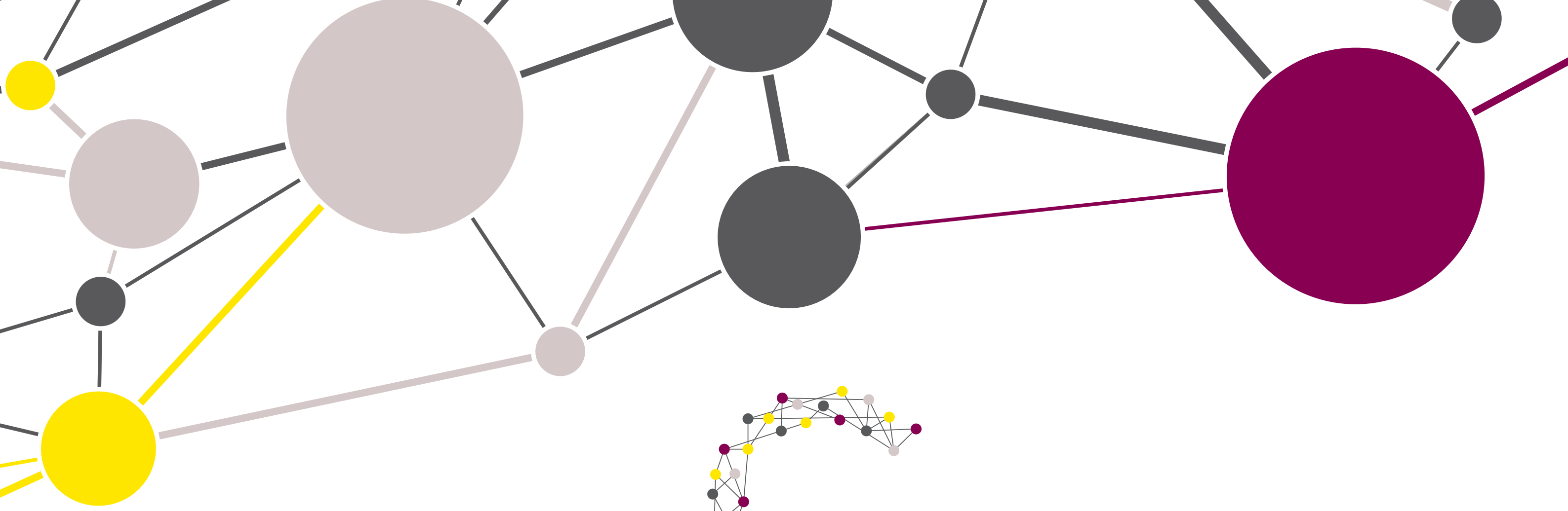

CYBERSEER

SMARTER CYBER SECURITY WITH INTELLIGENCE DRIVEN SOC

THE VISION TO PROTECT

WHITE PAPER

INSIDE THIS WHITE PAPER:

This document looks at the changing threat landscape, cyber criminal motivations and challenges for enterprises traditional security monitoring and detecting devices. The paper introduces a new category of managed detection and response for advanced threat detection that uses machine learning combined with human analytics as a recursive lifecycle approach across four key areas of defence: Prevention, Detection, Response and Prediction to maintain effective mitigation of both current and emerging cyber threats.

THE CURRENT THREAT LANDSCAPE

Threats to all organizations in today’s world have developed exponentially over the last 5 – 10 years. It seems like every day a new organisation is sadly making headlines due to becoming the latest victim of a cyber compromise. Attacks vary in their approach and ultimate target. Some attacks seek to steal Intellectual property or corruption a company’s data; others to deliberately cause disruption. All in all, the ultimate consequence for the victim organisation who’ve suffered a damaging cyber breach is a loss in brand value, dramatic reduction in share price and, under regulations such as General Data Protection Regulation (GDPR); a significant fine. Cyber breaches, or at least notification of breaches is becoming more common place within our weekly media headlines. Some say that the rate of compromise hasn’t increased greatly but the obligation to report it has. GDPR Article 33 mandates that an organisation will provide a notification of a personal data breach within 72 hours of becoming aware of it.

Cyber threats typically fall into a handful of threat categories including Phishing, Malware, DDoS and Insider Threat. In addition to this there are many types of threat actor whom utilise these techniques, amongst others and target organisations. These include Hacktivists, Organised Crime groups, state sponsored as well as malicious insiders. If you take a look at many of the recent cyber-related breaches that have made headline news; one or many of the above threat types are sighted as the method utilised to carry out the initial compromise of the targeted systems and the reasoning is either political, ideological or criminal. The main objective for all of these threat actors is to gain access to the target system using credentials. Valid Credentials are key to over 90% of successful compromises reported in recent years. Once obtained through theft, insider or other means; valid credentials allow you to hide in plain sight within the target environment and masquerade as a genuine user.

This makes it challenging for traditional security enforcing devices and monitoring tools to detect as all the attacker’s activity is being reported to the system as a valid user. This approach is supported by evidence in the Mandiant M-Trends report. The report states that the average number of days from compromise to detection in 2017 globally was 101 days. Focusing on EMEA only, this increased to 175 days with many organisations being made aware of breaches by external agencies. The report attributes this rise to increased notification programs by national law enforcement. These have uncovered attacks dating back a significant period of time, many of which involved active attackers in the target environment at the time of notification. In order to identify activity sooner, reduce the time between compromise and detection and subsequently reduce the impact of an organisation suffering the consequences of a damaging cyber breach, a new approach to cyber security is required.

Sun Tzu wrote in his famous book, The Art of War,

> "*If you know the enemy and know yourself, you need not fear the result of a hundred battles.*
>
> *If you know yourself but not the enemy, for every victory gained you will also suffer a defeat.*
>
> *If you know neither the enemy nor yourself, you will succumb in every battle."*

This mantra has stood the test of time and is in many Cyber Security related publications for good reason. It's important to understand your enterprise and also the threat actors who would target you, inclusive of their Tactics, Techniques and Procedures (TTP's). However, this alone won't reduce your time to detection of credentials-based breaches. To address the missing link, it's important to understand some of the environmental and ergonomic features of today's enterprise networks and how they've materialised. Traditionally organisations enlisted the services of boundary enforcing devices such as firewalls and proxies to act as a demarcation between the organisation and the outside world. This approach afforded a level of control as all communications with the outside world were via defined ingress and egress points. A fairly controlled threat landscape.

With the adoption of initiatives like bring your own device (BYOD) providing a cost effective and flexible approach to IT, employees can now work from anywhere and access the organisation systems remotely on their own devices, be it a laptop or smart phone. In some way's BYOD can be thought of in the same way as a prescription from your doctor, it's addressing a health complaint. In the instance of the corporate network, relating to the restrictive nature of operating with a rigid approach to carrying out business. The prescription addresses this by opening up the barriers introducing a flexible operating model and driving efficiencies, enabling email on the go etc via your smart phone or device. The trouble with this is that whilst the prescription resolves the original ailment it also introduces potentially damaging side effects that could ease the path to compromise for an attacker.

'MOST ATTACKS ARE OPPORTUNISTIC AND TARGET NOT THE WEALTHY OR FAMOUS, BUT THE UNPREPARED'

Embracing BYOD and other business efficiency enhancing convergence solutions increase the threat landscape and make it easier for an attacker to gain access without being detected. Without appropriate controls and monitoring in place, these platforms become easy targets for cybercriminals. Research presented within the Verizon Data Breach Investigation Report 2018 stated that '*Most cybercriminals are motivated by cold, hard cash. If there's some way they can make money out of you, they will. That could mean stealing payment card data, personally identifiable information or your intellectual property. And they don't care who they take it from. Ignore the stereotype of sophisticated cybercriminals targeting billion-dollar businesses. Most attacks are opportunistic and target not the wealthy or famous, but the unprepared*.' Without the ability to detect and minimise the impact of these advances, your network can become a sitting duck without defence.

Attacks on your environment come in all shapes and sizes with varying underpinning motives and your organisation being the direct or indirect target. As briefly mentioned earlier; from a Hacktivist where their goals are targeted because of political, social or moral outrage to Cyber criminals who are laser focused on obtaining money. Through to those of a Cyber

Terrorist whose motives are typically ideological. In addition, there are more unpredictable threats from 'script kiddies' who's motivation is selfishly for their own notoriety and to demonstrate their own cyber capabilities with little or no regard for what and who are affected as a result of their quest.

As mentioned previously; in nearly all reported breaches globally, the initial goal of an attack was to obtain valid credentials. Whether it be via phishing, malware or social engineering. Obtaining credentials allows the perpetrator to hide in almost plain sight masquerading as a valid employee as they move latterly through the network undetected. As a result, traditional controls such as Identity and Access Management (IDAM) solutions, Data Leakage Protection (DLP) and various boundary enforcing devices fail to stop this activity as, from their perspective, the utilised credentials are valid. Many enterprises embrace 2 factor authentication (2FA) in a move to strengthen access management. Whilst these solutions strengthen authentication, they don't eradicate the issue altogether. Attackers are smart. As an example, an attacker can infiltrate the initial logon challenge / response session via a basic man in the middle attack techniques to harvest the one-time 2FA credentials and gain successful access to the environment. Once in, they can remain persistent and may not be required to re-enter credentials for some time.

The majority of managed security services providers (MSSP) are delivering monitoring services today utilising legacy SIEM technologies in the hope that the combination of signals received from the various data points across the monitored estate will provide a level of detection that'll identify all known threats when coupled with the correlation rules that have been enabled within the SIEM tool. This simply isn't the case when considering the complex and sophisticated techniques utilised today and their approach can provide a false sense of security and leave monitored organisations exposed. Many of the organisations who are unfortunately the victims affected in recent breaches that made media headlines had technologies and services in place that failed to detect the compromise promptly. The reasons for these failures have been well documented but include insufficient logging scope, inability to associate context to observed activity and the failure of their Analysts in the ability to proactively threat hunt but also investigate potential issues swiftly with a high degree of accuracy.

Cyberseer is the cybersecurity managed detection and response provider powered by behavioural analytics and machine learning. This approach provides a real time intelligence-driven SOC, underpinned by the latest industry recognised technologies to deliver tangible benefits to the organisations who receive the service and subsequently reduce their chances of suffering the consequences of a damaging cyber breach.

WHAT IS AN INTELLIGENCE-DRIVEN SOC?

The Cyberseer service promotes a fresh approach to cyber security that's closely aligned to the guiding principles of an intelligence-driven SOC defined by information technology research and consultancy company Gartner. Gartner defined five main characteristics of an intelligence-driven SOC in their publication dated Nov 2015. At the time of being published, many of the techniques and technologies utilised today were not in existence. What was presented at the time of the publication was an accurate view that traditional log monitoring and event correlation capabilities are not sufficient to detect comprehensive threats and the techniques that are evading detection across todays threat landscape.

The 5 Gartner guiding principles documented are:

1. Deploy an adaptive security architecture.
2. Use advanced analytics to operationalise security intelligence.
3. Automate whatever and whenever it is feasible.
4. Use threat intelligence strategically and tactically.
5. Hunt and investigate.

Cyberseer managed detection and response service adopts a recursive lifecycle that aligns to these common principles to deliver a comprehensive real time advanced threat detection Service that is underpinned by leading edge, best of breed technologies to provide a level of visibility across the enterprise that's been inaccessible to many before. Cyberseer has developed an ecosystem of components that address advanced threat vectors that organisations are faced with in today's challenging cyber threat landscape. Figure 1 provides a logical overview of a typical service deployment. This integrates intelligence, advanced threat defence and protection technologies under an incident response framework. The Service has been designed to combine next generation technologies with expert human analysis to deliver on the vision of Cyberseer.

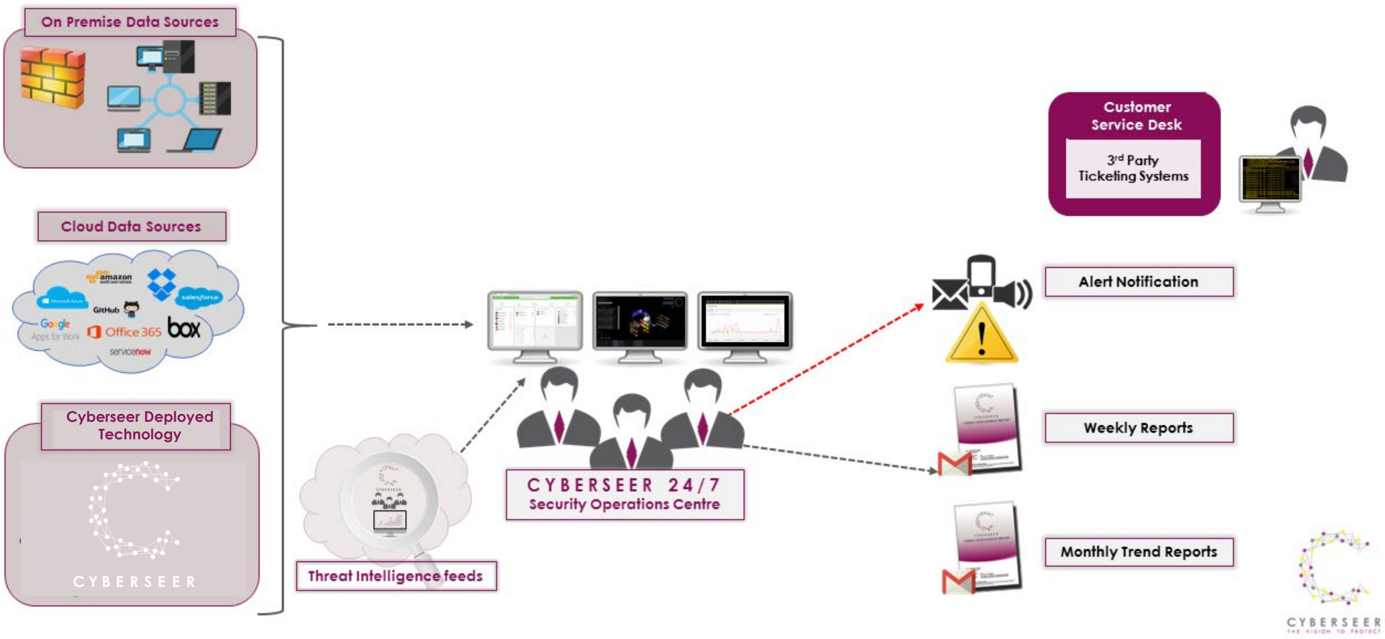

Figure 1: Logical overview of Cyberseer Service

Four main stages make up the Cyberseer Managed Service. The recursive process is designed around the need to provide continual improvement to the Service provided to maintain its effectiveness against both current and emerging cyber threats. Figure 2 outlines the stages of this process.

PREVENT

Understanding that no two deployments are equal; The Cyberseer Managed Advanced Threat Detection and Response Service is initially scoped based on a comprehensive understanding of the environment and the customer requirement. The proposed service provides a solid foundation and monitoring capability upon which Cyberseer can articulate the current threat landscape in relation to your organisation and then prescribe the correct service offing, underpinned by technology, to provide an effective solution to protect the organisation from harm.

The high-level output of this stage is:

- Defined monitoring topology inclusive of log source feeds (on prem/cloud), data flows etc.
- Traceability matrix of solution mapped back to requirements/objective.
- Agreed Customer communications plan.
- Service Scope/Service Review meetings.
- Updated monitoring scope (continual improvement)

DETECT

The 24x7 Service marries the expert skills and knowledge of industry leading analysts with threat intelligence, active threat hunting and behavioural analytics to understand the normal behaviour of your network/enterprise providing enhanced visibility whilst detecting anomalous activity immediately and early within the threat lifecycle. Be it the Identifying of lateral movement or an unusual account switch that's out of place. Spotting persistent attacks through comprehensive proactive threat hunting, across the entire cyber kill chain and identifying early traces of undiscovered threats as well as the initial steps of those associated with known TTP's and escalating this through to remediation swiftly with a robust incident handling and tracking process.

The high-level output of this stage is:

- Activity escalated as an incident.
- Activity escalated for automatic remediation
- Weekly Reports.

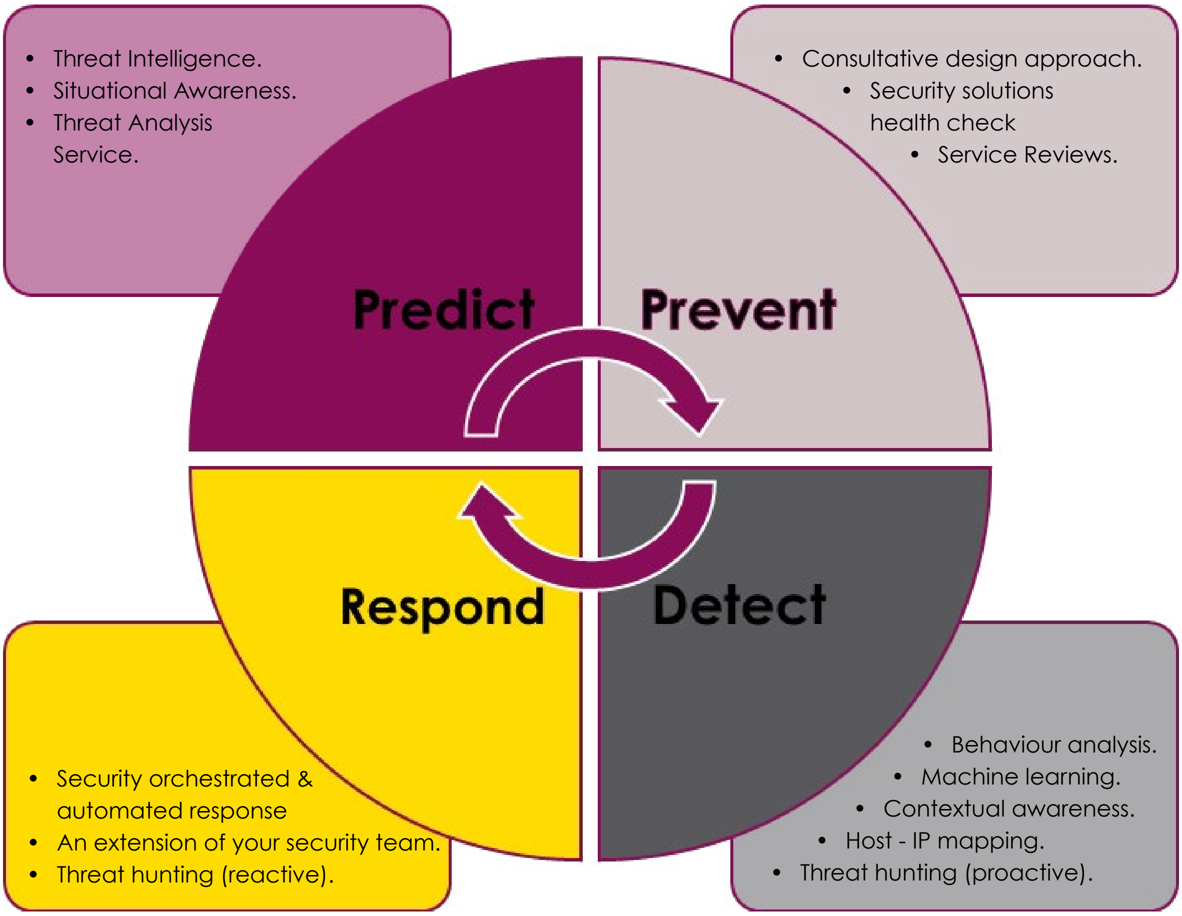
• Threat Intelligence.
• Situational Awareness.
• Threat Analysis Service.
• Consultative design approach.
• Security solutions health check
• Service Reviews.
Predict
Prevent
Respond
Detect
• Security orchestrated & automated response
• An extension of your security team.
• Threat hunting (reactive).
• Behaviour analysis.
• Machine learning.
• Contextual awareness.
• Host - IP mapping.
• Threat hunting (proactive).

Figure 2: Cyberseer Continual Service Improvement Lifecycle

RESPOND

Cyberseer provide immediate notification of high priority Incidents detected to a pre-defined customer escalation call plan. When required, Cyberseer will provide guidance and recommendations on remediation actions to take. Utilising tooling like Exabeam Incident Responder and Cylance PROTECT, Cyberseer can also support further investigation of Incidents and respond to threats directly through a series of automated playbooks. Playbooks provide a pre-defined Security Orchestration and Automated Response (SOAR) capability that effectively stich a series of individual actions together in support of a structured Incident Response process providing a complete, repeatable workflow for the swift remediation of Incidents. Playbooks are used to automate many of the tasks that an Analyst would do to increase accuracy and efficiency.

The high-level output of this stage is:

- Incidents escalated to Customer through predefined communications plan.
- Remediation of threats via SOAR playbooks.
- Recommendataions for system updates/ enhancements to service scope.

PREDICT

The Cyberseer Managed Service is underpinned by desire to remain current. Threats are constantly evolving, and our Analysts are continually researching the latest vulnerabilities and zero-day exploits. This research is utilised in the Pro-Active threat hunting carried out across the Cyberseer monitored customer environments. In support of this research, Threat Intelligence data is consumed from reputable sources and autonomously integrated into the monitoring solutions. Following Incidents, and where automation is possible, a new playbook may be created to ensure that the ability to respond quickly is maintained.

The high-level output of this stage is:

- Identification of artefacts from research/threat intelligence that are associated with Zero-day threats (IP addresses, network communications etc).
- Analyst Threat Reports.

Cyberseer provide customers with notification of activity in three main ways:

- Threat alerts are communicated directly to the primary customer contacts, for any threats which are deemed significant by our Analysts.
- Weekly threat updates providing a summary and technical detail of any newly classified threats. In addition, Management Information is also provided for the reporting period in a breakdown of the high-level activity observed and steps taken by Cyberseer Analysts.
- Monthly Threat Intelligence Reports contain the aggregated content from the previous four weekly threat update reports and month-on-month statistics trending of the overall changes in the customer threat level. This report also includes information about global threats/pandemics, any updates to the monitoring provided by Cyberseer in repsonse to these (new Threat Hunter searches etc.) and recommendations for the customer on steps that may need to be taken to secure the estate, patching etc.

CYBERSEER

☎ **CONTACT US +44 (0)203 823 9030**

If you would like to discuss any element of this white paper or find out about how the Cyberseer team can make difference within your organisation with regards to advanced threat detection, contact us today.

This white paper has been prepared by Cyberseer Ltd and contains information from a variety of sources.

info@cyberseer.net | www.cyberseer.net

Talk to us about customer use cases.

Demo the machine learning technology & the Cyberseer service.

Cyberseer have not sought to establish the reliability of these sources or verified information provided.