



Sales Enablement Pack   
Cyber Security Operations Centre

The first line of defence

# Cyber Security Operations Centre (CSOC) - Sales Enablement Pack

### The first line of defence

# The threat landscape is continually changing, with businesses becoming more exposed to new threats daily. This puts extra pressure on IT departments that may struggle to efficiently allocate their resources without an internal SOC team.

# You can benefit from our CSOC Service that utilises continuous threat intelligence and AI to proactively provide real-time security monitoring and alarming services to reduce risk and increase a company’s IT resilience, all managed by experienced security experts.

# Why is CSOC Important

* Around 39% of businesses reported having a cyber security breach or attack during 2022.
* Around 52% of business leaders say that they don’t know what to do in the event of a cyber security attack.
* The average cost a UK business suffered due to cyber attacks was £4,180 for smaller businesses, and between £9,270 and £22,700 for larger businesses in 2022.
* The CSOC Market revenue is estimated to reach $61,199.7 million by the year 2025.
* 30% of businesses reported an increase in cyber attacks during the Covid-19 Pandemic, with 35% of these requiring an incident response.
* Cyber Security insurers have dramatically increased their prices especially for those businesses not actively working to increase their cyber security defences.

# Challenges

* Businesses are struggling to keep up with the continuous and complicated threats that are being created.
* IT departments are not able to efficiently allocate resources towards cyber security.
* Needing a managed service to look after their infrastructure security as it can be complex and expensive to maintain an internal SOC team.
* Companies spending time, resource and investments looking for ways and insights to strengthen their security systems that tailor to their requirements.
* Businesses requiring additional capabilities such as endpoint detection and response features.
* The need for additional security visibility of their cloud assets.

# 

# Why Expo-e for CSOC

* Expo-e offers a fully managed CSOC solution, using AI and Threat Intelligence to provide real time security monitoring and alerting.
* Our solution runs off the platform and software from market leading vendor AlienVault now part of the AT&T group.
* Our service detects and reacts to threats in order to provide protection to your customers’ assets.
* We can offer a fully bespoke service tailored for the business needs and requirements.
* Our CSOC Solution uses a Unified Security Management (USM) Platform to create a full view of events across your customer’s network, highlighting areas that may benefit from improvement all within a single pane of glass.
* Through the USM platform we provide availability monitoring so if any monitored device goes down or is flapping, we will detect, notify, and act upon this for you and your customers.
* Our systems are also integrated with an Advanced Persistent Threat Database, which contains a full list of known vulnerabilities which is continuously updated by all users of the system.
* We have two different options for CSOC Services:
  + CSOC Lite – CSOC Service for Firewalls
  + CSOC USM Anywhere – SaaS based solution (default and best in most scenarios)
    - Essentials
    - Standard
    - Premium

**CSOC Lite**

* CSOC Lite is a cost effective entry point CSOS Solution, focused on monitoring security devices.
* It is a service that collects security logs generated from your customer’s firewall environment to give an overall insight into their security estate.
* Prioritisation of events is set with your customer prior to deployment and part of the ongoing service events that are reviewed at the agreed frequency.
* Your customer will have a full 24/7 monitoring solution, managed by a team of analysts that will notify them within a 60-minute SLA about any security events produced/seen by the customer firewalls.
* You and/or your customer can be given access to a read-only portal to the SIEM.
* Reports can be extracted from the platform in order to visualise statistical data about any captured event or alarm triggered by the SIEM solution.
* CSOC Lite can cover up to 3 active and 3 passive firewalls, if there are any requirements for more than 6 firewalls or servers, then the full CSOC Service is needed.

**CSOC USM Anywhere**

* Our CSOC USM Anywhere is the default CSOC option that will be used in most use cases.
* Our USM Anywhere Service is a fully managed end-to-end solution that enables centralised security monitoring of networks and devices in the cloud, on premise and in remote locations.
* It allows us to deliver powerful threat detection and incident response through the use of a single Unified Security Management (USM) platform.
* USM Anywhere SaaS based delivery model provides advantage for reducing deployment, infrastructure and operating costs.
* USM Anywhere price is based on storage, with data logs being stored in a Secure Cloud which is encrypted and transferred over a secure connection.
  + - As standard we offer 3 levels of USM Anywhere:
      * **Essentials** – 15 days of real-time event search, with simple fortnightly reports.
      * **Standard** – 30 days of real time event search, with monthly reports including trend analysis.
      * **Premium** - 90 days of real time event search, with monthly reports including trend analysis.

# List of reasons 'Why USM Anywhere'Why USM Anywhere

\*This needs to be slightly reworded to say ‘your’ customers

# Features & Benefits

**Automated Response Orchestration** – providing advanced security orchestration rules that will allow for the automation of actions and responses with direct integration with widely used Security tools such as Cisco Umbrella and Palo Alto Networks. This allows your customers to utilise their existing security investments without spending time and money on integrating systems and writing scripts to allow for automation.

**Centralised Security Monitoring** – Through USM Anywhere, we can ensure that both your customer’s Cloud and on-premise landscape are monitored. This ensures that your customers will not have any security blind spots.

**Cloud Native Build** – USM Anywhere utilises a unique security element of public cloud infrastructure, with the ability to API with many SaaS applications. This allows for greater control over the security of both the Cloud Infrastructure and SaaS application.

**Cost Savings** – Companies can have a lower TCO when investing in Expo-e’s CSOC USM Anywhere, as there is no CapEx spending on hardware. As USM Anywhere is a SaaS-based platform, upgrades and ongoing hardware maintenance are completed automatically. All of this saves valuable time and resource for your customer’s internal IT teams.

**Elastic, Cloud-Based Solution** – Allows your customers to scale the solution with their IT environment changes and grow without the need for setting up new hardware, eliminating the downtime for setup.

**Endpoint Detection & Response** – CSOC USM Anywhere extends threat detection and response to the endpoint. This provides crucial visibility into attacks that might not trigger traditional prevention rules while eliminating the cost and complexity of adding yet another endpoint solution.

**Resiliency** – The solution takes advantage of a highly resilient, secure cloud infrastructure which is fault-tolerant. This gives you and your customers peace of mind, as risks associated with hardware failure, power outages and human error are mitigated.

**Security Analytics** – The platform allows for custom search and views, to provide compliance-ready reporting and analysis, to investigate incidents easily.

**Single SaaS Platform** – Within a single pane of glass, you and/or your customers are able to view all of their security posture information within a single console without the need for multiple logins.

**Virtually Seamless Updates** – Your customers can also be assured that they have the most up to date software at all times, as there is no need to manually download and install updates, which will include the delivery of new features and functionality to address the ever-evolving threat cycles. Your customers can be guaranteed that they have the most effective security monitoring in place.

# AlienApps

Our Service offers a highly extensible platform that enables our CSOC team to deliver AlienApps (modular software components), that extends the USM’s threat detection and security orchestration capabilities to other IT and security applications. This means we can provide your customers with an end-to-end security monitoring and response service while seamlessly integrating with new applications as and when they become available on AlienApps.



# Features Matrix

# A screenshot of a computer Description automatically generated

*\*Hopefully we have a version of this that can be read as the font on this is so small.*

# Discovery questions to ask your customer

* Has your company adopted a working from home policy or other changes due to the current pandemic?
* Does your company have a cloud migration strategy in place and what are the time frames?
* Are you currently getting security visibility of your endpoints through other mechanisms?
* When was the last time you were audited or had a professional security professional assessment?
* How are you looking to enhance your infrastructure?
* What specific Compliance requirements do you need to adhere to?

# Qualification questions to ask your customer

* How many devices do your organisation use, and how many of them are windows servers, laptops, firewalls etc?
* Do you need to monitor endpoints outside of the network or in remote locations?
* Would you like the ability to query devices for additional forensic data as part of your investigation activities?
* Would you like our partner Expo-e, to actively monitor endpoints which will include active process and network activity?