Sentinel SOC Services

Service Definition

June 2022

Gold
Microsoft Partner

Microsoft

Contents

WHO ARE e2e

e2e-assure have been supporting organisations of all sizes with Security Operations Centre (SOC) services and Managed Detection & Response (MDR) for nearly 10 years, with our founders having over 20 years' experience within cyber security, which lead to the creation of e2e-assure. Our customers include some of the most complex and high risk government bodies, down to the smallest scale-up companies and everything in between.

e2e-assure are a Microsoft Gold Partner and have over 70 qualifications across Microsoft technologies, as well as over 70 SANS certifications for broader security expertise. See a full list of our qualifications and accreditations.

Having built out a successful operation within the UK, we expanded into Australia in 2018 and have a thriving Security Operations Centre (SOC) in Canberra, allowing us to improve our diversity of thought and deliver 24/7/365 services in a follow-the-sun model, or with UK or Australian sovereign services, as is required by many of our customers. All UK staff are Security Cleared, and Australian staff hold the equivalent level for Australia.

We work with organisations to improve their cyber security posture over time, building a cyber maturity programme that ensures investments are well planned and focused on having the biggest impact. This allows our customers to use cyber security as a source of competitive advantage, both through enabling business growth and in winning customers by demonstrating that they are not a supply chain risk. In addition to this we often work with our customers and their cyber insurers to prove they are insurable and help lower premium costs.

One of the questions we often ask ourselves as a business is “how can we hope to deal with the complex problems in cyber security, without diversity in our ways of thinking”? We always aim to actively build a diverse team and have a particular focus on neurodiversity, with our ‘e2e-engage’ team. Find out more about the team and read about the tangible business benefits we have seen from taking this approach.

INTRODUCTION

Microsoft Sentinel is a richly featured cloud-based Security Information & Event Management (SIEM) and Security Orchestration, Automation & Response (SOAR) tool. Sentinel assists Security Analysts in protecting an organisation from cyber threats through a range of functionality.

Some of the key reasons organisations are moving to Microsoft Sentinel include:

- **Coverage across diverse technologies through existing connectors** – The Sentinel portal contains connectors for the majority of security technologies in the market today.
- **Maximise access to talent pool** – As Sentinel becomes more prevalent, then the skills base is widening to enable recruitment of qualified staff.
- **Retain SIEM and internal knowledge** – by using Sentinel, an organisation can retain the data and knowledge in-house, whilst still having flexibility to move external partners.
- **Benefit from leading automation tools** – Sentinel has advanced SOAR capabilities that allow organisations to reduce manual work and thus free up human time.
- **Access to Microsoft Threat Intelligence** – Microsoft's extensive threat intelligence can be utilised in Sentinel to bolster and update proactive threat hunting or building playbooks.

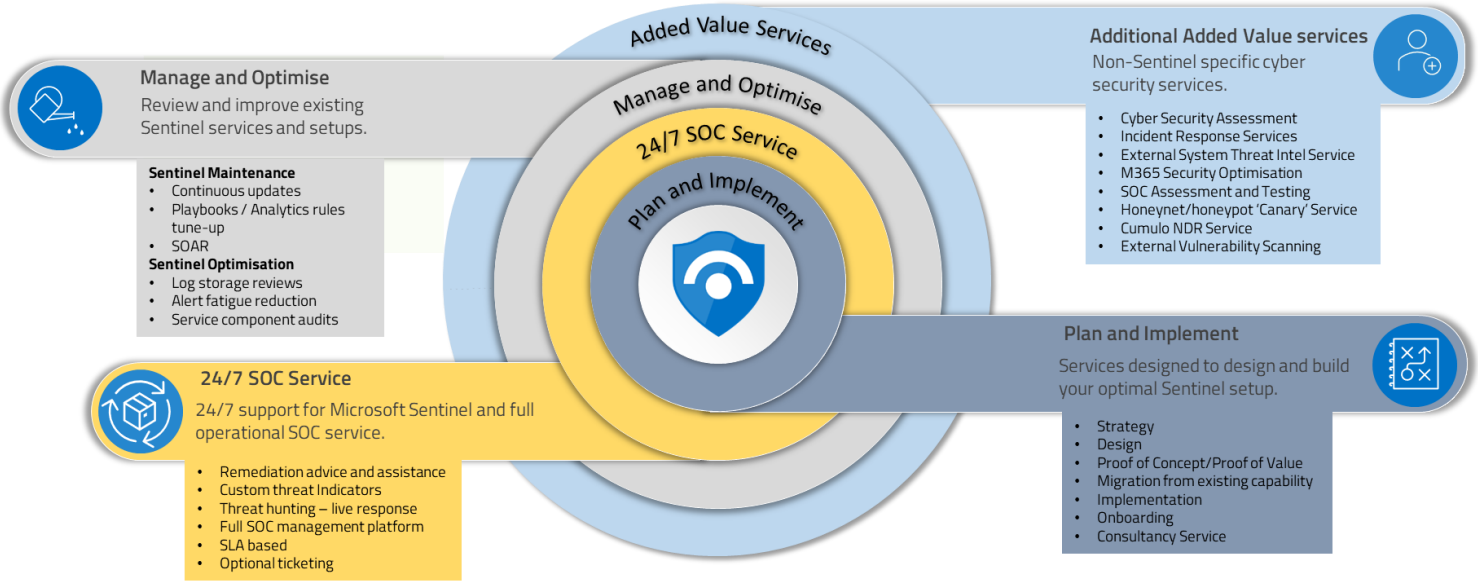
As with any piece of security technology the efficacy of Sentinel is also determined by the supporting technology, processes and people enabling its use.

Some of the key issues in getting the best out of Sentinel include:

- **SOC and Service Management** – Whilst Microsoft Sentinel comes with many benefits, it does not include fully featured SOC management platform.
- **Having enough skilled internal staff** – this is a challenge with all security technology not just Sentinel, and although Microsoft Sentinel skills are becoming more widespread, they are still scarce and expensive.
- **24/7/365 coverage** – Cyber-attacks can happen at any hour, day or night and often at the most unsociable hours. 24/7 coverage is essential and dramatically increases the number of staff required for monitoring if undertaken internally.
- **Alert overload** – By the very nature of Sentinel being open to ingest logs from diverse sources, it can create a challenge in having potentially too many alerts to deal with – alert fatigue. It takes time to triage alerts into incidents, so tuning is essential and requires extensive knowledge, preferably of multiple environments.
- **Complex and potentially costly in hybrid environments** – many organisations exist as 'hybrid' environments and given the nature of how Sentinel ingests logs this can become expensive if not managed pro-actively.
- **Limited data sources outside of logs** – Sentinel has limited integrations into network traffic analysis, network analytics tools and Intrusion Detection Systems, potentially limiting the context available for analysts to make informed decisions.

The e2e Sentinel SOC service is the key constituent in our range of services available for organisations either using Sentinel today or looking to utilise Sentinel going forward. The scope of the service covered in this document includes Plan and Implement, Sentinel SOC Service and Manage and Optimise, as outlined in the diagram below. Further services are available as required.

Sentinel Services Portfolio



Sentinel SOC Service

At e2e we break down our range of services for Sentinel into three main categories; Implementation, On-going services and additional value add services. In this document we do not cover the value-add services but focus on implementation and on-going services.

Implementation

Strategy

As a first stage in any engagement with a client e2e need to understand the strategy behind the use and adoption of any chosen security technologies. Dependent upon the client's existing level of cyber maturity, e2e can offer services to guide the client in developing a strategy suitable for their business, requirements and budget. The possible range of engagement is wide, from clients asking us to help set a new strategy through to those clients who are very comfortable with their strategy and require no input from us. In the latter case then this stage is merely an information gathering exercise.

For the last decade e2e has been working with organisations with widely varying requirements, size and market vertical. Along with a core staff with 20+ years cyber security experience, e2e can guide and assist clients in implementing the correct strategy for them. No two engagements are alike.

Assessment

Once e2e have a clear understanding of the strategy driving the use or implementation of Sentinel then we need to investigate the actual usage of the chosen security technologies. Given the nature of Sentinel, with unlimited capacity to accept feeds, this is potentially a complex undertaking and may require considerable input from the client.

Once the environment is fully understood e2e can map the best practices into Sentinel and include any suggested improvements to make best use of existing technologies and licenses. If required, this information can be mapped to the MITRE ATT&CK threat model used by Sentinel. This can also help identify any possible gaps in protection as well as highlight particular attack vectors for specific clients.

Design

As part of designing a specific environment for each client we look to Microsoft, industry and e2e best practice. This ensures each client gets what they need to address their unique environment. As part of the design we will look at the most appropriate log flows and storage, ensuring client policy is upheld whilst managing Azure costs. If there are unusual log requirements, or a need to reduce Azure costs, then the e2e proprietary Cumulo Appliance can be deployed (virtually in a cloud or on-prem), which as well as having native NDR capability, can be purposed to hold, minimise, compress, re-direct or re-image various logs. As all Cumulo technology is developed in-house, e2e have a unique capability to code the platform or appliance to suit a customer's requirements.

Once an overall design and architecture are agreed with the client then the project team will build up an agreed plan for the enablement of a fully live environment. Specialists will be scheduled alongside any necessary client resources to facilitate the final configuration of the deployment.

Enablement

After the final plan is signed off then it's time to get going. At this stage various specialist will carry out the work necessary to get the Sentinel implementation live to the agreed specification. Every implementation is unique but typical areas covered are:

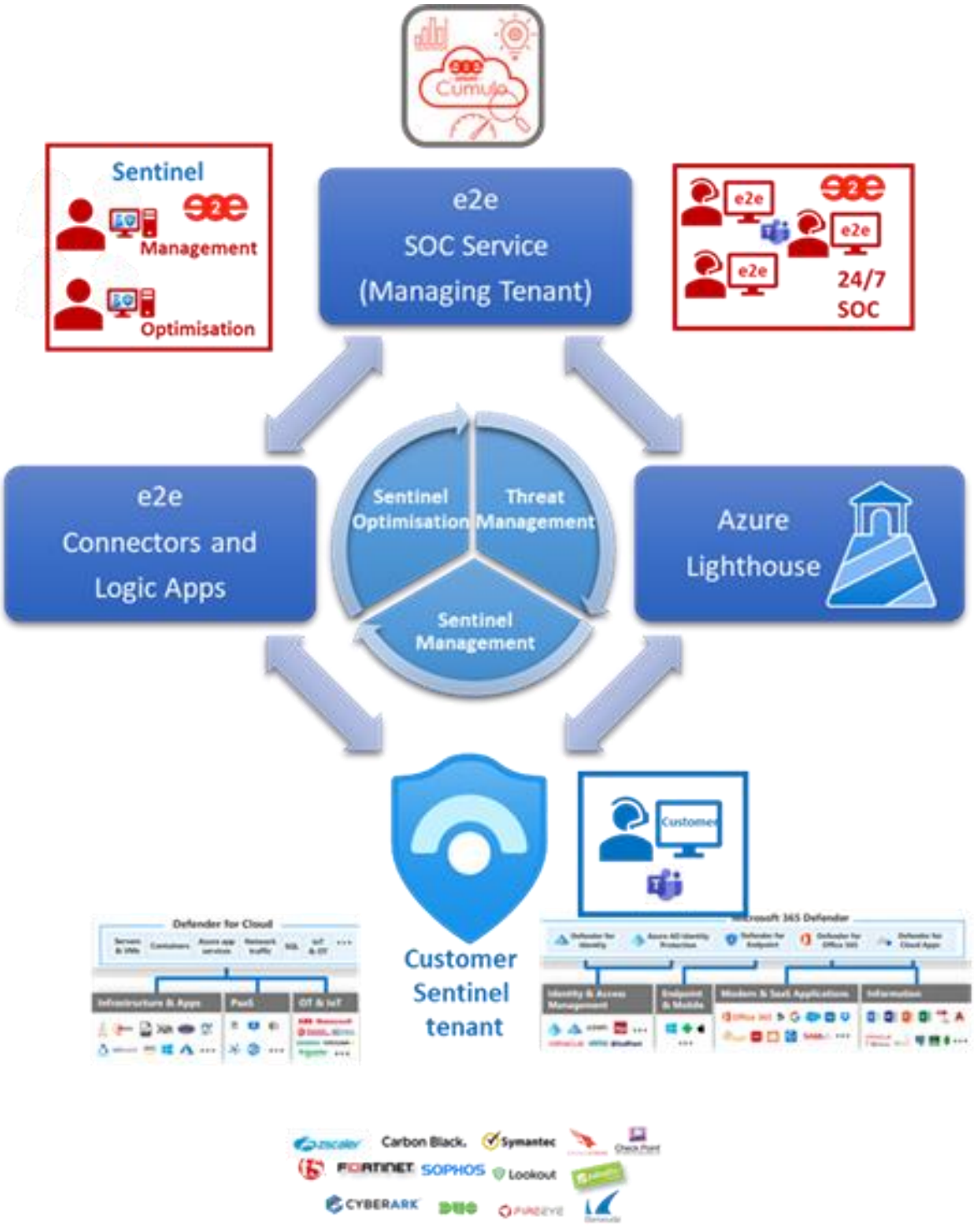
- Deployment of new Sentinel instance and Log Analytics (if required)
- Connection to e2e Lighthouse for management purposes
- Connection and testing of log connectors
- Custom log connectors built, tested and deployed
- Testing of native Microsoft connections, e.g. Defender services, M365, Azure
- Connect and test and multi-cloud environments (AWS, GCP or Oracle)
- Existing use cases and playbooks tested and updated as necessary
- Custom use cases and playbooks created and deployed as required
- Design, testing and implementation of any SOAR rules agreed with client
- Implementation and agreement of best practices
- RBAC deployed as agreed with client
- Configuration of log retention/management in Azure
- Deployment and configuration of Cumulo Appliance (NDR and/or log management) if required
- Connecting of Microsoft, e2e and any further customer supplied threat indicator feeds

Once both the client and e2e are happy with the Sentinel environment then it can be commissioned into the on-going services. Depending upon complexity this can take between 4 and 12 weeks, although commissioning into the on-going services can be completed before final sign off on the Sentinel environment if required. It is also possible to complete the Sentinel commission whilst continuing to use any exiting technology/services.

Enablement is carried out by a dedicated team whose sole focus is the commissioning of clients into the SOC service. Thus they have a broad range of skills, not just covering Sentinel and Cumulo but both the wider Microsoft security suite and 3rd party technology, such as Palo Alto, Cisco etc.

Architecture

e2e have a standard architecture which enables not just the monitoring of Sentinel but also its management and optimisation. Sentinel can ingest logs from an almost limitless number of sources, including all the Microsoft security solutions. e2e utilise both Azure Lighthouse and custom-built connectors, alongside Logic Apps to fully sync and manage the customer Sentinel instance. This enables both the e2e analysts and customer to leverage the Cumulo platform should they wish to. As part of the build the e2e Teams app is deployed into the customer environment to enable incident management, dashboarding and collaboration in the fully secure Microsoft environment. This enables high level management of the full SOC service without recourse to the Sentinel portal.



On-going Services

SOC Service

The SOC service is the core of everything we do and have been doing at e2e for the last 10 years. To this end we have developed our own, unique, SOC management platform, Cumulo. This provides us both with a breadth of capabilities unavailable to service providers simply using "of the shelf" products and the ability to custom develop capabilities as the need arises.

Monitoring

The Sentinel implementation is monitored 24/7 by experienced, Security Cleared analysts operating out of multiple UK based datacentres delivered with either 99.9% or 99.99% availability dependent upon requirements and budget.

The primary purpose of monitoring is to identify potential threats before they become issues and prevent them from escalating further. Sentinel AI, ML and UEBA provide most of the initial, automated investigation and remediation process, whilst e2e ML and human analysts triage and threat hunt, supported by Threat Indicator connectors like TAXII. This provides additional data to identify which threats are priorities, creating incidents which can then be managed through a ticketing system. The triage function will determine, via Sentinel/e2e playbooks, which priority the incident receives. The incident is then responded to within the relevant SLA or dropped if it is a false positive. In certain agreed circumstances automation will kick in via Sentinel SOAR rules, such as isolating a device if it has been compromised.

e2e has the capability of utilising its own Cumulo based ticketing or integration with the clients own ticketing solution, such as ServiceNow.

As part of the monitoring service the client's security posture is constantly reviewed and any areas requiring improvement will be flagged to the client with, where possible, suggested improvements. If required, e2e consultants can be retained to assist in any improvement works.

Incident Response and Remediation Assistance

Once an incident has been identified and given a priority it enters our incident response process. This can trigger multiple activities including the possible invocation of a SOAR rule (where client has agreed they want a human trigger before further automation) but will generally result in e2e contacting the client through the agreed process/medium. Typically, this will be via the dedicated Microsoft Teams app or chat, but can include email (encryption must be enabled), SMS or through ticketing automation.

Most incidents will result in the use of an e2e built playbook, deployed into Sentinel, which the analyst will work to whilst engaging with the client. This engagement will look to contain or remediate the incident and the analyst will work alongside the client until either outcome is reached. Containment is the usual first step to prevent issues expanding to other areas of the client's infrastructure. Once an issue is contained then we can look to assist in remediation, although the timeline for remediation is entirely dependent upon the identified issue. As part of the e2e playbooks, containment or remediation steps will be shared with the client and where enabled we will assist in deploying such measures. We very much see our role as being a pro-active part of the client's response team and will work closely with them, or any 3rd party, until such time as the issue is resolved.

Tickets are only closed once the client is happy that the issue has been dealt with.

Service Management

The Cumulo platform was developed from the beginning as a fully featured SOC platform, consequently it provides for full-service management including process flow ticketing, SLA management, service requests, analyst workflow tools and customer management. This enables a much richer data feed for customer dashboards, surfacing not just the security data but all of the service data too. It also enables e2e to ensure the most efficient customer management across all of our customers whilst enabling immediate best practice sharing.

An integral part of the offering is regular reviews of the service itself and of the client's security posture. This is usually undertaken on a monthly basis, however some clients also choose to have, shorter, weekly reviews as well. The overall health of our customer relationship is owned and managed by an account manager whose task is to ensure a customer is completely satisfied with the e2e service. This includes running the monthly updates and ensuring all the necessary people are present. Dependent upon any issues to be discussed this would normally include account manager themselves, a lead analyst from the SOC, a consultant and any necessary subject matter experts. Escalation processes are clearly defined and in place to ensure both internal and customer resource can raise any issues they believe need attention.

Sentinel Management

At first glance the basic management of a Sentinel instance appears to be relatively un-demanding given its cloud nature, but as the threat environment constantly changes and Microsoft are always improving the platform, then there is a considerable amount of housekeeping to attend to. These tasks include, but are not limited to, deploying new and updating existing analytic rules, reviewing data connectors and logs flow, ensuring log storage is optimised, ensuring workbooks and playbooks continue to work as expected and looking to leverage any new or upgraded features.

The on-going optimisation of logs is a key factor in controlling Azure spend on storage. Ensuring the multiple types of storage available within Azure are deployed in the optimum mix for ingestion, storage and retention is an on-going process which can change over time. The e2e platform, Cumulo, can also be utilised, alongside the Microsoft toolset, to ensure log management is optimised from a security and cost perspective. e2e functionality extends across:

- detailed experience of most log formats, ensuring log output from devices and applications is optimised at source for security purposes
- passing logs through Cumulo to strip and re-direct, if required, non-security data from the log
- the opportunity to off-Azure logs for long term retention if required
- the ability to deploy TAPs (Test Access Points) to multi-stream logs/data as required
- developing and deploying custom connectors for optimised security logging

Given that SOAR is implemented within Sentinel then this is a key feature which needs to be maintained. Changes in client workflow or infrastructure could impact on SOAR rules which would need updating as required. Post enablement, any new SOAR rules would need to be built/updated/agreed between the client and e2e and depending upon the final scope of any agreement, may or may not be chargeable.

On an annual basis e2e will facilitate an extended review session to also look, in detail, at the Sentinel implementation and to determine if this is still appropriate for the client and delivering as expected. This will cover areas including, further/better use of any Microsoft Licenses for security, audit and review: user access, log analytics workspace, log sources and storage, existing playbooks and workbooks.

Sentinel Optimisation

At all times e2e look to optimise the Sentinel implementation for two main reasons; it reduces the likelihood of incidents escalating (client risk) and it enables analysts to focus on the most important areas, including pro-active threat hunting.

One of the key advantages of Sentinel is automation, thus e2e look to leverage connectors, analytic rules and playbooks from multiple sources including Microsoft, the client (usually via private GitHub), the Sentinel community GitHub and of course our own e2e developed playbooks (also deployed from private GitHub). This can dramatically reduce the time to respond by pushing any necessary human interaction further down the workflow. It is potentially possible, given the right technology stack, to fully automate remediation in given scenarios.

Generally, in a SOC environment, the more logs, the lower the incidents, due to better correlation. To that end, as clients bring on new, relevant log sources, e2e would prefer they are connected to Sentinel. Most new log sources would be connected as part of the standard service where there is a pre-existing connector. If development work to build a proprietary connector is required, then that may generate a charge.

SLAs

SLAs are measured either from when Sentinel, via native processes, playbooks or direct analyst intervention (threat hunting etc.), surfaces an incident and when the SOC team notify the client through the agreed channel(s), or by the completion of agreed SOAR processes.

Sentinel SOC Service	Target
Service Availability	99.9% or 99.99%
Service Hours (Alerting and Response)	24/7
Security Incident - First Response (High)	**30 minutes**
Security Incident - First Response (Medium)	**60 minutes**
Security Incident - First Response (Low)	**90 minutes**
Security Incident - First Response (Informational)	**8 hours**
Service Hours for Service Requests	8am to 6pm Mon-Fri

CONTACT DETAILS

Please contact us for more information and a demo at info@e2e-assure.com