Compromise Assessment – Service Description

OFFERING OVERVIEW

DeepSeas' Compromise Assessment Service seeks to identify evidence of an active or historical security breach in Customer's IT systems by combining threat intelligence analysis, endpoint detection, and advanced threat hunting performed by an experienced team of DeepSeas cyber defense professionals.

The DeepSeas Compromise Assessment is typically conducted over an 8-week timeframe and includes the following activities:

- Analysis of Customer endpoint systems using Endpoint Detection and Response (EDR) software with the intent to identify evidence of past security threat events, active security threat events, and potentially unwanted system hygiene issues;
- Monitoring and analysis of active endpoint network and process activity using Endpoint Detection and Response (EDR) software;
- Analysis of external threat intelligence available through open, commercial, and dark web sources to determine if there is evidence of active security threats and possibly security vulnerabilities to Customer networks and data; and
- Preparation of a Compromise Assessment Findings Report that will identify compromised systems and related evidence, describe attacker activity and extent of observed compromise, identify potential high risk environment hygiene issues, and describe actionable findings and recommendations to remediate

DELIVERY TIMELINE

DeepSeas will work with the Customer to create an implementation plan, which will consist of deploying EDR technology, integrating EDR technology with Book Allen's cloud based cyber defense platform, and provisioning necessary access for DeepSeas cyber defense professionals.

STEP	DESCRIPTION	ESTIMATED DURATION
1. TECHNOLOGY DEPLOYMENT & PREPAREDNESS	Project Plan document will be produced that will detail status reporting, pulse check, working session and draft and final deliverable schedules.	2 weeks
2. THREAT IDENTIFICATION & ANALYSIS	Actionable notifications of threat activities and will be provided as alert-based evidence of cyber threats are discovered during the Compromise Assessment.	5 weeks

3. ACTIONABLE RECOMMENDATIONS	Weekly status calls will be held on day/time mutually agreed by the parties.	1 week

DELIVERABLES

The Compromise Assessment Service will produce the following Customer deliverables:

DELIVERABLE	DESCRIPTION	DOCUMENT FORMAT
PROJECT PLAN	Project Plan document will be produced that will detail status reporting, pulse check, working session and draft and final deliverable schedules.	MS PowerPoint
VALIDATED THREAT NOTIFICATIONS	Actionable notifications of threat activities and will be provided as alert-based evidence of cyber threats are discovered during the Compromise Assessment.	Email + Phone Call
WEEKLY STATUS CALLS	Weekly status calls will be held on day/time mutually agreed by the parties.	Phone Call / Tele-Meeting
REVIEW OF DRAFT COMPROMISE ASSESSEMENT REPORT	Parties meet to discuss findings from the Compromise Assessment to help ensure accuracy prior to finalizing the Final Report.	MS Word
FINAL COMPROMISE ASSESSMENT REPORT	Final Report that will include an executive summary of findings, detailed technical analysis of findings, and recommendations for containment and prevention of future compromise.	PDF

DELIVERABLE ACCEPTANCE

Customer shall have five (5) business days from its receipt of a Deliverable provided by DeepSeas to review and evaluate such Deliverable to determine whether the Deliverable substantially conforms with the specifications for the particular Deliverable as set forth herein, if any; and if no written acceptance or rejection is received by DeepSeas within such five (5) business day period, the Deliverable shall be deemed to be accepted.

1 Email MDR – Service Description

SERVICE OVERVIEW

DeepSeas' Email Managed Detection & Response service (Email MDR) delivers 24x7 triage and monitoring of suspected email phishing, compromise attacks reported by Customer users by simply pressing a button installed on users' Microsoft Outlook/O365. Suspicious emails identified are then isolated and aggregated in a separated, controlled cloud environment and forwarded to DeepSeas' managed detection and response (MDR) platform for human analysis, triage and disposition. Our team of highly experienced security analysts leverage superior tradecraft to review suspicious emails for evidence of phishing, malware, social engineering, zero-day exploits and other potential cyber threats that are delivered by email.

All users who submit suspected phishes receive an initial response acknowledging the submission and upon disposition of the phish, will receive a notification of the disposition by way of a mutually-agreed template. Additionally, a 'VIP list' is maintained, routinely updated and incorporated into the Email MDR program so that responses to Customer VIPs who submit suspected phishes are prioritized and responded to first. DeepSeas will evaluate suspected phishes within four (4) hours of their submission by a user via the Phish Button. If DeepSeas determines that there is a legitimate threat to the security of Customer's environment, we will immediately quarantine the email and send Customer a notification detailing our findings. Finally, DeepSeas will provide to Customer basic reporting about the Email MDR service performed on a monthly basis, such as the number of suspected phishes submitted and processed within a certain time period.

Our MDR program includes the following service elements:

- **Threat Detection** – DeepSeas threat detection provides review of alerts from, proactive enterprise search of, and targeted threat hunting using Customer security monitoring tools to identify and prioritize cyber threats.
- **Threat Notification** – Threat Notification reports are generated by DeepSeas cyber defense analysts to describe the nature, context, and severity of a validated threat along with remediation recommendations.
- **Threat Response** – DeepSeas cyber defense analysts provide Customers with response guidance and/or response actions for resolving threats. Response actions are defined in a mutually approved Customer MDR Runbook document.
- **Curated Threat Intelligence** – DeepSeas applies curated detection logic and analytics to security monitoring tools deployed in customer networks to improve the effectiveness of threat detection and response.
- **DeepSeas XDR Cyber Defense Platform** – DeepSeas XDR Cyber Defense Platform provides customers with a cloud-hosted technology architecture that supports data collection, analysis, automated response, and reporting capabilities across multiple attack surfaces.

1 THREAT RESPONSE

During onboarding, DeepSeas will work closely with Customer stakeholders to jointly develop a Customer MDR Runbook, which will detail individual responsibilities for responding to Threat Notifications delivered by DeepSeas. Response actions are typically categorized as one of the following:

RESPONSE TYPE	DESCRIPTION
GUIDED RESPONSE	Guided Threat Response provides customers with recommended response actions that the Customer’s internal team should complete to contain, mitigate, or remove a threat identified in a DeepSeas Threat Notification.
PROACTIVE RESPONSE	DeepSeas will perform specific threat containment response actions based upon the Statement of Work. Active Response actions may be combined with Guided Response actions to facilitate incident resolution. Example proactive response capabilities include endpoint system containment, proxy modification, firewall modification, and custom API integrations.
BREACH RESPONSE	Upon activation of a pre-negotiated Incident Response retainer, DeepSeas will provide dedicated and (as needed) on-site investigation, triage, recovery, and remediation.

Endpoint MDR – Service Description

SERVICE OVERVIEW

DeepSeas' Managed Detection & Response services (MDR) provide monitoring, detection, analysis, and response to validated security threats within client environments enrolled in one or more DeepSeas' MDR offerings. The DeepSeas Cyber Defense Team evaluates alerts generated by security monitoring technologies deployed within Customer environments. When DeepSeas determines that an alert is a legitimate threat to the security of the Customer's environment, a threat notification report will be delivered that provides detailed information associated with the threat and recommended courses of action. DeepSeas can also perform response actions, as necessary, in support of responding to threats.

DeepSeas' Endpoint Managed Detection and Response service (Endpoint MDR) delivers 24x7x365 endpoint threat detection, analysis, and response to validated cybersecurity threats within a customer's environment. Endpoint monitoring is a critical component of detecting and validating the severity and origination of a threat. Threat detection includes monitoring of alerts by DeepSeas cyber defense analysts who triage, examine, and categorize alerts generated from a specified endpoint detection and response (EDR) technology. DeepSeas, through its subject matter experts and technological capabilities, also provide threat hunting and detailed forensic investigation in support of the monitoring, detection, and response mission.

DeepSeas' Cyber Defense Team identifies potential security threats in Customer environments using a combination of alert enrichment and review, open and closed source cyber threat intelligence, enterprise data search, and targeted cyber threat hunting. When DeepSeas identifies and validates a potential security threat in a monitored Customer environment, a Threat Notification report is documented and delivered to the Customer in alignment with a scaled threat severity model. Should a threat be identified on an endpoint within the Customer's network environment, a Validated Threat Notifications report will be sent to the Customer and will include severity level, vector information, and recommended response actions to mitigate the threat. Threat Notification reports are created in the form of a case event in the DeepSeas customer portal. Depending on the threat severity, direct contact is made in accordance with the Customer-provided notification escalation order, per the Customer MDR Runbook that DeepSeas and Customer will mutually agree upon during kickoff.

Our MDR program includes the following service elements:

- **Threat Detection** – DeepSeas threat detection provides review of alerts from, proactive enterprise search of, and targeted threat hunting using Customer security monitoring tools to identify and prioritize cyber threats.
- **Threat Notification** – Threat Notification reports are generated by DeepSeas cyber defense analysts to describe the nature, context, and severity of a validated threat along with remediation recommendations.
- **Threat Response** – DeepSeas cyber defense analysts provide Customers with response guidance and/or response actions for resolving threats. Response actions are defined in a mutually approved Customer MDR Runbook document.
- **Curated Threat Intelligence** – DeepSeas applies curated detection logic and analytics to security

monitoring tools deployed in customer networks to improve the effectiveness of threat detection and response.

- **DeepSeas XDR Cyber Defense Platform** – DeepSeas XDR Cyber Defense Platform provides customers with a cloud-hosted technology architecture that supports data collection, analysis, automated response, and reporting capabilities across multiple attack surfaces.

SUPPORTED EDR PRODUCTS & LICENSING OPTIONS

DeepSeas supports both on-premises and cloud-based EDR solutions (see “List of Supported Endpoint Products” below).

LIST OF SUPPORTED ENDPOINT PRODUCTS				
PLATFORM	SUPPORT COMPONENTS			LICENSING OPTIONS
	Cloud Version	On-Premises Version	Curated Threat Intel	
VMware Carbon Black™	Yes	No	Yes	• Bring Your Own License[1] • Purchase Through DeepSeas[2]
CROWDSTRIKE Falcon™	Yes	N/A	Yes	• Bring Your Own License • Purchase Through DeepSeas (Falcon X and NGAV)
Endgame™	Yes	No	Yes	• Bring Your Own License
FireEye HX™	Yes	Yes	Yes	• Bring Your Own License
Microsoft Defender for Endpoint™	Yes	N/A	Yes	• Bring Your Own License
SentinelOne™	Yes	N/A	Yes	• Bring Your Own License
Tanium™	Yes	Yes	Yes	• Bring Your Own License

THREAT RESPONSE

During onboarding, DeepSeas will work closely with Customer stakeholders to jointly develop a Customer MDR Runbook, which will detail individual responsibilities for responding to Threat Notifications delivered by DeepSeas. Response actions are typically categorized as one of the following:

RESPONSE TYPE	DESCRIPTION

[1] Bring Your Own License - Customer can elect to purchase EDR through supplier of their choice. Customer owns licensing and any associated fees.

[2] Purchase Through DeepSeas - Customer can elect to purchase certain EDRs through DeepSeas who will provide as a cloud-hosted, third party EDR software platform as defined in a separate SaaS Agreement.

GUIDED RESPONSE	Guided Threat Response provides customers with recommended response actions that the Customer’s internal team should complete to contain, mitigate, or remove a threat identified in a DeepSeas Threat Notification.
PROACTIVE RESPONSE	DeepSeas will perform specific threat containment response actions based upon a defined MDR runbook. Active Response actions may be combined with Guided Response actions to facilitate incident resolution. Example proactive response capabilities include endpoint system containment, proxy modification, firewall modification, and custom API integrations.
BREACH RESPONSE	Upon activation of a pre-negotiated Incident Response retainer, DeepSeas will provide dedicated and (as needed) on-site investigation, triage, recovery, and remediation.

CURATED THREAT INTELLIGENCE

DeepSeas MDR customers benefit from continuous technical threat intelligence updates that are applied to tools and platforms managed by DeepSeas. DeepSeas’ cyber threat intelligence research team employs a rigorous methodology to generate, curate and publish threat intelligence analytics and detection signatures that are used to enhance the detection technologies deployed within Customer networks. The application of cyber threat intelligence improves threat detect and response through timely identification of adversary techniques and indicators and provides increased threat context during response activities.

DEEPSEAS’ CYBER DEFENSE PLATFORM

DeepSeas MDR customers integrate their security technology tools and have secure access to the DeepSeas XDR Cyber Defense Platform, a cloud hosted technology architecture that provides data collection, analysis, response, and reporting capabilities across multiple attack surfaces (e.g. endpoints, networks, and operations technology).

The following features and capabilities are included as part of the DeepSeas XDR Cyber Defense Platform:

Service Orchestration Appliance

The DeepSeas Service Orchestration Appliance is used to collect relevant data from the Customer-deployed security tools platforms or applications and to enable specified response actions using API (Application Programming Interface) communications. The appliance can be deployed physically or virtually. During service initiation, DeepSeas and Customer will agree upon the required number of Service Orchestration Appliances and the location(s) where deployment is required.

Cyber Threat Analysis and Response Framework

The DeepSeas Threat Analysis and Response Framework is a collection of automated capabilities that are used by the DeepSeas Cyber Defense Team to enrich, analyze, and respond to security alerts and threats within a Customer environment.

Customer Portal

The DeepSeas Customer Portal provides validated threat notification information, threat details, remediation support recommendations, and other information related to the level of service stipulated in the Statement of Work. The Customer Portal provides:

- **Threat Notification and Case Management** tracking solution which provides visibility into case activities such as real-time threat investigation information, case status, and other actionable information that the Customer can use to review and mitigate a validated threat.
- **Metrics and Reporting Insights** that quantify the status of Customer's MDR services.
- **Knowledge Management Documentation** describing the MDR service features and common Customer questions.
- **The Ability to Submit questions and Support Requests** to the DeepSeas Cyber Defense Team 24x7x365

24x7 Customer Hotline

The DeepSeas MDR Customer Hotline allows Customers to contact the DeepSeas Cyber Defense Team 24 hour a day, 365 days per year through a dedicated customer telephone number.

SERVICE ONBOARDING TIMELINE

The following table describes the typical steps DeepSeas undertakes together with the Customer to onboard and initialize our Endpoint MDR service

STEP	DESCRIPTION	ESTIMATED DURATION (WEEKS)
1. Kick-Off	DeepSeas and the Customer participate in a joint call to confirm services, service orchestration appliance placement (if required), shipping information, definition of a Customer MDR Runbook and other key details regarding the Services that shall be provided. During the Kick-Off, the Customer is introduced to their Technical Support Engineer (TSE) / Service Delivery Manager (SDM).	<1 WEEK
2. EDR Deployment	The Customer will deploy the EDR controller and EDR agents to endpoints as applicable and appropriate per the specific software solution and SOW.	1-3 WEEKS
3. Service Orchestration Appliance(s) Deployment	If needed, appliances are shipped within the continental United States with an estimated delivery time of 2-3 days (International shipping schedules will vary).	2-3 WEEKS

	Integration is confirmed when telemetry data flow from the EDR controller to the appliance is established and from the appliance(s) to DeepSeas.	
4. Baseline	DeepSeas will begin monitoring the EDR platform alerts and begin notifying the Customer of validated threats while creating a baseline for priorities, focus, and response.	1 WEEK
5. Service Optimization & Go-Live	DeepSeas services are fully operational and adjusted as needed to meet Customer needs, as defined in the Statement of Work. DeepSeas will provide reports and on-going communication to the Customer.	4+ WEEKS

Firewall / NGFW[3] Management – Service Description

SERVICE OVERVIEW

DeepSeas' Firewall & Next-Gen Firewall Management Service (FMS) provides 24x7 management and monitoring of Customer's firewalls, ensuring consistent configuration and tuning and that the appropriate updated versions of the firewall software and operating systems are running. DeepSeas will be responsible for normal configuration changes, as directed by Customer's designated point of contact, ticketing system maintenance and change process management. DeepSeas will collect in-scope firewall logs through the log output facility and may, if deemed necessary by our technical experts, deploy log collection appliance(s) to Customer's premises to support data ingestion and analysis.

Our FMS program includes the following service elements:

Configuration Management

1. 24x7 management of firewall changes, rule changes, policy configurations, modifications, etc. (limited to 10 rules or policy changes per month)
2. Foundational configuration of integrated firewall modules, blades or add-on, which may include IPS, web filtering, gateway anti-virus and application control modules.

- Full version software upgrades to existing firewall hardware with new versions as they become available and are validated as stable by DeepSeas (hardware upgrades are not included, nor are software upgrades that cannot be supported by existing hardware).
- Firewall maintenance, including patching and updates (e.g. hotfixes, firmware updates, software upgrades, etc.).
- Quarterly assessment and report of firewall policies via a formal policy configuration assessment.

Firewall Event Collection & Reporting

- Log collection, aggregation, and correlation analysis of security threats identified through firewall logs (includes log retention for up to one full year).
- Correlation of intelligence data to identify infected endpoints behind the firewall communicating outbound to malicious sites, bot networks, command and control centers, etc.

[3] NGFW = "Next Generation Firewall"

- Firewall up/down availability monitoring; standard operating procedures are to notify Customer within 15 minutes of the firewall or firewall connectivity being unavailable.
- Risk-based firewall event correlation, triage and security trend reporting.
- Web portal access for Customer to view firewall reports, log analysis, security activity metrics, report scheduling, support call tracking and current security alert information (includes interactive self-analysis tools and drill-down charts).

Threat Response Orchestration

- As part of a larger detection and response program, DeepSeas firewall management service can be integrated into threat response procedures via implementation of blocking action on specified customer firewall(s) to stop detected and confirmed malicious behavior.

SUPPORTED FIREWALL TECHNOLOGIES

DeepSeas supports the following advanced firewall technologies, one of which Customer is expected to procure, license, deploy and maintain:

LIST OF FIREWALL TECHNOLOGIES			
FIREWALL TECHNOLOGY	SUPPORT COMPONENTS		LICENSING OPTIONS
	Cloud Version	On-Premises Version	
CheckPoint™ NGFW	DeepSeas Managed	DeepSeas Managed	• Bring Your Own License[4]
Cisco® Secure Firewall	DeepSeas Managed	DeepSeas Managed	• Bring Your Own License
Fortinet™ Fortigate	DeepSeas Managed	DeepSeas Managed	• Bring Your Own License
Palo Alto Networks™ NGFW	DeepSeas Managed	DeepSeas Managed	• Bring Your Own License
SonicWall® NGFW	DeepSeas Managed	DeepSeas Managed	• Bring Your Own License

[4] Bring Your Own License - Customer can elect to purchase a supported platform through the supplier of their choice. Customer owns licensing and any associated fees.

CUSTOMER RESPONSIBILITIES

1. Provisioning and overall maintenance of firewall infrastructure and software aligned to the Supported Firewall Technologies listed above.
    - Customer assumes all risk and liability associated with changes and modifications made by Customer's personnel to the managed device(s) and relieves DeepSeas of its performance obligations and service level agreements based on any read/write modifications that Customer makes to devices managed by DeepSeas.
    - If Customer introduces a change to a devices configuration, rules, or policies that creates instability, security vulnerabilities, loss of functionality, or similar problems, DeepSeas may at its option and full discretion charge Customer for recovery from such changes to the device's reconfiguration.

Forward Deployed Resources – Service Description

OVERVIEW

Forward-Deployed Resources (FDRs) are DeepSeas cyber operations team members that are dedicated to supporting a specific customer cyber defense program. FDRs extend DeepSeas' managed detection & response (MDR) services and operate cross-functionally to maximize the depth and business integration the DeepSeas MDR services. To accomplish these objectives, DeepSeas FDRs are deeply embedded in the L1, L2, and L3 workflows typical of the standard cyber fusion center (CFC) model. Additionally, FDRs facilitate close coordination with both Customer and third-party resources and provide valuable business context to remote CFC analysts.

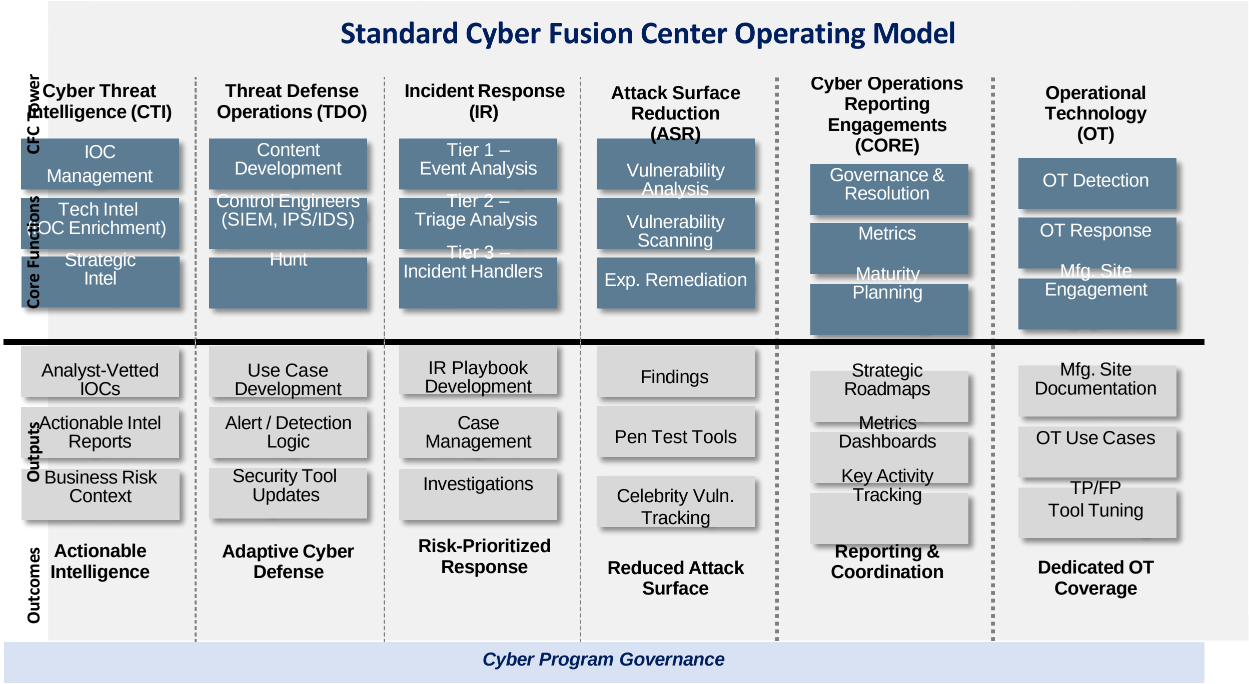
FDRs support the following MDR program elements:

- **Operations –** Global monitoring, detection and response across multiple attack surfaces while improving visibility and offering risk reduction in the form of dedicated response support.
- **Tradecraft –** DeepSeas' subject matter experts (SMEs) continually tune controls based on intelligence-driven analysis and generate advanced analytics to identify threats more proactively.
- **Partnership –** We prioritize performance, transparency, and accountability to build and sustain a trusted partner relationship between the DeepSeas and Customer security teams.

FORWARD-DEPLOYED CAPABILITIES

The following figure illustrates a standard CFC operating model:

1



Standard Cyber Fusion Center Operating Model

CFC Tower	Cyber Threat Intelligence (CTI)	Threat Defense Operations (TDO)	Incident Response (IR)	Attack Surface Reduction (ASR)	Cyber Operations Reporting Engagements (CORE)	Operational Technology (OT)
Core Functions	IOC Management	Content Development	Tier 1 – Event Analysis	Vulnerability Analysis	Governance & Resolution	OT Detection
	Tech Intel (IOC Enrichment)	Control Engineers (SIEM, IPS/IDS)	Tier 2 – Triage Analysis	Vulnerability Scanning	Metrics	OT Response
	Strategic Intel	Hunt	Tier 3 – Incident Handlers	Exp. Remediation	Maturity Planning	Mfg. Site Engagement
Outputs	Analyst-Vetted IOCs	Use Case Development	IR Playbook Development	Findings	Strategic Roadmaps	Mfg. Site Documentation
	Actionable Intel Reports	Alert / Detection Logic	Case Management	Pen Test Tools	Metrics Dashboards	OT Use Cases
	Business Risk Context	Security Tool Updates	Investigations	Celebrity Vuln. Tracking	Key Activity Tracking	TP/FP Tool Tuning
Outcomes	Actionable Intelligence	Adaptive Cyber Defense	Risk-Prioritized Response	Reduced Attack Surface	Reporting & Coordination	Dedicated OT Coverage

Cyber Program Governance

Cyber Fusion Center (CFC) Program Leader

The CFC Lead serves as a Program Manager for all DeepSeas activities. The CFC Lead serves as the Customer security leadership's primary point of contact for coordination efforts. The CFC Lead also acts as Lead Incident Handler to coordinate IR activities conducted by the remote CFC, and between the Customer, DeepSeas , and third-party IR and information technology (IT) resources. The CFC Lead will also be responsible for collecting and reporting key metrics to the Customer security team to provide insight into security program efficacy. Examples of such metrics include Mean Time to Detect (MTTD), Mean Time to Contain (MTTC) and Attacker Dwell Time. Additionally, the CFC Lead coordinates daily/weekly operational stand-up meetings, monthly leadership reviews, and quarterly business reviews.

Cyber Threat Intelligence (CTI) Analyst

Our CTI FDRs support the contextualization of threat intelligence on the Customer enterprise, with a focus on broader and deeper integration of the Threat Intel Platform (TIP) and CTI integration with various Customer lines of business.

Threat Defense Operations (TDO) Analyst

DeepSeas TDO specialists will work to further develop enhanced detections within the Customer toolset, with a focused effort on post-exploitation TTPs. Hunt will support the continued maturation of the Cyber Data Lake, enabling a near-real time search capability. TDO can also work with DeepSeas' Security Tools Effectiveness Assessment (STEA) tool to validate security controls.

Incident Response (IR) Analyst

Our IR FDRs help reduce response times for threats uncovered within the Customer’s enterprise and help drive greater contextualization of threat data into the CFC framework. Our SMEs prevent attackers from maintaining dwell time by applying superior tradecraft to improve detections and broaden correlations.

Attack Surface Reduction (ASR) Operations Analyst

Our LMR will continue to support the overall CFC governance functions, as well as drive fusion integration both within the CFC team as well as related cybersecurity functions. With a primary emphasis on defining standardized processes, meaningful data, and actionable reports, LMR will continue driving metrics initiatives, CFC team cadences, and fusion operations.

Cyber Operations Reporting Engagement (CORE) Analyst

Our CORE function supports the overall CFC governance functions, as well as drive fusion integration both within the CFC team as well as related cybersecurity functions. With a primary emphasis on defining standardized processes, meaningful data, and actionable reports, CORE analysts drive metrics initiatives, CFC team cadences, and fusion operations.

Operational Technology (OT) Security Analyst

DeepSeas OT security analysts will enable Customer to protect its manufacturing capabilities and ensure both safety & trust. The CFC’s OT team will accelerate the operationalization and integration of OT data into the CFC’s detection platform and enhance response readiness and capabilities.

Incident Response Retainer – Service Description

SERVICE OVERVIEW

DeepSeas' Incident Response Retainer Service (IR Retainer) consists of comprehensive and tailored incident response services that adhere to a typical incident response lifecycle (i.e. prepare, detect, respond, and recover) as detailed below. Upon receiving written request for support, DeepSeas will engage with Customer determine the type of IR services required. The agreed-upon type of response activities must be documented and agreed to in a written work plan between the parties before any such Services commence (email will suffice for this purpose). In addition, during any such active engagement periods, DeepSeas will provide the Customer project leader with weekly status reports in Microsoft Word or PowerPoint format, indicating the status of DeepSeas' activities

Our IR Retainer services are offered either on a pre-paid or post-paid basis. With a pre-paid IR Retainer, Customer is guaranteed a response time of ≤12 hours for remote support or ≤24 hours for on-site support within the United States, while response times for international destinations will be mutually agreed upon. With a post-paid IR Retainer, Customer will not be guaranteed response times, instead responding to Customers on a best-efforts basis depending on the urgency of the request.

Customer will also have access to a 24x7 support watch center throughout an IR engagement. Depending on the incident and Customer requests, DeepSeas and Customer will align on the appropriate response requirements and suggested response implementation tasks. This may include Customer providing to DeepSeas certain artifacts, sample data and access to certain systems to analyze and evaluate the response needs based on impact (e.g. logs, malware samples, forensic images, live response data sets).

DeepSeas Incident Response Retainer Service is fulfilled by DeepSeas strategic partner, Booz Allen Hamilton.

IR APPROACH

Our approach to IR services can be segmented into four (4) distinct stages:

Initiation - Requesting DeepSeas' incident response services starts with a call to our IR call center, where cyber watch staff are standing by 24x7x365 to coordinate IR support. Immediately after a call is received, the standby IR team lead is notified of the request for support and will contact Customer to gather additional details regarding the incident, the request for support, and response logistics. During the call or other communications, a determination for remote or on-site support will be made and DeepSeas’ response team will be assembled to support Customer.

Triage - Remote and/or on-site technical response support activities begin with a detailed consultation call or face-to-face meeting to understand the current state of Customer’s response, discover the available datasets and Customer toolsets that can aid the response, determine the entry point into the current response, identify any additional skillsets required of the response team and begin discussions to deploy toolsets, if required, to address any identified data or toolset gaps in Customer’s currently installed security monitoring and analysis stack.. At the conclusion of the consultation meeting, DeepSeas will immediately begin working with Customer to contain any ongoing attacker activity and, depending on incident severity, establish a war room and/or operational meeting tempo for the response. We will also provide ongoing support to CUSTOMER’s incident commander to coordinate interactions with response teams, the legal team, law enforcement, board, and regulators as required.

Detection and Analysis – DeepSeas technical analysts will collect relevant datasets and begin an iterative detection and analysis process to provide the detailed information and insights required for remediation and report generation efforts. DeepSeas will work with Customer to develop an evidence collection plan. We will identify available datasets and prioritize the collection plan based on currently known information about the intrusion. The collection plan status will be tracked by DeepSeas and adjusted as necessary based on investigation needs. If log data must be removed from Customer’s production environment for analysis, the information obtained and analyzed will be logged, stored and managed securely. DeepSeas digital forensic SMEs will also support Customer in matters requiring forensic acquisition and analysis. DeepSeas, at Customer’s request, will acquire forensic images, coordinate asset identification, perform forensic analysis and produce a full forensic report on the systems in question. The image acquisition can be performed with the industry standard imaging toolsets provided by DeepSeas or through enterprise forensic image acquisition toolsets installed within Customer’s environment. Through either acquisition method, chain of custody (CoC) will be maintained throughout the digital forensic lifecycle. Once the digital forensic image process is complete, DeepSeas will conduct a verification process examining the MD5 hash values to check the entirety and integrity of the collected data, verifying that the process produced a functional and complete forensic image. The forensic analyst will create a copy of the image and perform the necessary analysis to provide evidence relevant to the investigation. The data will be analyzed by experts in Network, Log, Forensics, or Malware analysis skillsets to quickly provide investigation results. In addition, online and social media data will be analyzed by experts in Disinformation Advisory skillsets to determine degree of mis- and disinformation spread by influential actors, corresponding confidence decline (based on news of the attack or based on experience with operational disruption), and potential impact on the business.

Remediation - As findings are developed through the Detection and Analysis process, the remediation phase is executed. DeepSeas will coordinate a three-part remediation process which includes, (1) containment, (2) eradication, and (3) recovery.

DeepSeas may also support ransomware remediation activities to include working with Customer to change any known compromised credentials, isolate machines with ransomware activity from the clean parts of the network and establish processes to prevent off-network machines from re-introducing the malware. Once the incident is contained, DeepSeas will work with Customer to understand whether suitable backups of any encrypted data are available to be restored. At the same time we will leverage our dedicated threat intelligence team to identify whether a given executable (if available) or encrypted file type is related to a known ransomware family and determine whether there are known weaknesses in the encryption and the attacker's typical timeline and reliability in responding to ransom payments, if needed. Once the data recovery plan has been established, DeepSeas will work with Customer to block known C2 channels, conduct widespread credential refreshes, and rebuild affected machines to eradicate the malware.

The following table provides further descriptions of the types of IR services that may be requested to be performed by DeepSeas (in conjunction with our strategic consulting services partner DeepSeas Hamilton, a global consulting firm with a 100+ year history):

OFFERING CATEGORY	OFFERING TYPE	DESCRIPTION
PREPARE	Incident Response Plan Development and/or Enhancement	Review and document your existing incident response capabilities, to identify and close support gaps.
	Playbook Integration	Details incident response roles, processes and procedures across various business units to help enable smooth coordination during an incident.
	Incident Response Tabletop Exercise	Run a mock cyber incident to test, practice, and evaluate roles, processes, and procedures across key stakeholders.
	Breach Readiness Assessment and Roadmap	Determine your technical ability to detect and quickly respond to

1

		a cyber incident.
DETECT	24x7 Response Hotline	Access to our IR Watch Center, where experienced cyber watch staff coordinate flyaway incident response support.
	Support Team Assembly	Identify and deploy appropriate resources, which may include staff with the following skillsets: digital forensics analysis, network analysis, malware and triage analysis, Advanced Persistent Threat (APT) hunting, and disinformation advisory.
	Containment Support	Develop and implement a strategy to remove a sophisticated intrusion. Includes the gap analysis required to determine the scope and cost of remediation planning.
RESPOND	Remediation Plan Implementation	Removal of malicious activity or threats from the network.
	Advanced Threat Analysis	Threat analysis by skilled analysts with extensive experience dealing with advanced threat actors, including highly sophisticated cybercriminal groups and nation states. Includes analysis of opportunistic bad actors pushing disinformation in a time of Customer vulnerability and/or in response to unfavorable results of intervention.
	Evidence Collection and Management	Provide proper collection and management of digital evidence for investigation purposes. Includes both short and long-term evidence storage, and the maintenance of an evidence chain of custody.
	Crisis and Incident Management	Coordinate non-technical incident management to help ensure smooth business operations across the enterprise for business units or other stakeholders impacted by the incident.
	Malware Reverse Engineering	If required, the reversal of bundled code or binaries extracted from the Customer environment will be performed in an attempt to determine code functionality, additional indicators associated with the malware family and investigation effort, or other pertinent information relevant to Customer.
RECOVER	Post-Mortem Assessment	A performance review of the incident response and the incorporation of any lessons learned into your incident response plans and playbooks.
	Incident Response Investigation and Litigation Support	Independent investigation of an intrusion for the purposes of improving future responses or providing an independent assessment under privilege for litigation support and compliance

1

		purposes. This does not include any provision of testimony or court appearances.
	Requests for Intelligence (RFIs) and Private Investigator Services	Provide RFIs which can be utilized to support a range of on demand services ranging from ransomware negotiation and certain Virtual Currency exchanges, data and digital asset recovery, and malware analysis, to threat actor profiles or threat landscape analysis.

Infrastructure Vulnerability Management – Service Description

SERVICE OVERVIEW

DeepSeas' Infrastructure Vulnerability Management solution ("IVM") provides the Client with customized vulnerability scanning (identification); triage of detected vulnerabilities within your network, based on a combination of your vulnerability management platform's internal risk scoring model and your organizations specific policies (prioritization); and response coordination including workflow/process setup and tracking, reporting, and trend analysis (remediation).

Our IVM program includes the following service elements:

- **Identify vulnerabilities** and mitigate risk to your network and IT assets. The IVM service includes scanning of your internal network devices, servers and other assets in on-premise and/or cloud environments. Different service levels and options are available that can be tailored to the specific needs of your organization.
- **Prioritize discovered vulnerabilities** and provide Customers with expert advice and the support they need to quickly and accurately triage vulnerabilities detected within your environment to ensure the most critical and high-risk network vulnerabilities are addressed as quickly as possible.
- **Coordinate vulnerability remediation** to help Customer identify vulnerabilities and provide expert guidance and specific recommendations to mitigate or remediate them, thereby helping you reduce your overall cycle time for vulnerability remediation.

VULNERABILITY IDENTIFICATION

Vulnerability Identification comprises i) vulnerability scan management; and ii) vulnerability reporting. and results management delivered by DeepSeas and leveraging commercially-available scanning tools.

i) Vulnerability Scanning

Our solution includes vulnerability scanning of the Client's internal "active" and "dark", Internet Protocol (IP) addresses. Scans of internal and cloud-based IPs are conducted from one or more Scan Appliances within your network or data center.

Included in Vulnerability Scanning are the following components:

- Manage/update scan profiles and scan schedules
- Manage/update asset groups, asset group owners and asset tags

- Launch asset discovery (“mapping”) scans
- Launch and verify execution of IVM scans, on-demand scans and policy compliance scans
- Review scan results and generate reports
- Troubleshoot any detected problems with scans, and;
- Schedule, prepare for and conduct quarterly scan review meetings (as add-on option)

ii) Vulnerability Reporting

After vulnerability scans are executed, the next step is to review and analyze the scan results, in the form of various vulnerability reports.

Included in Vulnerability Reporting are the following components:

- review scan results/reports,
- troubleshoot any detected problems with scan reports/report templates,
- manage reporting schedules/scheduled reports,
- prepare monthly reports for monthly review meetings with your designated technical/asset group owners,
- prepare and review quarterly scan reports

iii) Vulnerability Prioritization

DeepSeas will triage the results of the Customer’s ongoing vulnerability scans to determine which vulnerabilities require the most immediate attention, based on the relative risk they represent.

Included in Vulnerability Prioritization are the following components:

- Correlate vulnerabilities found during scanning activities with Customer’s existing internal compensating controls and analyse known cyber threats to adjust the remediation priority of the scan findings High severity vulnerabilities, as well those with known exploits and/or identified as newly discovered (zero-day) vulnerabilities, will generally be given the highest priority, as well as any other specific vulnerabilities the Customer wants the team to focus on during remediation.
- Review and consider the Customer’s vulnerability exception policy to determine if any of the discovered vulnerabilities may be granted an exception from remediation.
- Provide Risk Analysis for Discovered Vulnerabilities to Client's Asset Owners.

1

VULNERABILITY REMEDIATION COORDINATION

In coordinating the remediation of any infrastructure vulnerabilities discovered, DeepSeas will consider and analyse asset priorities, enterprise security strategies, and other IT environmental variables when presenting guidance and recommendations to your designated technical asset owners and/or points of contact (POCs).

For high priority vulnerabilities that the client requests further notifications of, DeepSeas will provide additional communications in the form of ticketing updates, email and/or phone calls to members of the onsite team. In addition, notifications of newly discovered vulnerabilities will be sent to your ticketing system (if it is supported by Customer's VM platform's API) and tickets will be created and assigned to your designated technical POCs, automatically.

Included in Vulnerability Remediation are the following components:

- Conduct monthly vulnerability management scan result review meetings with each of your designated asset group owners to help drive and coordinate remediation activities. The number of meetings is based on the number of scan/reporting cycles and asset group owners the Customer identifies during onboarding.
- Engage with the Customer's designated team members/technical POCs for monthly scheduled meetings and on-demand meetings (up to 3 per month) to discuss remediation executive summaries; review priorities; help answer any questions; provide recommendations; and assist with process workflow planning and details for the remediation of detected vulnerabilities.
- review the discovered vulnerabilities and recommended remediation steps and solutions with your designated asset owners/technical POCs, based on available information. IT asset owner-focused reports will also be compiled, reviewed and discussed to reflect the security status of the scanned assets.

SERVICE ONBOARDING TIMELINE

The following table describes the typical steps DeepSeas undertakes, together with Customer, to onboard and initialize our IVM service:

1

STEP	DESCRIPTION	ESTIMATED DURATION (WEEKS)
16. Kick-Off	DeepSeas and the Customer participate in a joint call to confirm services, service orchestration appliance placement (if required), shipping information, definition of a Customer IVM Runbook and other key details. During Kick-Off, the Customer is also introduced to their Technical Support Engineer (TSE) / Service Delivery Manager (SDM).	<1 WEEK
17. VM Tool Deployment Validation and Testing	Together, DeepSeas and the Customer will validate the Customer's deployment of their licensed VM tool to ensure all assets are mapped and data is flowing appropriately.	1-2 WEEKS
18. Baseline	DeepSeas will begin monitoring the EDR platform alerts and begin notifying the Customer of validated threats while creating a baseline for priorities, focus, and response.	1 WEEK
19. Service Optimization & Go-Live	DeepSeas services are fully operational and adjusted as needed to meet Customer needs, as defined in the Statement of Work. DeepSeas will provide reports and on-going communication to the Customer.	4+ WEEKS

Log Analytics – Service Description

SERVICE OVERVIEW

DeepSeas' log analytics solution provides a cloud hosted platform that provides collection, normalization, enrichment, storage, and high-speed search of security event logs and other machine data that can be helpful in investigating security threats, reviewing security activity trends, and performing analytical searching for various security operations purposes.

SERVICE ELEMENTS

DeepSeas Log Analytics includes the following service elements:

Security Event Log Management and Enrichment

- **Log Collection and Normalization** – Collection and normalization of device logs for In Scope Devices as received and processed in near real time, made available for customer access through the Customer Portal.
- **Event Log Enrichment –** DeepSeas Log Analytics will enrich customer log data through automated analysis. Event enrichment functionality include:
    - **Device and Asset Identification** - Log device asset identification, tracking, & reporting on customer device assets on the same network, subnet, or VLAN as the data collector, based on best efforts to auto-identify assets ingesting into the service.
    - **Scans Surveillance** – Identification and logging of network scans from external sources conducting vulnerability scanning.
    - **Event Log Correlations** – Pre-built correlations add additional event context to Customer security data to add further context and identification of notable security events.
- **Event Log Storage** - Logs are stored online for ninety (90) days, and additional log data is stored off-line for nine (9) months.

Customer Console and Log Analysis Features

- **Customer Console** – A web-based portal that includes dashboards, threat analysis tools, Log analysis tools, Report system, asset information, and administrative functions to manage access. Includes support for a single company configuration.
- **Full Log Text Search & Analysis –** Full Log Search & Analysis - Provides the ability to do ad hoc full text searching for any piece of data captured within the log. Any search created can be saved or scheduled as a recurring report.
- **Event Log Reporting** – Predefined & pre-canned standard templates, custom ad-hoc query tool, creation of customized reports that can be delivered by an automated schedule.

1

- **Log Analytics Collection Appliance** - Physical or Virtual Data Collector Appliance(s) for a single customer data collection site. Any physical Data Collectors will be provided as a pair for redundancy unless otherwise noted.

Optional Services

- **Custom Log Sources -** Includes log sources that require the support of custom or proprietary log formats
- **Additional Log Storage -** Additional year of log retention storage (per year) Note: Purchased in one-year increments.
- **Multi-tenant Portal -** Provides the ability for an organization to have multiple individual "sub- portals" under a master portal. Individual portals can be configured to roll-up select data for a single organization with multiple divisions, departments, branches or units.
- **Additional Collector(s) –** Additional Physical or Virtual Data Collector for additional locations or for adding additional capacity.

DATA COLLECTION

During scoping and pricing, DeepSeas, working with the Customer, will identify system data sources that will be collected by the log analytics solution and mutually-agree on data collection architecture, that will include:

- The location of machine data collection servers to deploy to the Customer environment(s)
- The network communication and configuration requirements to enable the Customer's system data sources to be forwarded to data collection servers and API data collection targets
- A deployment strategy and timeline for Customer data collection

Customer's Data Collection Responsibilities

- The Customer agrees to provide physical or virtual servers to host DeepSeas data collection software. If, during Service Implementation or anytime thereafter, larger, or additional servers are determined necessary to meet the Service goals (e.g., outcomes), the Customer agrees to provide them.
- The Customer agrees to monitor the performance of log analytics data collection server resources including memory utilization, disk storage, and compute processing performance, and to alert DeepSeas when resource utilization exceeds 85%.

DeepSeas' Data Collection Responsibilities

- DeepSeas will monitor the performance of data collection software that is installed on the Customer- provided data collection servers.
- DeepSeas will monitor the frequency of machine data sources being received by data collection software against a monthly data volume ingestion baseline.

SERVICE ONBOARDING

DeepSeas will work with the Customer to create an implementation plan, that will consist of gathering and confirming relevant information, scoping, and deploying data collection architecture. Duration of deployment will vary based upon scope of data integration plan.

STEP	DESCRIPTION	ESTIMATED DURATION (WEEKS)
20. DESIGN	DeepSeas will document a data collection design that will define objectives, identify in-scope data sources, and determine data collection architecture.	1-2 weeks
21. DEPLOY	DeepSeas will collaborate with Customer to implement a data collection architecture by deploying collection devices, validating ingestion of sample data, and establishing secure connections to DeepSeas Log Analytics platform.	1-2 weeks
22. ONBOARD	DeepSeas will collaborate with Customer to onboard environment data and configure ingestion of enrichment and source data.	2-8 weeks

CUSTOMER RESPONSIBILITIES

a) Customer shall provide designated Authorized Contacts for the Services including designated primary, secondary, and tertiary contacts and shall provide Supplier with Customer's designated contact for maintenance, technical support, and escalation prioritization.
b) Customer shall supply authorized Customer Contact's information, inclusive of contact priority, phone number, cell number, e-mail address, position title, and any escalation path information relevant to Customer's environment (such as a distribution list, or default contact group for escalations).
c) Customer shall designate an individual for Unanswered Ticket escalation or problem escalation including full contact information.
d) Customer shall maintain current and up-to-date contact information regarding designated Authorized Contacts within the Supplier's Client Security Portal.
e) Customer shall inform DeepSeas service delivery manager of planned or recent network environment changed that may impact ongoing availability of event log source data.

1 SUPPORTED DATA SOURCES

The following data sources are supported by DeepSeas Log Analytics Platform. Support for additional data sources may be available by request or through custom integration.

Category	Type	Vendor	Version
Identity	Active Directory	Microsoft	Active Directory
Endpoint	Anti-Virus	Bitdefender	Bitdefender_AV
Endpoint	Anti-Virus	Cisco	CiscoACS_SOD
Endpoint	Anti-Virus	Cylance	Cylance
Endpoint	Anti-Virus	ESET	ESET_NOD32
Endpoint	Anti-Virus	ESET	ESET_NOD32
Endpoint	Anti-Virus	Network Associates Inc.	McAfee ePO
Endpoint	Anti-Virus	McAfee	McAfee UVScan
Endpoint	Anti-Virus	McAfee	McAfee_ePO
Endpoint	Anti-Virus	Sonicwall	Sonicwall Anti_Virus
Endpoint	Anti-Virus	Sophos	Sophos Anti-Virus
Endpoint	Anti-Virus	Trendmicro	Trendmicro Anti-Virus
Endpoint	Anti-Virus	Symantec	Crowdstrike
Endpoint	Anti-Virus	CrowdStrike	Symantec Anti-Virus Corporate Edition
Endpoint	File Integrity	Bromium	File Integrity
Endpoint	File Integrity	Carbon Black	Application Control
Endpoint	File Integrity	Trendmicro	Trendmicro FIM
Endpoint	File Integrity	Tripwire Inc	File Integrity
Endpoint	Host Intrustion & Prevention	Cisco	Cisco Security Agent
Endpoint	Host Intrustion & Prevention	Cisco	Cisco Security Agent
Endpoint	Host Intrustion & Prevention	CounterTack	Sentinel
Endpoint	Host Intrustion & Prevention	Infocyte	Hunt Server
Endpoint	Host Intrustion & Prevention	MobileIron	MBCore

1

Endpoint	Host Intrustion & Prevention	OSSEC	OSSEC Host IDS
Endpoint	Host Intrustion & Prevention	Sonicwall	Sonicwall HIPS
Endpoint	Host Intrustion & Prevention	Trendmicro	Trendmicro HIPS
Endpoint	Malware Protection	Cisco	AMP
Endpoint	Malware Protection	Fire_Eye	NX
Endpoint	Malware Protection	Fire_Eye	NX
Endpoint	Malware Protection	Fortinet	FortiSandbox
Endpoint	Malware Protection	Ivanti	Endpoint Security
Endpoint	Malware Protection	MalwareBytes	EndpointSecurity
Endpoint	Linux/Unix	Amazon Web Services	AWS Linux
Endpoint	Linux/Unix	Brother	Printer
Endpoint	Linux/Unix	Cisco	Cisco_UCS
Endpoint	Linux/Unix	Dell, Inc.	DELL_Server
Endpoint	Linux/Unix	Hewlett Packard	UNIX
Endpoint	Linux/Unix	IBM	AS400
Endpoint	Linux/Unix	IBM	ZOS
Endpoint	Linux/Unix	Linux	Linux
Endpoint	Linux/Unix	NetApp	OnTap Cluster
Endpoint	Linux/Unix	NetApp	OnTap Cluster
Endpoint	Linux/Unix	PureStorage	Purity NAS
Endpoint	Linux/Unix	QNAP	QNAP NAS
Endpoint	Linux/Unix	RedHat	RedHat Linux
Endpoint	Linux/Unix	Sun Microsystems	Solaris
Endpoint	Linux/Unix	SUSE	Suse Linux
Cloud	Azure	Microsoft	Azure_Administrative
Cloud	Azure	Microsoft	Azure_API_Management
Cloud	Azure	Microsoft	Azure_App_Insights
Cloud	Azure	Microsoft	Azure_Autoscale_Events
Cloud	Azure	Microsoft	Azure_Diagnostics_Events
Cloud	Azure	Microsoft	Azure_HDInsight

1

Cloud	Azure	Microsoft	Azure_IIS
Cloud	Azure	Microsoft	Azure_Key_Vault
Cloud	Azure	Microsoft	Azure_Kubernetes_Service_(AKS)
Cloud	Azure	Microsoft	Azure_Networking_Resources
Cloud	Azure	Microsoft	Azure_NSG_Flow_Logs
Cloud	Azure	Microsoft	Azure_OS_Logs
Cloud	Azure	Microsoft	Azure_Recommendation
Cloud	Azure	Microsoft	Azure_Security_Center
Cloud	Azure	Microsoft	Azure_Service_Alert
Cloud	Azure	Microsoft	Azure_Service_Health
Cloud	Azure	Microsoft	Azure_SQL_DB
Cloud	Azure	Microsoft	Azure_Storage_Analytics
Cloud	Azure	Microsoft	Azure_Subscription_Monitoring
Cloud	Azure	Microsoft	Azure_Virtual_Machines
Cloud	Azure	Microsoft	Azure_WAF
Cloud	AWS	Amazon Web Services	Cloud_Trail
Cloud	AWS	Amazon Web Services	Cloud_Watch
Cloud	AWS	Amazon Web Services	Config
Cloud	AWS	Amazon Web Services	Guard Duty
Web Gateway	Web Proxy	Barracuda	Barracuda_WF
Web Gateway	Web Proxy	Blue Coat Systems	BLUECOAT SG
Web Gateway	Web Proxy	Blue Coat Systems	BLUECOAT SG
Web Gateway	Web Proxy	Cisco	Cisco_WSA
Web Gateway	Web Proxy	Forcepoint	Email Gateway
Web Gateway	Web Proxy	Forcepoint	Web Security
Web Gateway	Web Proxy	Fortinet	FortiWeb
Web Gateway	Web Proxy	Iprism	Iprism_WF
Web Gateway	Web Proxy	IronPort	IronPort_ESA
Web Gateway	Web Proxy	IronPort	IronPort_WSA

1

Web Gateway	Web Proxy	McAfee	Email Gateway
Web Gateway	Web Proxy	McAfee	Web Gateway
Web Gateway	Web Proxy	Microsoft	Threat Management Gateway
Web Gateway	Web Proxy	PROOFPOINT	Email Security
Web Gateway	Web Proxy	Radware	DefensePro_DOS
Web Gateway	Web Proxy	Sonicwall	Web Gateway
Web Gateway	Web Proxy	Trendmicro	Web Gateway
Web Gateway	Web Proxy	Websense	Websense Enterprise
Web Gateway	Web Proxy	Websense	Websense Enterprise
Web Gateway	Web Proxy	Websense	Websense Enterprise
Web Gateway	Web Proxy	Zix	Email_Encryption
Web Gateway	Web Proxy	Zscaler	Nanolog
DNS	DNS	BlueCat Networks	BLUECAT
DNS	DNS	BlueCat Networks	BLUECAT
DNS	DNS	Cisco	CISCO
DNS	DNS	DNS Security	DNS
DNS	DNS	InfoBlox	InfoBlox
DNS	DNS	InfoBlox	InfoBlox
DNS	DNS	Simple_DNS	SDNS
DNS	DNS	Sonicwall	SONICWALL
DHCP	DHCP	DHCP Security	DHCP
DHCP	DHCP	Sonicwall	DHCP
Network	FireWall	Avantail	Avantail VPN
Network	FireWall	Amazon Web Services	Firewall
Network	FireWall	Barracuda	Barracuda_FW
Network	FireWall	Barracuda	VPN
Network	FireWall	Check Point	SOHO
Network	FireWall	Check Point	Checkpoint Firewall
Network	FireWall	Cisco	Meraki_FW
Network	FireWall	Cisco	Cisco VPN Concentrator

1

Network	FireWall	Cisco	ASA_PIX_FW
Network	FireWall	Clavister	VS
Network	FireWall	CloudCover	Barrier1
Network	FireWall	Forcepoint	Firewall
Network	FireWall	Fortinet	FortiGate FW
Network	FireWall	Hewlett Packard	HPFireWall
Network	FireWall	Microsoft	Internet Security and Acceleration Server
Network	FireWall	Juniper Networks	SSL VPN
Network	FireWall	Juniper Networks	JunOS
Network	FireWall	Netmotion	Mobility_VPN
Network	FireWall	Netscreen	Netscreen Firewall
Network	FireWall	Palo Alto Networks	Firewall
Network	FireWall	Arbor Networks	PeakflowSP
Network	FireWall	pfSense	SG Firewall
Network	FireWall	Secure Computing	SecureComputing Firewall
Network	FireWall	Sonicwall	Sonicwall Firewall
Network	FireWall	Sophos	Firewall
Network	FireWall	VMware	NSX
Network	FireWall	WatchGuard Technologies	Firebox
Network	FireWall	Zscaler	Nanolog
Network	Network Access Control	Armis	NAC
Network	Network Access Control	Enterasys	Enter_NAC
Network	Network Access Control	ForeScout	CounterACT
Network	Network Access Control	Trustwave	Mirage NAC
Network	NetFlow	Cisco	Cisco_Netflow
Network	NetFlow	VCloud	VPC_Netflow
Network	NetFlow	NETFLOW	NETFLOW
Network	NetFlow	AWS	VPC_Netflow
Network	NetFlow	Microsoft	Azure_NSG_Flow_Logs

1

Network	Network Detection and Response	Cisco	Cisco NIDS
Network	Network Detection and Response	CloudCover	Barrier1
Network	Network Detection and Response	DarkTrace	DCIP
Network	Network Detection and Response	DB Networks	DBN6300
Network	Network Detection and Response	Fortinet	Fortinet IPS
Network	Network Detection and Response	Fortinet	Fortinet IPS
Network	Network Detection and Response	Fortinet	Fortinet IPS
Network	Network Detection and Response	IBM	PROVENTIA
Network	Network Detection and Response	McAfee	Network IPS
Network	Network Detection and Response	Security Onion	SecOnion_IPS
Network	Network Detection and Response	Snort	SNORT IDs
Network	Network Detection and Response	Sourcefire	Sourcefire Intrusion Sensor
Network	Network Detection and Response	Tanium	Threat Response
Network	Network Detection and Response	TippingPoint	UnityOne
SaaS	O365	Microsoft	Office 365
SaaS	O365	Microsoft	Office365_Advance_Threat_Protection_(ATP)
SaaS	O365	Microsoft	Office365_Audit_events
SaaS	O365	Microsoft	Office365_Azure_AD
SaaS	O365	Microsoft	Office365_Azure_AD_Identity_Protection
SaaS	O365	Microsoft	Office365_DLP
SaaS	O365	Microsoft	Office365_Exchange
SaaS	O365	Microsoft	Office365_Graph_Security_API
SaaS	O365	Microsoft	Office365_Microsoft_Cloud_App_Security_(MCAS)
SaaS	O365	Microsoft	Office365_Microsoft_Teams

1

SaaS	O365	Microsoft	Office365_Share_Point
SaaS	O365	Microsoft	Office365_Sway
SaaS	O365	Microsoft	Office365_Threat_Detection
SaaS	O365	Microsoft	Office365_Yammer
Web Application Firewall	Web Application Firewall	Breach WAF	Breach WAF
Web Application Firewall	Web Application Firewall	Cloudflare	Cloudflare_WAF
Web Application Firewall	Web Application Firewall	F5 Networks	ASM
Web Application Firewall	Web Application Firewall	Imperva	SecureSphere WAF
Web Application Firewall	Web Application Firewall	ModSecurity	ModSecurity Firewall
Web Application Firewall	Web Application Firewall	Trustwave	WAF

MDR Service Levels

The following tables describe DeepSeas’ service level agreements (SLAs) and service level defaults:

THREAT NOTIFICATION SERVICE LEVEL AGREEMENTS

THREAT SEVERITY	DESCRIPTION	TARGET NOTIFICATION TIME*	TARGET SERVIC E LEVEL	MINIMUM NOTIFICATION TIME	MINIMUM SERVICE LEVEL
Level 1 **Critical**	• Could cause severe business impact/service disruption to critical services/systems • Risk potential includes financial, reputational, regulatory, legal, etc. • Targeted attack / attempts by internal or external parties • Repeated attempts to obtain or export unauthorized information or access • Generates public interest	<15 minutes	99.99%	30 minutes	99.5%
Level 2 **High**	• Major impact to multiple critical systems or services • Major impact to sensitive data • Multiple malware infections on internal network – 5 hosts and up – or suspected ransomware • Potential for public interest	<15 minutes	99.99%	30 minutes	99.5%
Level 3 **Moderate**	• Any infection beyond potentially unwanted program/adware • Malware infection on 1-4 hosts • Potential for service disruption on users	<1 hour	99.99%	2 hours	99.5%
Level 4 **Low**	• Impacts a single system or service • Impacts a non-critical enterprise system or service • Potential unfriendly or unintentional activity by internal or external parties	<1 hour	99.99 %	4 hours	99.5%

** Notification Time commences upon formal determination that an alert is a validated threat and input into the validated threat system.*

SERVICE LEVEL AGREEMENT DEFAULTS

SERVICE LEVEL DEFAULTS	CUSTOMER CREDIT

1

0-1	0% of monthly service charges for the Services
2-4	5% of monthly service charges for the Services
5-6	10% of monthly service charges for the Services
7 or more	15% of monthly service charges for the Services

Threat Severity Scale

DeepSeas' Cyber Defense Team identifies potential security threats in Customer environments using a combination of alert enrichment and review, open and closed source cyber threat intelligence, enterprise data search, and targeted cyber threat hunting. When DeepSeas identifies and validates a potential security threat in a monitored Customer environment, a Threat Notification report is documented and delivered to the Customer in alignment with a scaled threat severity model. Threat Notification reports are created in the form of a case event in the DeepSeas customer portal. Depending on the threat severity, direct contact is made in accordance with the Customer-provided notification escalation order, per the Customer MDR Runbook and as described below:

THREAT SEVERITY	THREAT DESCRIPTION	DEEPSEAS NOTIFICATION
Level 1 **Critical**	• Could result in severe business impact or service disruption to critical services or system(s) • Risk potential includes financial, reputational, regulatory, legal, etc. • Targeted attack/hack attempts by internal or external parties • Repeated attempts to obtain or export unauthorized information or access • Could have significant public impact	Within 30 minutes of detecting a critical validated threat, a DeepSeas cyber defense analyst will make direct contact with the Customer and create a case record in the customer portal. In the event a critical threat is detected and validated, the cyber defense analyst will deliver comprehensive updates to the Customer until the incident is contained using any mode of communication necessary or as preferred by the Customer.
Level 2 **High**	• Could result in a major impact to multiple critical services or systems • Risk potential includes major impact to sensitive data • Typically includes malware infections within the network on five or more hosts • Could have impact on the public	Within 60 minutes of threat declaration by a DeepSeas cyber defense analyst, the analyst will notify customer point of contact by phone and email, create a case in the customer portal. In the event a high threat is detected and validated, the analyst will deliver comprehensive updates to the Customer until the incident is contained using any mode of communication necessary or as preferred by the Customer.

1

Level 3 **Moderate**	• Defined as an infection beyond a potentially unwanted program/adware • Typically includes malware infections within the network on 1-4 hosts • Presents a potential for service disruption • Based primarily upon network traffic anomalies • Repeated violations of Customer's information Security Policies	Within 4 hours of threat declaration by a DeepSeas cyber defense analyst, the analyst will create a case in the customer portal and notify customer point of contact by email.
Level 4 **Low**	• Potential impact is on a single system or service • Impact detected is on a non-critical enterprise system or service • Potentially unwanted or unintentional activity by internal or external parties • Activity violates Customer's Information Security Policies • Threat Notification reports will be delivered to the Customer based upon potential Customer and public impact	Within 4 hours of threat declaration by a DeepSeas cyber defense analyst, the analyst will create a case in the customer portal and notify customer point of contact by email.

Network MDR – Service Description

SERVICE OVERVIEW

DeepSeas' Network Managed Detection and Response Service ("Network MDR") provides 24x7x365 network threat detection, analysis, and response to validated threats. Network MDR leverages the deployment of network intrusion detection technology onto the Customer's network to securely monitor network traffic for malicious activity. Suspicious observations are delivered to the DeepSeas' cloud-hosted defense platform for triage and analysis. DeepSeas will work with the Customer during the service initiation phase to install, configure, and validate network data collection.

Our Network MDR solution leverages DeepSeas' patented out-of-band, full-packet capture and inspection network sensors (physical and/or virtual) that provide static, analytic-based monitoring and detection. This capability enables recursive file carving, Yara-based detection, and comprehensive metadata analysis. Sensors deployed on the network are available in three sizes – 500 Mbps, 1 Gbps and 10 Gbps – and can be installed behind a firewall or other perimeter security prevention technology. Comprehensive network coverage may also include sensors deployed within internal network demarcation points to monitor east/west (internal) network activity. To optimize intrusion detection, the sensor type and positioning within a Customer's network shall be determined upon review of the customer's operational environment by a DeepSeas solutions architect.

Our MDR program includes the following service elements:

- **Threat Detection** - DeepSeas threat detection provides review of alerts from, proactive enterprise search of, and targeted threat hunting using Customer security monitoring tools to identify and prioritize cyber threats.
- **Threat Notification** - Threat Notification reports are generated by DeepSeas cyber defense analysts to describe the nature, context, and severity of a validated threat along with remediation recommendations.
- **Threat Response** - DeepSeas cyber defense analysts provide Customers with response guidance and/or response actions for resolving threats. Response actions are defined in a mutually approved Customer MDR Runbook document.
- **Curated Threat Intelligence** – DeepSeas applies curated detection logic and analytics to security monitoring tools deployed in customer networks to improve the effectiveness of threat detection and response.
- **DeepSeas XDR Cyber Defense Platform -** DeepSeas XDR Cyber Defense Platform provides customers with a cloud-hosted technology architecture that supports data collection, analysis, automated response, and reporting capabilities across multiple attack surfaces.

1

Should a threat be identified on an endpoint within the Customer's network environment, a Validated Threat Notifications report will be sent to the Customer and will include severity level, vector information, and recommended response actions to mitigate the threat

SUPPORTED TECHNOLOGIES AND LICENSING OPTIONS

The DeepSeas Network Sensor is available as both a physical on-prem appliance or as a virtual machine. We also support DARKTRACE sensors, provided the Customer procures the appliances directly from them and Customer retains responsibility for maintenance.

Our network sensors can be licensed through one of two options:

- Licensing Option 1 (most common): The Customer can elect to lease network sensor(s), whereby DeepSeas will perform all required maintenance at no cost to the Customer. In this instance, the Customer agrees to support DeepSeas in performing maintenance when on-site presence is required at a Customer facility.
- Licensing Option 2: The Customer can elect to purchase Network Sensor Appliances directly, inheriting the manufacturer's warranty. In this instance, Customer would agree to perform any necessary maintenance to ensure the appliance is performing adequately to ensure monitoring and reporting outcomes can be met; or

LIST OF SUPPORTED NETWORK SENSOR TECHNOLOGIES

PLATFORM	SUPPORT COMPONENTS			LICENSING OPTIONS
	Cloud Version	On-Premises Version	Curated Threat Intel	
DeepSeas Network Sensor	No	Yes	Yes	• Lease Through DeepSeas • Purchase From DeepSeas
DARKTRACE™	Yes	Yes	Yes	• Lease or Purchase Directly From DARKTRACE

THREAT RESPONSE

During onboarding, DeepSeas will work closely with Customer stakeholders to jointly develop a Customer MDR Runbook, which will detail individual responsibilities for responding to Threat Notifications delivered by DeepSeas. Response actions are typically categorized as one of the following:

RESPONSE TYPE	DESCRIPTION
GUIDED RESPONSE	Guided Threat Response provides customers with recommended response actions that the Customer's internal team should complete to contain, mitigate, or remove a threat identified in a DeepSeas Threat Notification.
PROACTIVE RESPONSE	DeepSeas can perform select threat containment response actions based upon the Statement of Work. Active Response actions may be combined with Guided Response actions to facilitate incident resolution. Example proactive response capabilities include server quarantine, proxy modification, firewall modification, and custom API integrations.
BREACH RESPONSE	Upon activation of a pre-negotiated Incident Response retainer, DeepSeas will provide dedicated and (as needed) on-site investigation, triage, recovery, and remediation.

SERVICE ONBOARDING TIMELINE

The following table describes the typical steps DeepSeas undertakes together with the Customer to onboard and initialize our Network MDR service

STEP	DESCRIPTION	ESTIMATED DURATION (WEEKS)
23. Kick-Off	DeepSeas and the Customer will participate in a joint call to confirm services, network sensor specifications, shipping information, definition of a Customer MDR Runbook, and other key details regarding the Services to be provide. At the Kick-Off, the Customer is introduced to their Technical Support Engineer (TSE) / Service Delivery Manager (SDM).	<1 WEEK
24. Shipping	DeepSeas will coordinate the shipping of network sensors to the Customer's location(s). Shipping times vary based on location and range from 2 days+ for U.S. domestic locations and up to 30+ days for international locations. International shipments requiring Importer of Record (IOR) coordination with the Customer which may delay shipping timelines.	<2 WEEKS (DOMESTIC) 4+ WEEKS (INTERNATIONAL)
25. Network Sensor Installation and Traffic Validation	DeepSeas will work with the Customer regarding scheduling of installation of Network Sensors with DeepSeas, providing support and guidance by either email or phone. Installation includes allowing connectivity to DeepSeas' data center(s) through any firewalls; racking the appliance(s); inputting appropriate	<1 WEEK

1

	IP addresses and customer IDs; testing; and rebooting. After validating successful sensor functionality, DeepSeas will capture and validate network traffic from the installed network sensor. Network traffic will be reviewed with the Customer to ensure the network sensor has the appropriate visibility thereby ensuring service outcomes can be met.	
26. Baseline	DeepSeas will begin monitoring the network sensor alerts and begin notifying the Customer of validated threats while creating a baseline for priorities, focus, and response.	<1 WEEK
27. Service Optimization and ‘Go Live’	DeepSeas monitoring services are fully operational and adjusted as needed to meet Customer needs. DeepSeas provides reports and on-going communication to the Customer.	4+ WEEKS

OT MDR – Service Description[5]

SERVICE OVERVIEW

DeepSeas' Operational Technology (OT) Managed Detection and Response Service ("OT MDR") provides 24x7x365 threat detection, analysis, and response to verified threats. Threats are detected and verified by the DeepSeas cyber defense analysts by reviewing alerts from an OT threat detection technology installed on Customer's (or the Customer's 3rd party) OT network. Threat detection includes monitoring of alerts by DeepSeas cyber defense analysts who triage, examine, and categorize alerts generated from a specified OT Security Technology.

DeepSeas has developed a library OT specific threat detection analytics that power alerts, dashboards, and reports within DeepSeas' Cyber Defense Platform to enable increased contextualization of the validated threat notifications and related reports. DeepSeas will update and tune OT threat detection analytics as necessary to meet the service outcomes defined by working with the Customer. As part of its OT MDR service DeepSeas will also provide an OT specific Customer MDR Runbook that describes general remediation recommendations to specific categories of OT threats. During the initial scoping discussions DeepSeas, in working with the Customer, will identify one or more Customer points of contact who will be responsible for response to Validated Threat Notifications that are created by DeepSeas.

Our OT MDR program includes the following service elements:

- **Validated Threat Notifications:** Contextualized, prioritized, and actionable notification of cyber security threats that align ownership and enable clear action
- **OT Security Asset Inventory:** An inventory report that details OT assets in Customer monitored OT environments. OT Asset Inventory enables increased context and understanding of OT environments.
- **OT Security Risk Reports**
  - *Vulnerability Risk Reports:* A report that describes OT asset vulnerabilities and severity based upon asset visibility and threat intelligence.
  - *Process Integrity Risk Reports:* Reports that will leverage data from passive OT monitoring tools to provide customer with OT process integrity information.
  - *Site Risk Profile Reports:* A report that will provide Customer OT site staff with ta summary of security risks related to a specific OT site location.

[5] OT = Operational Technology

SUPPORTED OT TECHNOLOGIES

We support three industry-leading OT technologies and two licensing options, as shown below:

LIST OF SUPPORTED OT PASSIVE MONITORING PRODUCTS				
	SUPPORT COMPONENTS			
PLATFORM	Cloud Version	On-Premises Version	Curated Threat Intel	LICENSING OPTIONS
Claroty™	Customer Managed	DeepSeas Managed	DeepSeas Managed	● Bring Your Own License[6] ● Purchase Through DeepSeas [7]
Armis™	Customer Managed	DeepSeas Managed	DeepSeas Managed	● Bring Your Own License ● Purchase Through DeepSeas
Nozomi Networks™	Customer Managed	DeepSeas Managed	DeepSeas Managed	● Bring Your Own License

DATA INTEGRATION

Our service collects security monitoring data from an Application Programming Interface ("API") specific to the OT Passive Monitoring Tool chosen and collects relevant data. This capability enables specified collection and (as applicable) response actions within the Customer's OT environment. Additionally, DeepSeas has the capability to leverage additional data sources that may already exist within the environment to help contextualize the data from the OT Passive Monitoring tool and provide Customer tailored dashboards and reports to enable cyber awareness within the site environment. During the

[6] Bring Your Own License - Customer can elect to purchase a supported platform through the supplier of their choice. Customer owns licensing and any associated fees.

[7] Purchase Through DeepSeas - Customer can elect to purchase certain SIE licenses

scoping and pricing discussions, DeepSeas, in coordination with the Customer will identify any additional specific OT security data sources that could enable further contextualization of the OT Passive Monitoring Tools (e.g. OT firewall data) within the Cyber Defense Platform.

THREAT RESPONSE

During onboarding, DeepSeas will work closely with Customer stakeholders to jointly develop a Customer MDR Runbook, which will detail individual responsibilities for responding to Threat Notifications delivered by DeepSeas. Response actions are typically categorized as one of the following:

RESPONSE TYPE	DESCRIPTION
GUIDED RESPONSE	Guided Threat Response provides customers with recommended response actions that the Customer's internal team should complete to contain, mitigate, or remove a threat identified in a DeepSeas Threat Notification.
PROACTIVE RESPONSE	DeepSeas will perform specific threat containment response actions based upon the Statement of Work. Active Response actions may be combined with Guided Response actions to facilitate incident resolution. Example proactive response capabilities include system containment, proxy modification, firewall modification, and custom API integrations.
BREACH RESPONSE	Upon activation of a pre-negotiated Incident Response retainer, DeepSeas will provide dedicated and (as needed) on-site investigation, triage, recovery, and remediation.

SERVICE ONBOARDING TIMELINE

DeepSeas will work with the Customer to create an implementation plan, that will consist of gathering and confirming relevant information, scoping, and deploying SIEM data collection architecture, implementing SIEM Rules and Use Cases and service activation.

STEP	DESCRIPTION	ESTIMATED DURATION (WEEKS)
28. Assess	DeepSeas and the Customer will conduct a series of workshops to understanding the existing OT environment. This will include topics such as existing OT security data sources, key stakeholders, skills needed to respond to validated threats within the OT environment	2-3 WEEKS

1

29. OT Passive Monitoring Tool	If not already in place the Customer will deploy the OT passive monitoring tool and the centralized management console to the identified locations with the OT network to enable threat detection. Integration is confirmed when telemetry data flow from the OT Passive Monitoring Tool is established from the appliance(s) to DeepSeas.	4+ WEEKS (depending on number of sites)
30. Baseline	As the data is integrated into DeepSeas Cyber Defense Platform, the DeepSeas Cyber Defense Team will begin monitoring the OT threat detection alerts and begin notifying the Customer of validated threats while creating a baseline for priorities, focus, and response.	5+ WEEKS (depending on number of sites)
31. Enhance	If additional data sources were identified during the assess step, DeepSeas will work with the Customer to onboard that data and configure ingestion of enrichment and source data.	6 WEEKS
32. Managed Operations	DeepSeas will provide Customer with remote services that deliver essential response actions as agreed on in customer contract.	ONGOING

Penetration Testing – Service Description

SERVICE OVERVIEW

DeepSeas' Penetration Testing (Pen Test) service delivers internal, external, web application or social engineering penetration testing that is designed to identify and exploit vulnerabilities within Customer's network. Our team of industry-certified practitioners will replicate current, sophisticated tactics, techniques, and procedures (TTPs) and leverage a mix of open-source, commercial and custom tools to identify system weaknesses. Our Pen Testers will then apply their technical expertise to exploit those flaws. Vulnerabilities identified will be validated through exploitation, and any identified compromised systems will be utilized to leverage additional attacks (exploit chains). This will provide a cost effective and efficient method for reviewing the security posture of Customer's internal systems

Together, DeepSeas and Customer will work to ensure that testing will be performed with minimal disruption to Customer's ongoing mission-critical operations. After completing a comprehensive test, our team of security professionals will submit a detailed report listing findings and recommendations.

SERVICE DELIVERY

DeepSeas' Pen Test service comprises a three-phased approach:

1) Test Planning & Rules of Engagement
2) Testing execution; and
3) Analysis & Reporting

Phase 1 – Test Planning & Rules of Engagement

In this initial phase, the DeepSeas team will work with Customer to define the objectives of the testing process and to develop a rules of engagement (ROE) document. The ROE details testing limitations, boundaries, and constraints; as well as definitions of valid targets, valid tests, reporting procedures, and test completion criteria. The ROE also details points of contact and other test administrative details. Information for the ROE will be gathered during an initial Technical Interchange Meeting (TIM) with Customer that will kick off the engagement. Using the information collected, DeepSeas will draft a ROE document and submit it to the designated Customer personnel for approval.

DeepSeas will use the results of this step to refine the testing goals and document the types of penetration techniques that the team will use. We will also describe the safeguards to prevent against accidental interference with Customer systems, as well as identify ways that these authorized attacks can be distinguished from malicious attacks that may occur during the execution of the penetration test. The information collected will be submitted with the date and time of the penetration test along with the IP addresses from which testing will be conducted. The testing team will hold a kick-off briefing via teleconference and use the meeting to address logistical planning and any desired modifications to the test plan.

Phase 2 – Test Execution

The DeepSeas' Penetration Testing team will begin executing internal penetration testing from the perspective of a compromised user or a malicious actor. Our methodology for internal testing consists of two steps: i) Discovery; and ii) Attack & Exploitation.

Discovery: DeepSeas will map Customer's environment and identify potential vulnerabilities by performing extensive data gathering through network and application scanning. We will leverage traditional tactics with open-source intelligence gathering around a targeted component in order to uncover any known vulnerabilities and gain additional insight into Customer's security posture.

Attack & Exploitation: Following the identification of a vulnerability, the Pen Test team will attempt to exploit discovered vulnerabilities to validate that it is both present and exploitable. The Pen Test team will attempt to move laterally through the network and determine what information is accessible from a successful compromise using the processes and limitations documented and agreed to in the ROE. We leverage hundreds of verified exploits and popular libraries such as Metasploit, Exploit-DB, SecurityFocus, in addition to proprietary knowledge, when conducting security tests. During the exploitation phase of testing, our team will work in full cooperation with Customer technical personnel using the processes and limitations documented in the ROE. The primary goal of the simulated attacks will be to gain administrative privileges or escalate user privileges, access an operating system command line, or access sensitive data. When a vulnerability is successfully exploited, granting the test team unauthorized access to a resource (e.g., system, file, software, or software library), the Pen Test team will immediately stop testing the exploited system. Only the Customer program manager or a designee can authorize continued exploitation.

Phase 3 – Analysis & Reporting:

All testing activities will be recorded and available to Customer through system logs and practitioner documentation. This information will be available during the test to both the test team and to Customer POCs. This data will be used to analyze the findings and complete testing reports, including spot and final reports. artifacts, visual evidence, and other associated documentation.

DeepSeas will apply a risk-focused approach for each of our findings in order to establish residual risk ratings. These risk ratings will be calculated using guidance from NIST 800-30 and will take into consideration the likelihood and impact of the vulnerability or control deficiency. The likelihood evaluation will take into consideration the threat source's motivation and capability, the nature of the control, as well as the effectiveness of any existing compensating controls that may reduce the overall potential for exploitation. The impact analysis will take into consideration the mission of the system, its data and criticality, the sensitivity of the data processed, and any other potential for loss from a confidentiality, integrity, and availability perspective. Upon deriving the likelihood and impact ratings, DeepSeas will establish a risk rating for all findings identified in the penetration testing process.

DELIVERABLES

The following table lists the deliverables DeepSeas will provide to Customer:

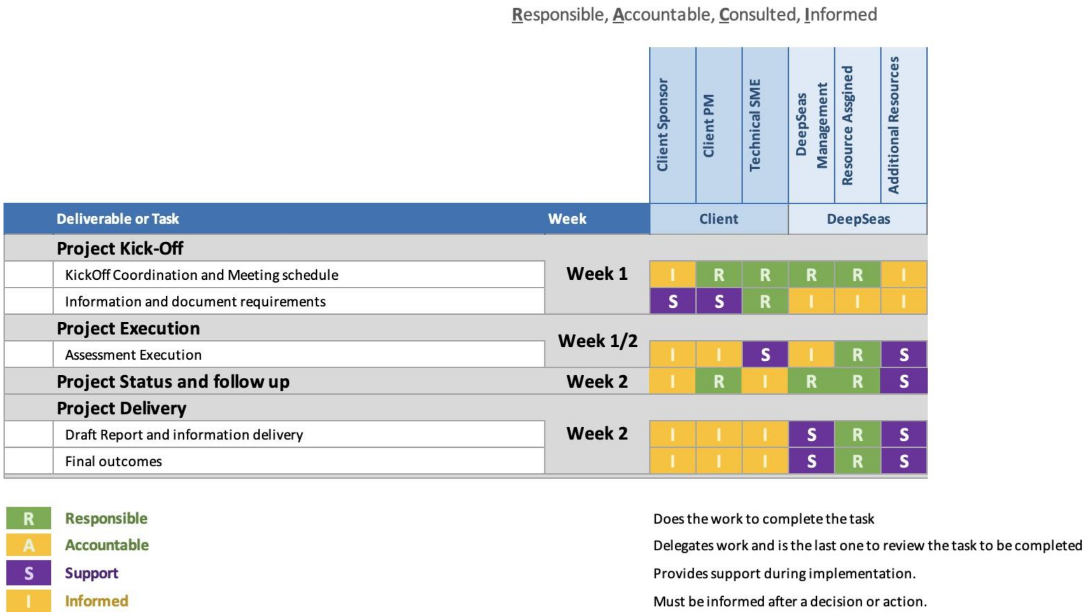
DELIVERABLE	DESCRIPTION	DOCUMENT FORMAT
RULES OF ENGAGEMENT (ROE)	A procedural document establishing guidelines for all testing activities and detailing the scope of the engagement. It will include all activities to be performed, the outputs to be produced, and any potential testing constraints.	MS Word
DETAILED PEN TEST FINDINGS REPORT	Provides details on discovered vulnerabilities, including a description, potential impact, technical and programmatic recommendations, host identified, and common vulnerability reference(s).	MS Word or MS Excel PDF File
EXECUTIVE PRESENTATION	A final executive-level overview of the testing activities performed given to key Customer stakeholders. A summary of findings will be presented and significant, high risk issues will be highlighted for additional discussion.	MS PowerPoint
RETEST FINDINGS REPORT	Every penetration testing assessment will include a re-test assessment of CRITICAL and HIGH findings presented on the final report. This re-test assessment can be executed up to 30 days after delivery of the primary test report.	Update on initial MS Word file

DELIVERABLE ACCEPTANCE

Customer shall have five (5) business days from its receipt of a Deliverable provided by DeepSeas to review, evaluate, and provide feedback or acceptance. If no written acceptance or rejection is received by DeepSeas, the Deliverable shall be deemed to be accepted.

Shared Responsibilities Model

1



Responsible, Accountable, Consulted, Informed

Deliverable or Task	Week	Client Sponsor	Client PM	Technical SME	DeepSeas Management	Resource Assgined	Additional Resources
		Client			DeepSeas		
Project Kick-Off							
KickOff Coordination and Meeting schedule	Week 1	I	R	R	R	R	I
Information and document requirements		S	S	R	I	I	I
Project Execution	Week 1/2						
Assessment Execution		I	I	S	I	R	S
Project Status and follow up	Week 2	I	R	I	R	R	S
Project Delivery							
Draft Report and information delivery	Week 2	I	I	I	S	R	S
Final outcomes		I	I	I	S	R	S

R	Responsible	Does the work to complete the task
A	Accountable	Delegates work and is the last one to review the task to be completed
S	Support	Provides support during implementation.
I	Informed	Must be informed after a decision or action.

DeepSeas Responsibilities:

a) Work with the client on the definition of the schedules, and approve for the execution period and days for the execution of tasks.

b) Definition of the specialized task force and consultants for the execution of the tasks indicated in the RACI model.

c) Identify risk factors that may jeopardize the correct execution of the processes, tasks, activities, and final deliverables of the project.

d) Monitoring of general activities, specific activities based on the service contracted by the client, deviations from activities, and follow-up plans.

e) Requests for general and additional requirements for the execution of the tasks and activities of each contracted service.

f) Coordination of specific work sessions for the activities contracted by the client.

g) Delivery of the reports and partial and final reports of the services contracted by the client.

Client Team Responsibilities

a) Work with DeepSeas consultants to schedule the execution of the activities associated with the contracted services in a way that does not impact the client's essential services of its daily operations.

b) Attend meetings and working sessions scheduled by DeepSeas, which include, but are not limited to:

- Kickoff
- Request for requirements

- Clarification of doubts and understanding of requirements
- Project monitoring
- Project deviations
- Partial project deliveries
- Final project deliveries

c) Assess and accept the risk factors that harm the correct execution of the contracted services identified by DeepSeas.

d) Internal coordination of meetings with internal areas (of the client) that must be involved within the associated activities per service.

e) Delivery of requirements requested by DeepSeas for the correct execution of the activities of the services contracted and defined.

f) Assist or delegate to third parties the attendance at the work sessions coordinated by DeepSeas, for the execution, investigation, assessments, and delivery of activities associated with the contracted services.

g) Acceptance of partial or final reports by DeepSeas.

Security Tools Effectiveness Assessment – Service Description

SOLUTION OVERVIEW

DeepSeas' Security Tools Effectiveness Assessment (STEA) offers a comprehensive evaluation of Customers' cyber defense controls against an extensive catalog of simulated attacks to reveal potential security weaknesses within a customer's environment. Offered as either a short-term assessment or as an ongoing managed service, STEA is designed to test endpoint security from an attacker's perspective by mimicking real-world attacks in a test environment, providing complete visibility into which events are blocked, detected & alerted, logged and/or not logged. The results are then scored and mapped to the MITRE ATT&CK framework and compiled into detailed reports to inform strategic decision-making and prioritization of future cyber initiatives.

Our STEA is typically conducted over an 8-week timeframe and delivers the following outcomes:

- **Detection/Prevention Control Testing** – Proactive discovery of deficiencies in logging and/or reporting events to SIEM, development of endpoint security checks and documentation of baseline controls to meet TDO and Customer needs.
- **Deep Understanding of Controls** – Enablement of both automatic and manual testing to ensure that simulated attacks correctly trigger blocks or alerts as intended.
- **Security Operation IT Infrastructure Testing** – Development of high-fidelity signatures and patterns recognition without generating false positive alerts when deploying new detection use cases.
- **Detection Content Validation** – Verification of detection controls and customer use cases to maximize defensive posture and support regulatory compliance requirements.
- **Audit/Compliance Reporting** – Periodic, formal threat and risk assessments for critical systems to validate security controls with documentation for audit purposes.
- **Improved Strategic Planning** – Enablement of superior prioritization of cyber initiatives based on value and risk, guided by assessment results.

DELIVERY TIMELINE

Our STEA solution is delivered on time frame from 3 to 8-week execution windows, depending of the requirements and scope of the project comprising the following three steps:

STEP	DESCRIPTION	ESTIMATED DURATION
4. **TECHNOLOGY DEPLOYMENT & PREPAREDNESS**	• Kick-off meeting, architecture review, and baselining of existing controls • Issue dissolvable third-party simulation agent to Customer on standard image test platform • Decide threat actors/TTPs to simulate • Execute test and prepare campaigns	1 - 2 weeks
5. **DISCOVERY & BENCHMARKING**	• Execute simulated campaigns to test baseline controls agreed upon in Step 1 • Review logs and alerts across platforms to confirm detection/prevention • Establish whitelists in close coordination with Customer	2- 5 weeks
6. **REFINE, MEASURE & REPORT**	• Integrate updated simulation campaigns aligned to threat priorities as they change • Re-testing and audit compliance reporting • Prepare and deliver a comprehensive report (“Deliverable”) on Customer’s overall cyber posture	1 - 2 weeks

DELIVERABLES

As part of our STEA, DeepSeas will provide Customer with the following:

DELIVERABLE	DESCRIPTION	DOCUMENT FORMAT
PROJECT PLAN	Project Plan document will be produced that will detail status reporting, pulse check, working session and draft and final deliverable schedules.	MS PowerPoint
WEEKLY STATUS CALLS	Weekly status calls will be held on day(s)/time(s) mutually agreed to by DeepSeas and Customer.	Phone Call / Tele-Meeting
DRAFT STEA REPORT	Parties meet to discuss findings from the Security Tools Effectiveness Assessment to ensure relevance accuracy prior to finalizing the Final Report.	MS Word
FINAL STEA REPORT	Final Report that will include an executive summary of findings,	PDF

	detailed technical analysis of findings, and actionable recommendations to improve detection.	

DELIVERABLE ACCEPTANCE

Customer shall have five (5) business days from its receipt of a Deliverable provided by DeepSeas to review and evaluate such Deliverable to determine whether the Deliverable substantially conforms with the specifications for the particular Deliverable as set forth herein, if any; and if no written acceptance or rejection is received by DeepSeas within such five (5) business day period, the Deliverable shall be deemed to be accepted.

DeepSeas Responsibilities:

a) Work with the client on the definition of the schedules, and approve for the execution period and days for the execution of tasks.
b) Definition of the specialized task force and consultants for the execution of the tasks indicated in the RACI model.
c) Identify risk factors that may jeopardize the correct execution of the processes, tasks, activities, and final deliverables of the project.
d) Monitoring of general activities, specific activities based on the service contracted by the client, deviations from activities, and follow-up plans.
e) Requests for general and additional requirements for the execution of the tasks and activities of each contracted service.
f) Coordination of specific work sessions for the activities contracted by the client.
g) Delivery of the reports and partial and final reports of the services contracted by the client.

Client Team Responsibilities

a) Work with DeepSeas consultants to schedule the execution of the activities associated with the contracted services in a way that does not impact the client's essential services of its daily operations.
b) Attend meetings and working sessions scheduled by DeepSeas, which include, but are not limited to:
    - Kickoff
    - Request for requirements
    - Clarification of doubts and understanding of requirements
    - Project monitoring
    - Project deviations
    - Partial project deliveries
    - Final project deliveries

c) Assess and accept the risk factors that harm the correct execution of the contracted services identified by DeepSeas.

d) Internal coordination of meetings with internal areas (of the client) that must be involved within the associated activities per service.

e) Delivery of requirements requested by DeepSeas for the correct execution of the activities of the services contracted and defined.

f) Assist or delegate to third parties the attendance at the work sessions coordinated by DeepSeas, for the execution, investigation, assessments, and delivery of activities associated with the contracted services.

g) Acceptance of partial or final reports by DeepSeas.

SIEM MDR – Service Description[8]

SERVICE OVERVIEW

DeepSeas' SIEM Managed Detection and Response ("SIEM MDR") service delivers 24x7x365 event analysis and supervised response to validated threats. Our Cyber Defense Team detects threats by reviewing alerts from one or more system event log aggregation servers installed on the Customer's (or the Customer's third party) network.

DeepSeas will deploy a core set of alerting rules and analytics ("SIEM Rules") to enable increased contextualization of the Customer's machine data. DeepSeas will update and tune SIEM Rules as necessary to meet the Service goals (e.g., outcomes).

As a managed detection and response-based service provider, DeepSeas uses Endpoint Detection and Response (EDR) technology and Network Detection and Response (NDR) technology as primary threat detection methods. SIEM Rules are used by the DeepSeas to contextualize and enrich endpoint and network alerts.

As determined necessary to meet the service goals (i.e., outcomes), DeepSeas will deploy SIEM Rule correlation logic ("SIEM Use Cases") which will be used by the DeepSeas Cyber Defense Team as a primary threat detection alerts.

Our MDR program includes the following service elements:

- **Threat Detection** - DeepSeas threat detection provides review of alerts from, proactive enterprise search of, and targeted threat hunting using Customer security monitoring tools to identify and prioritize cyber threats.
- **Threat Notification** - Threat Notification reports are generated by DeepSeas cyber defense analysts to describe the nature, context, and severity of a validated threat along with remediation recommendations.
- **Threat Response** - DeepSeas cyber defense analysts provide Customers with response guidance and/or response actions for resolving threats. Response actions are defined in a mutually approved Customer MDR Runbook document.
- **Curated Threat Intelligence** – DeepSeas applies curated detection logic and analytics to security monitoring tools deployed in customer networks to improve the effectiveness of threat detection and response.
- **DeepSeas XDR Cyber Defense Platform -** DeepSeas XDR Cyber Defense Platform provides customers with a cloud-hosted technology architecture that supports data collection, analysis, automated response, and reporting capabilities across multiple attack surfaces.

[8] SIEM = Security Information & Event Monitoring

Should a threat be identified on an endpoint within the Customer's network environment, a Validated Threat Notifications report will be sent to the Customer and will include severity level, vector information, and recommended response actions to mitigate the threat.

SUPPORTED SIEM TECHNOLOGIES

We support three industry-leading SIEM platforms and two licensing options, as detailed below:

LIST OF SUPPORTED SIEM TECHNOLOGIES

PLATFORM	SUPPORT COMPONENTS			LICENSING OPTIONS
	Cloud Version	On-Premises Version	Curated Threat Intel	
Splunk Cloud™ Enterprise Security Application	Customer Managed	DeepSeas Managed	DeepSeas Managed	• Purchase Through DeepSeas [9] • Bring Your Own License[10]
Securonix;™ Cloud	Customer Managed	DeepSeas Managed	DeepSeas Managed	• Purchase Through DeepSeas • Bring Your Own License
Microsoft Sentinel™	Customer Managed	DeepSeas Managed	DeepSeas Managed	• Bring Your Own License

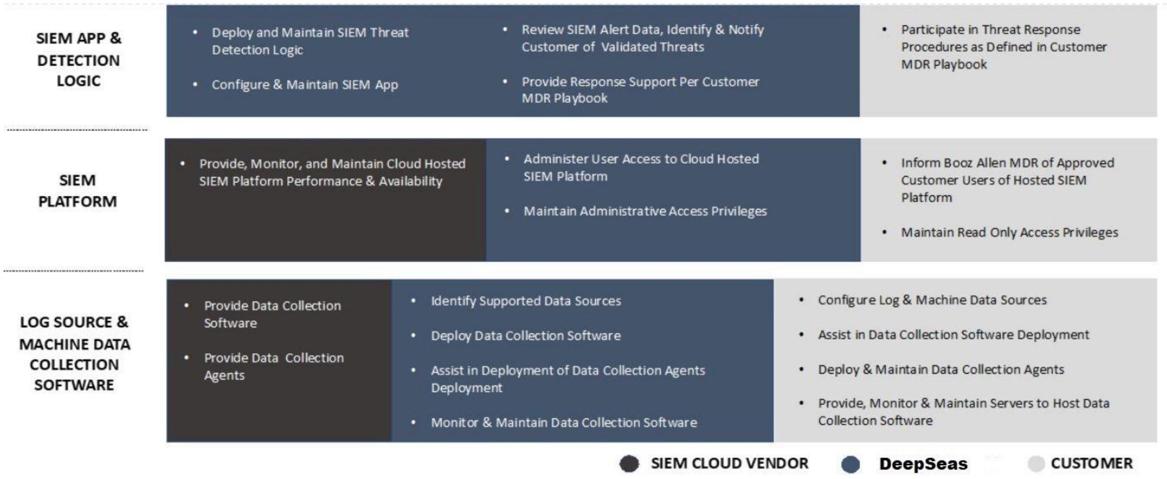
SIEM MDR SHARED RESPONSIBILITIES

The following graphic summarizes the respective and/or shared responsibilities between DeepSeas, the Customer, and the SIEM cloud vendor:

[9] Purchase Through DeepSeas - Customer can elect to purchase certain SIEM licenses.

[10] Bring Your Own License - Customer can elect to purchase a supported platform through the supplier of their choice. Customer owns licensing and any associated fees.

1



SIEM APP & DETECTION LOGIC		• Deploy and Maintain SIEM Threat Detection Logic • Configure & Maintain SIEM App • Review SIEM Alert Data, Identify & Notify Customer of Validated Threats • Provide Response Support Per Customer MDR Playbook	• Participate in Threat Response Procedures as Defined in Customer MDR Playbook
SIEM PLATFORM	• Provide, Monitor, and Maintain Cloud Hosted SIEM Platform Performance & Availability	• Administer User Access to Cloud Hosted SIEM Platform • Maintain Administrative Access Privileges	• Inform Booz Allen MDR of Approved Customer Users of Hosted SIEM Platform • Maintain Read Only Access Privileges
LOG SOURCE & MACHINE DATA COLLECTION SOFTWARE	• Provide Data Collection Software • Provide Data Collection Agents	• Identify Supported Data Sources • Deploy Data Collection Software • Assist in Deployment of Data Collection Agents Deployment • Monitor & Maintain Data Collection Software	• Configure Log & Machine Data Sources • Assist in Data Collection Software Deployment • Deploy & Maintain Data Collection Agents • Provide, Monitor & Maintain Servers to Host Data Collection Software

● SIEM CLOUD VENDOR ● DeepSeas ● CUSTOMER

DATA COLLECTION

During scoping and pricing, DeepSeas, working with the Customer, will identify system data sources that will be collected by the SIEM solution and mutually-agree on a Security Information and Event Management deployment architecture, that will include:

- The location of machine data collection servers to deploy to the Customer environment(s)
- The network communication and configuration requirements to enable the Customer's system data sources to be forwarded to data collection servers and cloud hosted SIEM platform
- A deployment strategy and timeline for Customer data collection

Customer's Data Collection Responsibilities

- The Customer agrees to provide physical or virtual servers to host SIEM data collection software, as well as data collection agents (as needed) to be deployed to endpoint data sources as determined necessary to meet the Service goals (e.g., outcomes). If, during Service Implementation or anytime thereafter, larger, or additional servers are determined necessary to meet the Service goals (e.g., outcomes), the Customer agrees to provide them.
- The Customer agrees to monitor the performance of SIEM data collection server resources including memory utilization, disk storage, and compute processing performance, and to alert DeepSeas when resource utilization exceeds 85%.

DeepSeas' Data Collection Responsibilities

- DeepSeas will monitor the performance of SIEM data collection software that is installed on the Customer- provided data collection servers.
- DeepSeas will monitor the frequency of machine data sources being received by SIEM collection software against a monthly data volume ingestion baseline.

1

THREAT RESPONSE

During onboarding, DeepSeas will work closely with Customer stakeholders to jointly develop a Customer MDR Runbook, which will detail individual responsibilities for responding to Threat Notifications delivered by DeepSeas. Response actions are typically categorized as one of the following:

RESPONSE TYPE	DESCRIPTION
GUIDED RESPONSE	Guided Threat Response provides customers with recommended response actions that the Customer's internal team should complete to contain, mitigate, or remove a threat identified in a DeepSeas Threat Notification.
PROACTIVE RESPONSE	DeepSeas will perform specific threat containment response actions based upon the Statement of Work. Active Response actions may be combined with Guided Response actions to facilitate incident resolution. Example proactive response capabilities include system containment, proxy modification, firewall modification, and custom API integrations.
BREACH RESPONSE	Upon activation of a pre-negotiated Incident Response retainer, DeepSeas will provide dedicated and (as needed) on-site investigation, triage, recovery, and remediation.

SERVICE ONBOARDING TIMELINE

DeepSeas will work with the Customer to create an implementation plan, that will consist of gathering and confirming relevant information, scoping, and deploying SIEM data collection architecture, implementing SIEM Rules and Use Cases and service activation.

STEP	DESCRIPTION	ESTIMATED DURATION

1

		(WEEKS)
33. Initiation	• **DESIGN** – DeepSeas will document a solution design that will define objectives, identify in-scope data, define use cases, and determine data collection architecture. • **BUILD** – DeepSeas will collaborate with Customer to implement a data collection architecture and SIEM platform by deploying collection devices, validating SIEM ingestion of sample data, and establishing secure connections to cloud SIEM platform. • **ONBOARD –** DeepSeas will collaborate with Customer to onboard environment data and configure ingestion of enrichment and source data.	1-4 WEEKS
34. Stabilization	• **DEPLOY –** DeepSeas will deploy initial threat detection rules and use cases. • **BASELINE & TUNE – DeepSeas will observe** the initial use case alerts and collaborate with Customer to tune log sources, collection filters, rules and use cases based on feedback from DeepSeas. • **DOCUMENT –** DeepSeas will document a Customer MDR Runbook that describes how SIEM use cases will be reviewed and managed.	2-8 WEEKS
35. Managed Operations	**EVENT ANALYSIS & RESPONSE –** DeepSeas will provide Customer with remote services that deliver essential response actions as agreed on in customer contract.	ONGOING

Threat Hunting & Anomaly Detection Service Description

SERVICE OVERVIEW

DeepSeas' Threat Hunting & Anomaly Detection Service applies advanced machine learning and data science techniques to Customer provided machine data to identify network, entity, and user behavior anomalies that may represent an increased cyber security risk. DeepSeas experienced threat hunt team reviews and investigates environment anomalies, as well as apply additional threat intelligence informed methods to search for and validate the potential presence of advanced threats.

SERVICE ELEMENTS

DeepSeas Threat Hunting & Anomaly Detection Service includes the following service elements:

Security Event Log Management and Enrichment

- **Log Collection and Normalization** – Collection and normalization of device logs for In Scope Devices as received and processed in near real time, made available for customer access through the Customer Portal.
- **Event Log Enrichment –** DeepSeas Log Analytics will enrich customer log data through automated analysis. Event enrichment functionality include:
  - **Device and Asset Identification -** Log device asset identification, tracking, & reporting on customer device assets on the same network, subnet, or VLAN as the data collector, based on best efforts to auto-identify assets.
  - **Event Log Correlations** – Pre-built correlations add additional event context to Customer security data to add further context and identification of notable security events.
- **Event Log Storage** - Logs are stored online for ninety (90) days, and additional log data is stored off-line for nine (9) months.

Anomaly Detection & Advanced Analytics

- **Anomaly Detection Platform** – A DeepSeas data lake application which provides network behavioral analytics, security visualization tools, threat intelligence, and support for Advanced Correlation Sources.
- **AI & Machine Learning** - Distinct applications that analyze log and alert data and use different ML approaches (unsupervised and supervised), that result in fewer false positives and can provide detection of unknown attacks.

- **Advanced Correlation for DNS** – analysis of DNS traffic to detect threats based on behavior analysis of both normal and abnormal traffic patterns of DNS requests
- **Advanced Correlation for DHCP** – provides the ability to historically associate leased IP addresses with all past users and computer names, which provides visibility to administrators and analysts researching security issues
- **User Behavior Analysis (UBA)** – Includes behavioral analysis of User access activity, including account changes, privileged account monitoring.
- **Asset Behavior Analysis (ABA)** – Behavioral analysis of assets to determine if potential threats exist based on monitoring deviations of device behavior.

Customer Console and Log Analysis Features

- **Customer Console** – A web-based portal that includes dashboards, threat analysis tools, Log analysis tools, Report system, asset information, and administrative functions to manage access. Includes support for a single company configuration.
- **Event Log Reporting** – Predefined & pre-canned standard templates, custom ad-hoc query tool, creation of customized reports that can be delivered by an automated schedule.
- **Log Analytics Collection Appliance** - Physical or Virtual Data Collector Appliance(s) for a single customer data collection site. Any physical Data Collectors will be provided as a pair for redundancy unless otherwise noted.

THREAT HUNT OPERATIONS

DeepSeas Threat Hunters will operate following 8x5 schedule and apply a repeatable threat hunting methodology that follows a repeatable 8-week cycle.

Phase	Duration	Description
Hypothesize & Prepare	1 Week	• Create threat matrix • APT actors' plans & intentions via cyber threat intelligence • Identify client's critical data and/or systems • Identify target data sets and search collection techniques
Investigate & Enrich	4 Weeks	• Conduct advanced threat hunting in alignment with threat hunt plan.
Remediate & Report	1 Week	• Contain and remove adversary access to networks • Deploy new rules & alerts to automate future

		detection/disruption - Improve and uplift controls via Gap Analysis - Inform risk management & resource allocation

REQUIRED DATA SOURCES

The following data sources are recommended as minimum integration sources to enable DeepSeas Threat Hunting & Anomaly Detection Service.

Category	Supported Vendor Products
Endpoint Detection & Response Data	- Carbon Black - Microsoft Defender for Endpoint - SentinelOne
Identity Event Data	- Active Directory
Netflow Event Data	- Cisco - vCloud - Netflow Standard - AWS VPC Netflow - Microsoft Azure NSG Flow Logs
DNS Event Data	- BlueCat Networks - Cisco - DNS Security - InfoBlox - Simple_DNS - SonicWall
DHCP Event Data	- DHCP Security - SonicWall

DATA COLLECTION REPONISIBILITIES

During scoping and pricing, DeepSeas, working with the Customer, will identify system data sources that will be collected by the log analytics solution and mutually-agree on data collection architecture, that will include:

- The location of machine data collection servers to deploy to the Customer environment(s)

- The network communication and configuration requirements to enable the Customer's system data sources to be forwarded to data collection servers and API data collection targets
- A deployment strategy and timeline for Customer data collection

<u>Customer's Data Collection Responsibilities</u>

- The Customer agrees to provide physical or virtual servers to host DeepSeas data collection software. If, during Service Implementation or anytime thereafter, larger, or additional servers are determined necessary to meet the Service goals (e.g., outcomes), the Customer agrees to provide them.
- The Customer agrees to monitor the performance of log analytics data collection server resources including memory utilization, disk storage, and compute processing performance, and to alert DeepSeas when resource utilization exceeds 85%.

<u>DeepSeas' Data Collection Responsibilities</u>

- DeepSeas will monitor the performance of data collection software that is installed on the Customer- provided data collection servers.
- DeepSeas will monitor the frequency of machine data sources being received by data collection software against a monthly data volume ingestion baseline.

SERVICE ONBOARDING

DeepSeas will work with the Customer to create an implementation plan, that will consist of gathering and confirming relevant information, scoping, and deploying data collection architecture. Duration of deployment will vary based upon scope of data integration plan.

STEP	DESCRIPTION	ESTIMATED DURATION (WEEKS)
36. DESIGN	DeepSeas will document a data collection design that will define objectives, identify in-scope data sources, and determine data collection architecture.	1-2 weeks
37. DEPLOY	DeepSeas will collaborate with Customer to implement a data collection architecture by deploying collection devices, validating ingestion of sample data, and establishing secure connections to DeepSeas Log Analytics platform.	1-2 weeks
38. ONBOARD	DeepSeas will collaborate with Customer to onboard	2-8 weeks

	environment data and configure ingestion of enrichment and source data.	

CUSTOMER RESPONSIBILITIES

f) Customer shall provide designated Authorized Contacts for the Services including designated primary, secondary, and tertiary contacts and shall provide Supplier with Customer's designated contact for maintenance, technical support, and escalation prioritization.

g) Customer shall supply authorized Customer Contact's information, inclusive of contact priority, phone number, cell number, e-mail address, position title, and any escalation path information relevant to Customer's environment (such as a distribution list, or default contact group for escalations).

h) Customer shall designate an individual for Unanswered Ticket escalation or problem escalation including full contact information.

i) Customer shall maintain current and up-to-date contact information regarding designated Authorized Contacts within the Supplier's Client Security Portal.

j) Customer shall inform DeepSeas service delivery manager of planned or recent network environment changed that may impact ongoing availability of event log source data.

Virtual CISO – Service Description

SERVICE OVERVIEW

The DeepSeas Virtual Chief Information Security Officer (vCISO) service partners DeepSeas customers with a part time strategic security advisor who can remove the burden and stress of managing a security program by bringing expertise and knowledge to the customer's business.

The service comprises a standard security strategy program playbook that begins with the development of a risk assessment and a security roadmap. Client stakeholders can align budgets and strategic security initiatives to guide the security program and benefit from ongoing access to their part time virtual CISO.

DELIVERY APPROACH

Leveraging DeepSeas strategic partner Booz Allen Hamilton, vCISO will provide the same expertise and capability as a full-time CISO without the associated level of overhead, benefits and training. An experienced CISO will follow a repeatable methodology accepted by the industry and a streamlined and tailored customer's unique business need.

DeepSeas vCISO Delivery Methodology consists of the following:

- **Define** managed assets and set patching policy requirements
- **Implement** program best practices to minimize the attack surface
- **Validate** control effectiveness regularly to measure threat readiness
- **Align** business needs to prioritize critical assets

RESONSIBILITITES AND OBJECTIVES

The vCISO will provide a fixed number of monthly support hours to the Customer and will apply those hours as mutually agreed to with Customer stakeholder to support the following responsibilities and objectives.

vCISO Responsibilities

- Cybersecurity strategic planning and roadmap execution
- Cybersecurity controls oversight
- Cybersecurity risk management oversight
- Cybersecurity governance/ operational oversight

- Cybersecurity executive reporting
- Cybersecurity related insurance advisory

vCISO Objectives

- Build a cybersecurity culture
- Understand Customer's strategy and business environment to build the most relevant roadmap
- Serve as a trusted cybersecurity advisor enabling leadership to make risk-informed decisions
- Ongoing governance and program tracking to refine and enhance security posture
- Provide recommendations and guidance to deploy next level defenses

INITIAL SECURITY POSTURE ASSESSMENT & SECURITY PLAN

Within the first month of vCISO program kick-off the vCISO will complete an initial security posture assessment for the organization which will deliver a recommended set of near- and long-term security program maturity recommendations. The recommendations made within this assessment will be used as an input to future ongoing vCISO support.

ACTIVITY	DESCRIPTION
Introductory Meeting	vCISO will meet with key business stakeholder to gain an understanding of the organization, business goals and current security program.
High-level Security Posture Review	vCISO will coordinate and lead two interviews, each 1-2 hours in duration to determine: Executive organizational security perspective Technical interview with current security/IT team
Security Posture Deliverable Report	vCISO will present a PowerPoint based review of the assessment results document that will provide a subjective view of the organization's maturity levels across the various security domains required for an effective security program. The report will include: • Immediate recommended actions to strengthen organization security program • Longer-term security projects prioritized by urgency

1

ON-GOING SECURITY LEADERSHIP SUPPORT

In an ongoing basis, and within the limit of the monthly retainer, vCISO will continue to apply use real-world experience and industry leading practices to understand customer security program needs and integrate practical solutions.