered final or definitive. It's recommended to validate these estimates with the service provider of your choice. Costs presented are based on the pricing of Azure cloud services in the Australia East region as of May 2024.

Future Opportunities

This Managed SOC/SIEM service provides immediate coverage, effectively addressing the primary identified threats such as Compromised Accounts, Services, Systems, and Ransomware/Malware.

You can choose to stay at this level and maintain a steady state of operational security posture without any additional costs.

Or the service can be further extended with investment to cover additional threats, technology platforms or detection use cases. Potential areas of coverage may encompass network devices, cloud-based environments or business applications.

Alternative options - Introduction

Our investigations indicate a managed SOC/SIEM is the most appropriate and cost-effective solution for many organisations. However, for some organisations, an alternative solution may be a better fit.

Alternative option 1

Internal security operations with Microsoft Defender XDR for organisations who don't need the extensive capabilities that a SIEM provides.

Alternative option 2

Internal security operations with Microsoft Sentinel SIEM for organisations where the outsourcing of a SOC/SIEM is not an option.

The next pages will assist you in determining whether any of these alternative solutions would work for your organisation.

Alternative option 1: Internal Security Operations using Microsoft Defender XDR

1

What is it?

Extended Detection & Response (XDR) refers to a unified security platform which addresses threats within differing technology areas for an organisation.

Microsoft Defender XDR, along with Entra ID Protection, is a suite of detection & response capability providing comprehensive coverage across key threat vectors of Identity, Endpoint and Productivity.

The XDR platform needs to be supported by an internal Security Operations team within the organisation who are responsible for detecting, investigating, and responding to cyber events.

Who should consider it?

Organisations comfortable limiting security monitoring to Microsoft Defender XDR data sources, that have up to 30 days log retention and don't need 3rd party integration or automation.

XDR is limited to Microsoft Defender XDR data sources and therefore suits organisations only needing or wanting to include these sources in their monitoring.

Organisations where the outsourcing of a SOC/SIEM is not an option.

This option addresses the key threats to the tertiary sector (Compromised Accounts, Services, and Systems; Malicious Code & Ransomware), and requires licensing for Microsoft M365 E5/A5, or E3/A3 + E5/A5 Security Add-On.

Alternative option 2: Internal Security Operations using Microsoft Sentinel SIEM

2

What is it?

Security Information and Event Management (SIEM) refers to an extensible monitoring system which can ingest and analyse data from various data sources across your organisation.

Microsoft Sentinel is a full featured SIEM which can be used in conjunction with Defender XDR to extend and enhance the security operations capability of an organisation.

The SIEM would need to be supported by an internal Security Operations team within the organisation who are responsible for detecting, investigating, and responding to cyber events.

Who should consider it?

Organisations wanting to have security monitoring sources outside of Microsoft Defender XDR, have greater than 30 days log retention, or want 3rd party integration or automation.

SIEM is extensible and can ingest and analyse data from various data sources and therefore suits organisations with more complex security monitoring requirements.

Organisations where the outsourcing of a SOC/SIEM is not an option.

This option addresses the key threats to the tertiary sector (Compromised Accounts, Services, and Systems; Malicious Code & Ransomware), and requires licensing for Microsoft M365 E5/A5, or E3/A3 + E5/A5 Security Add-On.

Compare alternative options

Internal Security Operations using Microsoft Defender XDR

Data sources

Identity: Entra ID Protection, Defender for Identity.
Device: Defender for Endpoint
Productivity: Defender for Office.

Internal Security Operations Requirements

Capability and capacity to manage your XDR.
Team capacity for detection and response in a timely manner on a 24/7 basis.
Establishment of Standard Operating Procedures (SOPs), collateral and centralised knowledgebase.

Implementation costs

$20k for Security Partner to configure Defender XDR
$x implementation effort internal*
$x establishment of Standard Operating Procedures (SOPs), collateral and centralised knowledgebase*

Ongoing costs

Resourcing: 1-2 FTE additional**
Azure costs: $0

Internal Security Operations using Microsoft Sentinel SIEM

Data sources

Identity: Entra ID and Azure Activity Logs, Entra ID Protection, Defender for Identity.
Device: Defender for Endpoint
Productivity: Defender for Office, Microsoft 365 Activity.

Internal Security Operations Requirements

Capability and capacity to manage your SIEM.
Team capacity for detection and response in a timely manner on a 24/7 basis.
Establishment and maintenance of Standard Operating Procedures (SOPs), collateral and centralised knowledgebase.

Implementation costs

$40k for Security Partner to deploy & configure Microsoft Sentinel & configure Defender XDR
$x implementation effort internal*
$x establishment of Standard Operating Procedures (SOPs), collateral and centralised knowledgebase*

Ongoing costs

Resourcing: 2-3 FTE additional**
Azure costs: $5k - $15k per year depending on organisation size.

*Because each organisation is different, it's not possible to calculate the following costs:

- internal implementation activities (see earlier overview of activities and indication of effort required)
- establishing an internal Security Operations function including artefacts like SOPs, collateral and knowledgebase.

**These alternative options are based on delivering the same outcome as a managed 24/7 solution. The FTE effort estimates need to be applied across several people to support 24/7. If the internal security operations team is not properly resourced and equipped, the implemented XDR or SIEM will have limited added value.

For more information

Visit the TEC website
www.tec.govt.nz/teo/working-with-teos/improving-cyber-security-in-the-tertiary-sector/soc-siem

Or contact DEFEND:

Call	0800 233 336
Email	information@defend.co.nz
Web	defend.co.nz

DEFEND®

Tertiary Education Commission
Te Amorangi Mātauranga Matua