CYBERSEER
THE VISION TO PROTECT

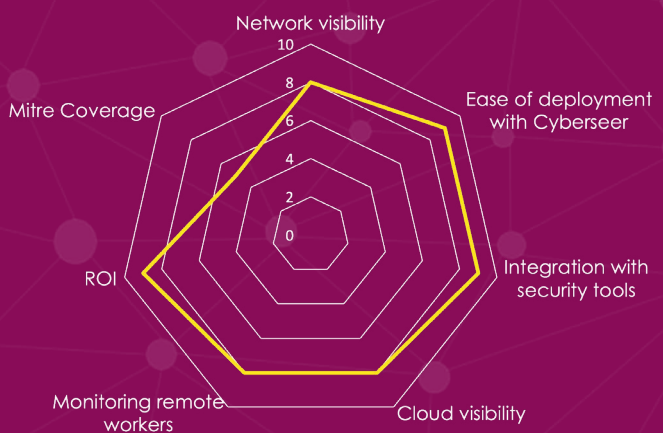
DARKTRACE

Cyberseer SOC & Darktrace

Solution brief

Discover how Darktrace combined with Cyberseer's SOC overcome resource issues by delivering a true AI service across all environments whether Datacentre, Cloud, or SaaS.

Darktrace at a glance:



Approximate read time: 6 min

THE VISION TO PROTECT

Executive Summary & Key Benefits

- Machine learning technology models your unique environment
- 24/7 SOC service
- Actionable intelligence from Tier 3 Forensic Analysts
- Reduced dwell time
- Increase detection efficiencies
- 24x7 threat detection
- Threat hunting
- Actionable intelligence from network and cloud sensors
- Eliminate noise and prioritise threats

Cyberseer has partnered with Darktrace to deliver true AI across all environments, whether Datacentre, Cloud or SaaS. Cyberseer will continually monitor your deployment, making you aware of the critical threats. All triage and prioritisation are done by Cyberseer's expert Analysts.

The Challenge

Today's businesses are undergoing monumental changes. Digital transformation projects and the move to the cloud are all having an overwhelming impact on security.

Operations teams are trying to maintain stability whilst developers and the business require regular changes. The security teams are constantly working to try and secure these environments. With the fast pace of development, security teams just cannot keep up. How do you detect threats in the cloud, if you have no visibility into cloud and SaaS environments?

Typically SOC's are the key to securing your environment but with the average large enterprise deploying security products from 70+ different vendors, the enormous number of alerts generated per day means that the SOC team are continually overwhelmed by the sheer volume. Identifying actual threats against the noise is a major challenge as "analysts are spending 30 minutes on average to investigate each event and only about 1 in 5 alerts are related to a unique security event"*. The SOC therefore struggle to pinpoint the critical incidents versus the noise and a significant number of alerts are ignored due to the sheer volume.

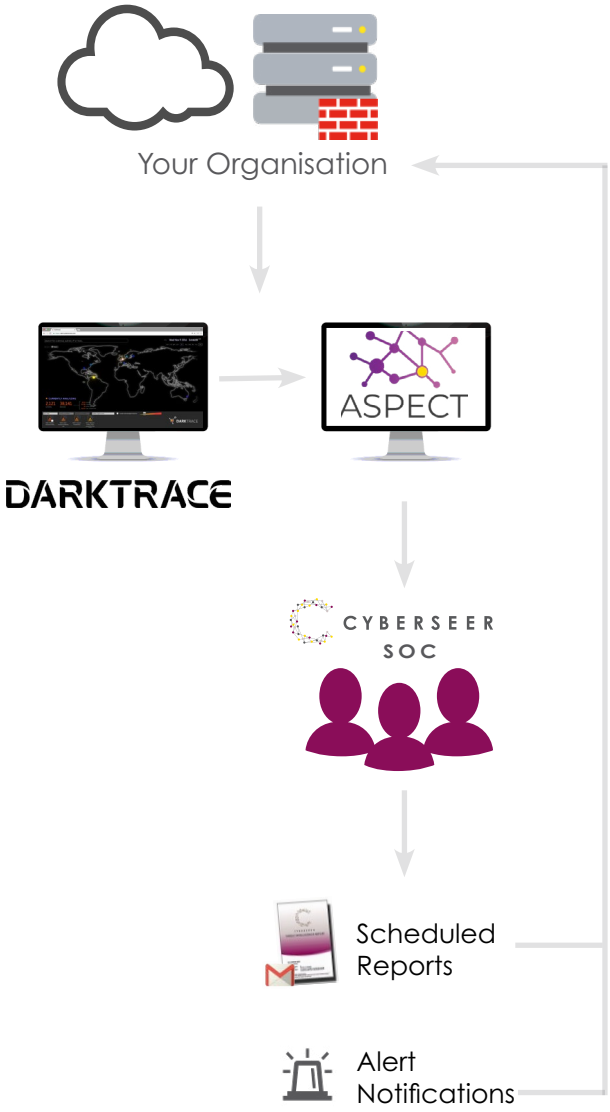
Organisations migrating to new services, whether IaaS, PaaS or SaaS only increase the attack surface, creating further alerts. This combined with the number of attackers increasingly making use of AI, means that detecting legitimate threats is critical to the security of the organisation. The SOC needs to have effective tools.

The Solution

Organisations that deploy Darktrace benefit from Enterprise-wide protection. Darktrace like the human immune system detects what is normal for your enterprise, rather than applying what it thinks should be normal based on other similar companies and predefined rules. Darktrace learns what is 'self' by ingesting network traffic from sensors across your environments which allows it to detect subtle changes that could be indicative of a threat.

ASPECT from Cyberseer - is at the core of the Cyberseer SOC. It is a proprietary, 24x7, distributed platform that integrates with Darktrace via API to pull alerts for enrichment, prioritisation and escalation to our Forensic Analysts. The automation of these repetitive and time-consuming processes, along with the enrichment of alerts with internal and external contextual threat data, enables us to do more with less by efficiently and effectively identifying and routing priority threats to Analysts, which in turn reduces the time to respond minimising threat dwell time.

Darktrace learns by procesing raw network data to build up a pattern of life for all users, devices and the network in the environment, whether that be in your data center, branch office, cloud or SaaS. Having a unified view of your entire digital estate allows for threats to be tackled quickly. Darktrace autonomous response technology Antigena can inoculate both e-mail and network-based attacks, ensuring malicious e-mails or malware on machines are stopped in real-time. This allows for compromised hosts to immediately resume normal functionality without being taken offline. At a later date the device can be scheduled into a maintenance window for reimaging.



All Cyberseer SOC Analysts are Tier 3 people who are trained to comprehensively threat hunt, triage and investigate prioritised activity.

Cyberseer Analysts work as an extension of your security team and build up a good understanding of your environment and organisation. This style of working relationship is key as it provides further context for the Analysts to understand the impact of a threat in your environment. Also, when you are contacted out-of-hours you will not need to bring the Analyst up-to-speed on your environment which further reduces your overall response time.

Cyberseer Analysts perform an initial triage process to classify an incident, before alerting the customer using pre-defined communications channels and escalation contacts. The Analyst will walk the customer through their current understanding of the incident and classification that has been assigned, and then support the customer with their response efforts and investigate the activity further.

Cyberseer provides all customers with three types of reports:

1. Priority incident reports detailing escalated priority threats
2. Weekly reports detailing all threat tickets raised during the week
3. Monthly trend reports detailing the number of incidents, threat classifications, breaches by attack phase, total threats and risk scores.

Benefits

- **24/7 Priority Threat Detection.**
  Outsourcing this process is an economic answer to resource issues.

- **Reduce Time-to-Detection.**
  Cyberseer find important signals in large data sets and quickly prioritise alerts, reducing your business risk.

- **Improve Your Team's Productivity.**
  We reduce alert fatigue and take all the heavy lifting out of threat detection.

- **Speed up Threat Hunting.**
  Using Cyberseer Forensic Analysts to interrogate customer data sets for subtle and sophisticated signals.

About Darktrace

Founded in 2013 by mathematicians from the University of Cambridge, Darktrace was the first company to develop an AI system for cyber security.Darktrace founders also include cyber security experts from government intelligence backgrounds, united in their mission to fundamentally transform the ability of organisations to defend their most critical assets in the face of rising cyber-threat.

Darktrace's pioneering technology, the Enterprise Immune System, applies AI to the cyber defence challenge for the first time, detecting cyber-threats that existing, legacy systems cannot.

It quickly became clear that the technology was powerful enough to identify a diverse range of threats at their earliest stages – including insider attacks, latent vulnerabilities, cloud-based threats and even state-sponsored espionage.

DARKTRACE

About Cyberseer

Keeping your business safe is your number one priority. It's ours too. Fusing advanced detection technologies with deep forensic expertise, we help you join all the dots to rapidly distil threats. Our innovative solutions give you the confidence and proactive control you need – whatever comes your way.

We're here to help you keep your people and your reputation safe 24x7. It's what we do for companies around the world every day.

With Cyberseer, you're no longer on your own.

If you would like to know more about our Managed Security Service or the advanced technologies that we use, then please get in touch.

CYBERSEER

CONTACT US +44 (0)203 823 9030
info@cyberseer.net

Source: https://bricata.com/blog/how-many-daily-cybersecurity-alerts/

axi ADDISON LEE MARKERSTUDY LIMITED TRADEX INSURANCE SERVICES ganado advocates MIZUHO Knight Frank