



RE: TALANOS CYBER SECURITY OPERATIONS CENTRE - G-CLOUD

We would like to thank you for the opportunity to respond to your request for building and managing your Security Operations Centre capability. This service definition document was created with great care and represents a comprehensive, realistic response to common requirements which we hope gives you some insight into how we treat our customers. It truly is our belief that we have a valuable service to bring to a partnership with yourselves.

Personally, I look forward to meeting with you and answering your questions.

Kind Regards,

Andrew Papastefanou
Managing Director – Talanos Cybersecurity
+44 (0)7947 601897
andy@taloscs.com

Security Operations Centre G Cloud 13 Service Definition

May 2022



Executive Summary

The world has changed forever due to COVID-19 and with the workforce facing a permanent move to working from home, company budgets are being reallocated to the speedy transition towards digital.

What threats lurk from the home office where it is essential to keep people working and motivated at the potential expense of security? Most organisations are not ready for this.

Our prediction is that this rapid transformation will hasten in the unprecedented adoption of the cloud, zero trust networking and the digital identity becoming the new 'edge'.

Talanos Cybersecurity's core services are aligning with these three trends to provide a future proof and holistic view on an organisation's cyber security.

Adoption of Cloud – Be Everywhere

The AlienVault SIEM that is the technology pillar of Talanos' services is itself cloud based and connects to both cloud and on-premise environments. A number of pre-built integrations and plugins provide a single view of the enterprise assets and correlate events across them to detect indicators of compromise. Integrated threat intelligence drawn from a global community of customers and security researchers ensures that the SIEM engine is automatically updated with the latest detection rules.

Zero Trust Architecture

Zero Trust Architectures treat all entities and network requests as untrusted until verified, and therefore inspect and log all traffic; continuously monitor interactions and adjust as needed. Forrester have listed the following practical steps that organisations can follow to implement Zero Trust – (1) Identify and map the flows of sensitive data, (2) Employ network segmentation with Zero Trust micro-perimeters, (3) Continuously monitor your ecosystem using analytics and (4) Embrace automation and orchestration. Although not directly a Talanos deliverable, our service strategy incorporates and supports many aspects of Zero Trust and can be used by the customer to plan a roadmap and start the journey towards Zero Trust.

Identity is Security

Where most MSSP's are focused on external threats, Talanos can additionally govern the identities of authorised and privileged users, analysing their patterns of good behaviour. Identity brings context to what would otherwise be meaningless interactions between endpoints and understanding 'why' transactions occur is critical in detecting nuanced behaviour like fraud, unintentional insider exploitation and advanced persistent threats.



Technology, architecture and strategy aside, the most important component in a Managed Detection and Response service is its people. You cannot automate creativity and curiosity and you cannot buy ingenuity and experience. Talanos is extremely proud of the people it employs and invests heavily in their selection, training and well-being. In return, they fight alongside our customers in the trenches, care deeply about their role as partner and deliver exceptional work.

We hope that you would partner with us to prepare your organisation for this new world.



Table of Contents

Executive Summary	3
Table of Contents	5
Response to Requirements	7
NIST CSF Requirements Mapping	7
Identify	7
Protect.....	16
Detect.....	23
Respond.....	29
Recover.....	33
Supplier Information	34
History	34
Technology	35
Overview	35
Gartner	37
Sensors Requirements.....	38
Data Security	38
IT Resilience & Disaster Recovery.....	39
Business Continuity	40
Documentation	42
Project Documentation	42
Operational Documentation.....	42
Standards	42
Price.....	44
Implementation & Support	44
Build	44
Run	45
Operating Hours.....	46
Managed Detection & Response Team	47
Incident Response Process	47
Monitor	49
Service Levels	51
Service Credits.....	52

Manage	53
Service Review Meetings.....	53
Key Personnel.....	53
Transition	54
Knowledge Management & Training.....	54
Exit Services.....	55



Response to Requirements

NIST CSF Requirements Mapping

The Talanos proposal has been mapped to the NIST Cybersecurity Framework as well as the implemented controls from NIST SP 800-53, Revision 5, for ease of reference.

Identify

Asset Management	Common Requirement	Talanos Response	Specific NIST SP 800-53, REV. 5 Controls Implemented
ID.AM-1: Physical devices and systems within the organization are inventoried	Assets must be identified and categorised based on attributes, such as by OS	<p>COMPLIANT</p> <p>AlienVault has built-in asset discovery which discovers physical and virtual assets running on-premises and in cloud environments (including GCP, AWS, Azure, VMware, Hyper-V). Talanos have developed reporting that highlights the changes between asset scans to indicate newly added or removed assets.</p>	<p>CM-8 System Component Inventory</p> <ul style="list-style-type: none"> • CM-8(1) UPDATES DURING INSTALLATION AND REMOVAL • CM-8(2) AUTOMATED MAINTENANCE • CM-8(3) AUTOMATED UNAUTHORIZED COMPONENT DETECTION • CM-8(5) NO DUPLICATE ACCOUNTING OF COMPONENTS • CM-8(7) CENTRALIZED REPOSITORY
ID.AM-2: Software platforms and applications within the organization are inventoried	Two-way integration with Jira, or asset inventory should be supported	<p>COMPLIANT</p> <p>AlienVault has a pre-built AlienApp for Jira. As USM Anywhere surfaces events, alarms, and vulnerabilities, your team determines which items require the opening of a new Atlassian Jira issue. Rather than manually opening each issue in the Jira user interface (UI) and entering the relevant alarm, event, or vulnerability information, you can use the AlienApp for Jira response actions to automatically create the Jira issue with the subject and description fields pre-populated with content from your USM Anywhere environment. The following table lists the available actions from the AlienApp:</p>	

		<p>Actions for the AlienApp for Jira</p> <table border="1"> <thead> <tr> <th>Action</th> <th>Function</th> </tr> </thead> <tbody> <tr> <td>Create a new issue from an alarm.</td> <td>Run this action to generate a new Jira issue directly from an alarm. This action is available when you launch a response action directly from an alarm or a response action in an orchestration rule.</td> </tr> <tr> <td>Create a new issue from a vulnerability.</td> <td>Run this action to generate a new Jira issue directly from a vulnerability. This action is available when you launch a response action directly from a vulnerability.</td> </tr> <tr> <td>Create a new issue from an event.</td> <td>Run this action to generate a new Jira issue directly from an event. This action is available when you launch a response action directly from an event.</td> </tr> <tr> <td>Create a new issue from event based orchestration rule</td> <td>Run this action to generate a new Jira issue directly from an orchestration rule that triggers from a matching event. This action is available when you launch a response action in an orchestration rule.</td> </tr> </tbody> </table> <p>A video of the integration can be seen here (Module 5 > Jira AlienApp): https://cybersecurity.att.com/training/self-paced-training</p>	Action	Function	Create a new issue from an alarm .	Run this action to generate a new Jira issue directly from an alarm. This action is available when you launch a response action directly from an alarm or a response action in an orchestration rule.	Create a new issue from a vulnerability .	Run this action to generate a new Jira issue directly from a vulnerability. This action is available when you launch a response action directly from a vulnerability .	Create a new issue from an event .	Run this action to generate a new Jira issue directly from an event. This action is available when you launch a response action directly from an event .	Create a new issue from event based orchestration rule	Run this action to generate a new Jira issue directly from an orchestration rule that triggers from a matching event. This action is available when you launch a response action in an orchestration rule .	<ul style="list-style-type: none"> • CM-8(8) AUTOMATED LOCATION TRACKING • CM-8(9) ASSIGNMENT OF COMPONENTS TO SYSTEMS <p>CP-2 Contingency Plan</p> <ul style="list-style-type: none"> • CP-2(8) IDENTIFY CRITICAL ASSETS
Action	Function												
Create a new issue from an alarm .	Run this action to generate a new Jira issue directly from an alarm. This action is available when you launch a response action directly from an alarm or a response action in an orchestration rule.												
Create a new issue from a vulnerability .	Run this action to generate a new Jira issue directly from a vulnerability. This action is available when you launch a response action directly from a vulnerability .												
Create a new issue from an event .	Run this action to generate a new Jira issue directly from an event. This action is available when you launch a response action directly from an event .												
Create a new issue from event based orchestration rule	Run this action to generate a new Jira issue directly from an orchestration rule that triggers from a matching event. This action is available when you launch a response action in an orchestration rule .												
ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	Additional Value Added	<p>COMPLIANT</p> <p>Analysts have the ability to tag and group assets dynamically through rules or by manually grouping them. Groups can then have priority and weight assigned to them in correlation rules to be treated differently. You would use asset grouping in cases such as business critical assets, HIPAA assets, PCI CDE assets, Windows assets, etc.</p> <p>Talanos will work with the customer to identify and group critical assets.</p>											

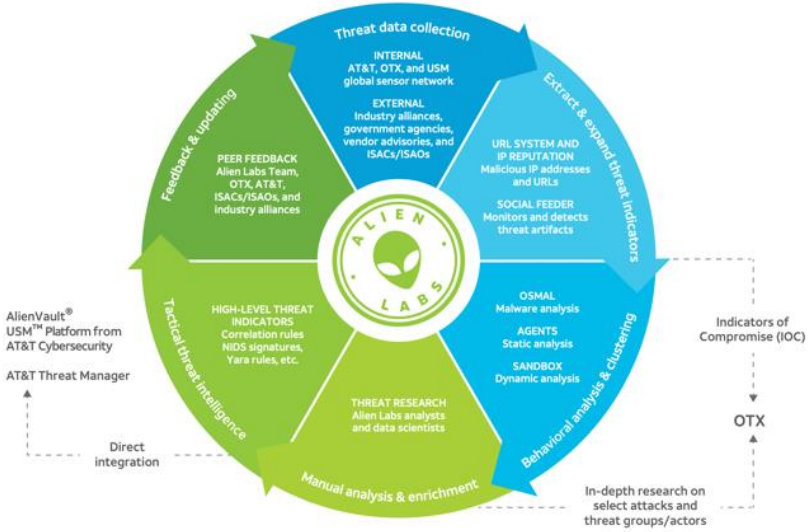
Business Environment	Common Requirement	Talanos Response	Specific NIST SP 800-53, REV. 5 Controls Implemented

ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	Additional Value Added	<p>COMPLIANT</p> <p>Talanos believes that Managed Detection and Response will become a critical service of the organisation and will work to develop a customised BCP to cater for various environmental states in the customer estates. The global team will use all channels available to them to ensure that communication continues and that the service is delivered uninterrupted through a disaster scenario. The requirements and plan will be gathered and delivered during the rollout project.</p>	<ul style="list-style-type: none"> CP-11 Alternate Communications Protocols
---	------------------------	---	--


Governance	Common Requirement	Talanos Response	Specific NIST SP 800-53, REV. 5 Controls Implemented
ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	Additional Value Added	<p>COMPLIANT</p> <p>A key deliverable of the project rollout will be to determine the service management process for the customer which in addition to clarifying the technology and process will also define the people roles and responsibilities. The process will be agreed between all parties and regular monthly feedback sessions will be used to tune the process.</p> <p>Talanos have existing personnel security procedures which have been approved by other financial services organisations and so we're confident our control will satisfy the customer's requirements. We are happy to comply with any 3rd party risk assessment requests, if required.</p>	<ul style="list-style-type: none"> PS-7 EXTERNAL PERSONNEL SECURITY


Risk Assessment	Common Requirement	Talanos Response	Specific NIST SP 800-53, REV. 5 Controls Implemented
ID.RA-1: Asset vulnerabilities are identified and documented	Vulnerabilities must be associated with an asset, and tracked through the	COMPLIANT	<p>CA-7 Continuous Monitoring</p> <ul style="list-style-type: none"> CA-7(3) TREND ANALYSES CA-7(4) RISK MONITORING O/S

	service	<p>After completing an asset scan, AlienVault can be scheduled or manually invoked to perform vulnerability scans. Scans can be unauthenticated or authenticated and be run in one of three profiles:</p> <p>USM built-in vulnerability scan profiles</p> <table border="1" data-bbox="801 387 1675 603"> <thead> <tr> <th>Profile Name</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Deep</td> <td>A non-destructive full and slow scan.</td> </tr> <tr> <td>Default</td> <td>A non-destructive full and fast scan. Use this profile if the target system tends to break or crash with the scanning requests.</td> </tr> <tr> <td>Ultimate</td> <td>A full and fast scan including destructive tests. It includes stress tests that can crash the target system. For example, filling a network switch with random MAC addresses.</td> </tr> </tbody> </table> <p>AlienVault identifies systems susceptible to known vulnerabilities, or that may not have antivirus installed and/or operational and tracks these against the asset.</p>	Profile Name	Description	Deep	A non-destructive full and slow scan.	Default	A non-destructive full and fast scan. Use this profile if the target system tends to break or crash with the scanning requests.	Ultimate	A full and fast scan including destructive tests. It includes stress tests that can crash the target system. For example, filling a network switch with random MAC addresses.	<ul style="list-style-type: none"> • CA-7(5) CONSISTENCY ANALYSIS • CA-7(6) AUTOMATION SUPPORT FOR MONITORING
Profile Name	Description										
Deep	A non-destructive full and slow scan.										
Default	A non-destructive full and fast scan. Use this profile if the target system tends to break or crash with the scanning requests.										
Ultimate	A full and fast scan including destructive tests. It includes stress tests that can crash the target system. For example, filling a network switch with random MAC addresses.										
	Vulnerabilities must be able to be marked as false positives or risk accepted without appearing in subsequent reports, aside as being noted as accepted	<p>COMPLIANT</p> <p>Talanos will work with the customer to define the vulnerability management program to ensure that vulnerabilities discovered are prioritised and remediated over time. Risk accepted vulnerabilities are never removed from reports but rather noted as accepted and organised so as not to distract but never forget about them.</p> <p>Talanos will also work with the customer to track and implement the remediation strategies when related to assets under their management. In all cases, vulnerabilities can be raised as individual tickets that can be tracked through to completion – subsequent vulnerability scans will then determine the risk as remediated.</p> <p>Finally, a NIST control relevant to AlienVault itself has been implemented to allow AlienVault to automatically keep itself and its vulnerability database updated to ensure that the SIEM is not at risk.</p>	<p>SI-2 Flaw Remediation</p> <ul style="list-style-type: none"> • SI-2(3) TIME TO REMEDIATE FLAWS AND BENCHMARKS FOR CORRECTIVE ACTIONS • SI-2(5) AUTOMATIC SOFTWARE AND FIRMWARE UPDATES 								
ID.RA-2: Cyber threat intelligence is received	Threat Intelligence must be used to inform and	COMPLIANT	SI-5 Security Alerts, Advisories, and Directives								

<p>from information sharing forums and sources</p>	<p>contextualise all aspects of the service</p>	<p>The AlienVault database is continuously updated with threat intelligence from the Open Threat Exchange (OTX) and the AlienVault Labs Security Research Team ensures that the USM platform has the latest vulnerability signatures and indicators of compromise.</p>  <p>The diagram illustrates the Alien Labs Threat Intelligence Cycle, a continuous loop of six stages: <ul style="list-style-type: none"> Threat data collection: INTERNAL (AT&T, OTX, and USM global sensor network) and EXTERNAL (Industry alliances, government agencies, vendor advisories, and ISACs/ISAOs). Extract & expand threat indicators: URL SYSTEM AND IP REPUTATION (Malicious IP addresses and URLs), SOCIAL FEEDER (Monitors and detects threat artifacts), and OSMAL (Malware analysis). Behavioral analysis & clustering: AGENTS (Static analysis) and SANDBOX (Dynamic analysis). Manual analysis & enrichment: THREAT RESEARCH (Alien Labs analysts and data scientists) and In-depth research on select attacks and threat groups/actors. Tactical threat intelligence: HIGH-LEVEL THREAT INDICATORS (Correlation rules, NIDS signatures, Yara rules, etc.) and Direct integration with AlienVault® USM™ Platform from AT&T Cybersecurity and AT&T Threat Manager. Feedback & updating: PEER FEEDBACK (Alien Labs Team, OTX, AT&T, ISACs/ISAOs, and industry alliances). The cycle outputs Indicators of Compromise (IOC) to the OTX. </p> <p>Talanos also receive training from Immersive Labs on the latest cybersecurity trends which contains detailed reports on threats, TTPs and normally a live sandbox environment on which to experiment with the exploit.</p>	<ul style="list-style-type: none"> • SI-5(1) AUTOMATED ALERTS AND ADVISORIES • PM-15 Security and Privacy Groups and Associations
	<p>Threat intelligence must be shared with the customer</p>	<p>COMPLIANT</p> <p>Talanos runs a threat hunting program using the MITRE ATT&CK framework to proactively detect threats in the customer environment. The results of the threat hunting exercise as well as a summarised report of threat trends are presented to the customer on a monthly basis to share intelligence.</p>	<ul style="list-style-type: none"> • PM-16 Threat Awareness Program

		<p>A basic license for Dark Web monitoring is also included with AlienVault SIEM which monitors public and dark web sources for the trade of stolen credentials. Intelligence reports include VIP customer members and are regularly shared with the team.</p>	
ID.RA-3: Threats, both internal and external, are identified and documented	<p>Threats within the estate should be identified, recorded and communicated to the customer</p>	<p>COMPLIANT</p> <p>One of the first deliverables in the project rollout is a risk assessment workshop that aims to identify critical areas of the estate and potential issues that may exist or require special monitoring. This is the customer’s opportunity to share its understanding of the threats to its environment to Talanos. A register of privileged access and VIP users is noted in the session.</p> <p>Starting with the customer’s understanding of the environment, Talanos monitors the good as well as the bad patterns of behaviour in the estate to detect both malicious and accidental insider threats to build profiles of access – ideally linking with an Identity Governance and Access Management system to add identity context to the transactions.</p> <p>On a monthly basis, a service review meeting is held with the customer to share new threats identified and potential remedial actions that should be taken to mitigate the risk. Risks raised in these sessions should be recorded in the company’s IT Risk Register.</p>	<ul style="list-style-type: none"> PM-12 Insider Threat Program
	<p>External feeds and events identified across the customer’s estate must be used to inform external threat landscape, that should be identified, recorded and communicated to the customer.</p>	<p>COMPLIANT</p> <p>See answer to ID.RA-2. In addition to paid subscription intelligence, Talanos often use various sources of Open Source Intelligence OSINT to glean additional threat intelligence.</p> <p>All threats, internal and external, are noted by Talanos, tracked and regularly communicated with the customer. Changes to the environment and threat landscape will raise / lower the awareness in certain areas to focus on the prioritised threats.</p>	<p>RA-3 Risk Assessment</p> <ul style="list-style-type: none"> RA-3(2) USE OF ALL-SOURCE INTELLIGENCE RA-3(3) DYNAMIC THREAT AWARENESS RA-3(4) PREDICTIVE CYBER ANALYTICS

	<p>All threats should include impacts</p>	<p>AlienVault assist the Talanos team by using machine learning and state-based correlation to detects and predict threats not yet materialised.</p> <p>COMPLIANT</p> <p>Talanos uses the FAIR Institutes taxonomy for information and operational risk where risks are defined as the probable frequency and probable magnitude of future loss.</p>  <p>If the customer agrees, risks will be communicated in these terms to standardise the process. Talanos will then configure the SIEM to align the definitions and impact weighting accordingly.</p>	
--	---	--	--

			
	<p>The customer must be able to record self-identified threats</p>	<p>COMPLIANT</p> <p>The customer is given an opportunity to record threats from the program initiation all the way through the service delivery during monthly service reviews (or as required by escalating to the service delivery manager). This is handled as a threat awareness program rather than in an automated risk management system (where the discussion is ultimately recorded).</p>	<ul style="list-style-type: none"> PM-16 Threat Awareness Program
<p>ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk</p>	<p>Additional Value Added</p>	<p>COMPLIANT</p> <p>The ultimate goal of the Managed Detection and Response service is to manage risk. Discovering a threat by itself is important but can be of little use without the ability to estimate the associated risk to an asset. For threats associated with vulnerabilities for example, USM Appliance assigns a risk factor to each vulnerability found in the system, which corresponds with the Common Vulnerability Scoring System (CVSS) v2.0 severity ratings provided by the National Vulnerability Database (NVD). USM Appliance also compares the detected vulnerability with the Common Vulnerabilities and Exposures (CVE) list and associates it with the CVE ID when a match is found.</p>	<p>RA-2 Security Categorization</p> <ul style="list-style-type: none"> RA-2(1) IMPACT-LEVEL PRIORITIZATION

		<p>Vulnerability Risk Factors and CVSS Scores</p> <table border="1"> <thead> <tr> <th>Risk Factor</th> <th>CVSS Scores</th> </tr> </thead> <tbody> <tr> <td>High</td> <td>7.0 – 10.0</td> </tr> <tr> <td>Medium</td> <td>4.0 – 6.9</td> </tr> <tr> <td>Low</td> <td>0.0 – 3.9</td> </tr> <tr> <td>Info</td> <td>0.0 and no CVE associated</td> </tr> </tbody> </table> <p>All other risks are determined in relation to loss event frequency and loss magnitude.</p>	Risk Factor	CVSS Scores	High	7.0 – 10.0	Medium	4.0 – 6.9	Low	0.0 – 3.9	Info	0.0 and no CVE associated	
Risk Factor	CVSS Scores												
High	7.0 – 10.0												
Medium	4.0 – 6.9												
Low	0.0 – 3.9												
Info	0.0 and no CVE associated												
ID.RA-6: Risk responses are identified and prioritized	Additional Value Added	<p>COMPLIANT</p> <p>AlienVault further classifies threats across a kill-chain taxonomy based on their risk levels allowing responses to be identified and prioritised.</p> <p>A medium term service strategy looks at a program of improvements to be implemented to mitigate risks and this is reported on in the monthly service review meetings.</p>	<ul style="list-style-type: none"> PM-4 Plan of Action and Milestones Process 										

Supply Chain Risk Management	Common Requirement	Talanos Response	Specific NIST SP 800-53, REV. 5 Controls Implemented
ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	Additional Value Added	<p>COMPLIANT</p> <p>Talanos are routinely involved in customer’s PCI audits to ensure that controls can be evidenced but we’re taking this a step further with CREST accreditation planned to take place in 2023. The customer have the opportunity to assess the service through SLA measurement, 3rd party risk assessments and audit – should they wish to do so.</p>	

Protect

Supply Chain Risk Management	Common Requirement	Talanos Response	Specific NIST SP 800-53, REV. 5 Controls Implemented
PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	The respondent should describe any services that may provide and integrate with the core offering in relation to managing user identities, including generic, guest and service accounts, as well as any other form of interactive or non- interactive account within the the customer estate and cloud environments – such as CASB	<p>COMPLIANT</p> <p>AlienVault monitors successful and failed logon events to assets across your on-premises and cloud environments, as well as to cloud applications including Office 365. Most organisations are moving their Access Management capability to Azure for SSO through Microsoft authentication services and a wealth of information is gathered through this Identity Provider and Microsoft’s ATP.</p> <p>Talanos also provide services (both implementation and managed) relating to Identity Governance (IGA) and has partnerships with Saviynt (pure cloud and preferred), SailPoint and Oracle. Identity Governance deals with the Joiner, Mover, Leaver lifecycle of identities as well as their assignment to accounts and entitlements across systems in the environment. Regular recertification (attestation) campaigns are run to determine whether identities adhere to the principles of least privilege and do not violate segregation of duties controls. Talanos has built connectors to bring the analytics from these platforms into the SIEM to add identity context to transactions.</p> <p>Talanos also provide services (both implementation and managed) related to Privileged Account Management (PAM) where privileged user and service accounts are catalogued and closely managed to ensure single points of accountability. In many cases, the end-user of the privilege is unaware of the underlying credential being used because the service is proxied. Again, Talanos has built connectors to bring the analytics from Saviynt’s PAM, Delinea and Beyond Trust into the SIEM to monitor privileged access.</p> <p>* Both PAM and IGA have been excluded from this service definition but the customer are welcome to discuss the details of these services with Talanos.</p>	<ul style="list-style-type: none"> AC-2(4) AUTOMATED AUDIT ACTIONS IA-4(4) IDENTIFY USER STATUS
PR.AC-3: Remote access is managed	Additional Value Added	COMPLIANT	AC-17 Remote Access

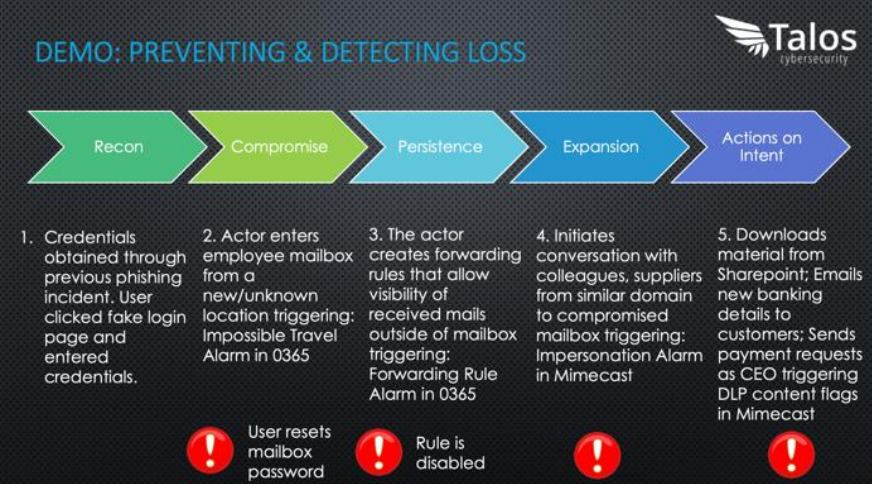




		<p>AlienVault can identify which assets have remote access services running and generally for what purpose they are being used. Further integration into remote access management systems allow information to be monitored more closely.</p> <p>Implementation of PAM and IGA would augment this data and monitoring capability further.</p>	<ul style="list-style-type: none"> • AC-17(1) MONITORING AND CONTROL • AC-17(3) MANAGED ACCESS CONTROL POINTS • AC-17(4) PRIVILEGED COMMANDS AND ACCESS • AC-17(5) MONITORING FOR UNAUTHORIZED CONNECTIONS
--	--	---	--

Awareness and Training	Common Requirement	Talanos Response	Specific NIST SP 800-53, REV. 5 Controls Implemented
PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities	Additional Value Added	<p>COMPLIANT</p> <p>See response to ID.GV-2. Talanos also regularly undergoes practical Blue Team training with CyberGym and Blue Team Security to experience and defend against Advanced Persistent Threats. The scenarios are always impossible to win scenarios allowing the team to execute their roles and responsibilities throughout the kill chain.</p> <p>The Sandbox labs of Immersive Labs also allow the team to experience and explore specific TTPs and better understand the markers and flags that would indicate compromise.</p>	<p>AT-3 Role-Based Training</p> <ul style="list-style-type: none"> • AT-3(3) PRACTICAL EXERCISES <p>IR-2 Incident Response Training</p> <ul style="list-style-type: none"> • IR-2(1) SIMULATED EVENTS • IR-2(2) AUTOMATED TRAINING ENVIRONMENTS • IR-2(3) BREACH


Data Security	Common Requirement	Talanos Response	Specific NIST SP 800-53, REV. 5 Controls Implemented
PR.DS-1: Data-at-rest is protected And;	Informational regarding AlienVaults stance on Data Security.	<p>USM Anywhere architecture and processes are designed to protect your data in transit and at rest.</p> <p>Data Collection All data sent from the USM Anywhere Sensor deployed in your on-premises or cloud environment to the USM Anywhere service in the AlienVault Secure Cloud</p>	<p>SC-28 Protection of Information at Rest</p> <ul style="list-style-type: none"> • SC-28(1) CRYPTOGRAPHIC PROTECTION • SC-28(2) OFFLINE STORAGE

<p>PR.DS-2: Data-in-transit is protected</p>		<p>is encrypted and transferred over a secure TLS 1.2 connection. Each sensor generates a certificate to communicate with the USM Anywhere service. This means that all communication is uniquely encrypted between each sensor and USM Anywhere.</p> <p>All forensic data (raw logs) is backed up on an hourly basis. The data collected in USM Anywhere is secured using AES-256 encryption for both hot (online) storage and cold (offline) storage.</p> <p>Data Access Your data in USM Anywhere is treated as highly confidential, and only a select few AT&T Cybersecurity staff members have access. This group of employees uses multi-factor authentication (MFA) to access the AlienVault Secure Cloud. Strict internal controls and automation enable support for the service while minimizing administrative access.</p> <p>AT&T Cybersecurity also has a formal information security program that implements various security controls to the National Institute of Standards Technology (NIST) Cyber Security Framework. Key controls include: Inventory of Devices, Inventory of Software, Secure Configurations, Vulnerability Assessment, and Controlled Use of Administrative Privileges. Additionally, AT&T Cybersecurity conducts security self-assessments on a regular basis.</p> <p>Single-Tenant Data Store Unlike other SaaS solutions that use a multi-tenant architecture, AT&T Cybersecurity uses a single-tenant data store architecture to securely store your data. With USM Anywhere, your data is stored in its own dedicated data store, which is completely isolated from other customers' data. Unlike multi-tenancy, which is prone to data leakage and breakage that can affect multiple customer accounts, single-tenancy ensures that all customers' data is kept separate and leak-proof.</p> <p>Cold Storage Data Integrity USM Anywhere offers secure long-term log retention, known as cold storage. By default, USM Anywhere stores all data associated with a customer's subdomain in</p>	<p>SC-11 Trusted Path</p> <ul style="list-style-type: none"> • SC-11(1) IRREFUTABLE COMMUNICATIONS PATH
--	--	--	--

		<p>cold storage for the life of the active USM Anywhere subscription at no additional charge.</p> <p>USM Anywhere uses a write once, read many (WORM) approach to log storage to prevent log data from being modified or otherwise tampered with. You can download your raw logs at any time. If you do not renew your subscription, AT&T Cybersecurity will keep the raw logs for 14 days after your subscription expires, giving you a grace period to restart your service. Within the 14 days, no data is collected until your license is reactivated. Therefore, data is lost between license expiration and reactivation. After 14 days, your data will be destroyed.</p>	
<p>PR.DS-5: Protections against data leaks are implemented</p>	<p>The respondent should describe any services that may provide protection against data loss across the customer estate. Including perimeter, endpoint, email, file transfer or other means of data transport that can be inspected.</p>	<p>COMPLIANT</p> <p>AlienVault monitors for communications with known malicious IP addresses, which could identify exfiltration of data and with Cisco Umbrella SOAR capability, the IP could be blacklisted for immediate remediation.</p> <p>The AlienApp for O365 also monitors for changes to Office 365 policies including Data Leakage Protection (DLP) and information management. The Talanos connector for Mimecast also allows the DLP logs to be monitored as part of a broader mail surveillance campaign – picking out specific keywords, file types and numbers that match a regular expression (such as national insurance numbers or birthdays).</p>	<p>SC-7 Boundary Protection</p> <ul style="list-style-type: none"> • SC-7(9) RESTRICT THREATENING OUTGOING COMMUNICATIONS TRAFFIC • SC-7(10) PREVENT EXFILTRATION • SC-7(11) RESTRICT INCOMING COMMUNICATIONS TRAFFIC • SC-7(12) HOST-BASED PROTECTION • SC-7(16) PREVENT DISCOVERY OF SYSTEM COMPONENTS

		 <p>DEMO: PREVENTING & DETECTING LOSS</p> <p>Recon → Compromise → Persistence → Expansion → Actions on Intent</p> <ol style="list-style-type: none"> 1. Credentials obtained through previous phishing incident. User clicked fake login page and entered credentials. 2. Actor enters employee mailbox from a new/unknown location triggering: Impossible Travel Alarm in 0365 3. The actor creates forwarding rules that allow visibility of received mails outside of mailbox triggering: Forwarding Rule Alarm in 0365 4. Initiates conversation with colleagues, suppliers from similar domain to compromised mailbox triggering: Impersonation Alarm in Mimecast 5. Downloads material from Sharepoint; Emails new banking details to customers; Sends payment requests as CEO triggering DLP content flags in Mimecast <p>  User resets mailbox password  Rule is disabled   </p>	
<p>PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity</p>	<p>Additional Value Added</p>	<p>COMPLIANT</p> <p>AlienVault sensors and agents include File Integrity Monitoring (FIM) which detects and reports on access and changes to system binaries, content locations, and critical configuration files. This feature has been used by customers to also determine the accuracy of implemented changes during approved change control windows.</p> <p>Unplanned changes to critical managed files are raised as security incidents through the service management process and these tickets can be raised automatically.</p>	<p>SI-7 Software, Firmware, and Information Integrity</p> <ul style="list-style-type: none"> • SI-7(1) INTEGRITY CHECKS • SI-7(2) AUTOMATED NOTIFICATIONS OF INTEGRITY VIOLATIONS • SI-7(3) CENTRALLY MANAGED INTEGRITY TOOLS • SI-7(5) AUTOMATED RESPONSE TO INTEGRITY VIOLATIONS • SI-7(7) INTEGRATION OF DETECTION AND RESPONSE • SI-7(8) AUDITING CAPABILITY FOR SIGNIFICANT EVENTS

Information Protection Processes and Procedures	Common Requirement	Talanos Response	Specific NIST SP 800-53, REV. 5 Controls Implemented
PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	The respondent must work with the customer to update and develop plans to include the activities, roles and responsibilities provided to the customer	<p>COMPLIANT</p> <p>See responses to ID.BE-5 and ID.GV-2. Talanos has existing plans and a subset of these will be customised for the customer’s environment. Talanos have the capability to run from three geographically separate sites in different timezones and with different religions ensuring uninterrupted service 24x7x365.</p> <p>Talanos will work with the customer to assign roles and responsibilities throughout the:</p> <ul style="list-style-type: none"> • Service Management Plan • Incident Response Plans • Business Continuity Plan • Threat Management Program and; • Vulnerability Management Program 	<p>CP-7 Alternate Processing Site</p> <ul style="list-style-type: none"> • CP-7(1) SEPARATION FROM PRIMARY SITE
PR.IP-10: Response and recovery plans are tested	Additional Value Added	<p>COMPLIANT</p> <p>Talanos regularly tests and tunes incident response plans through its threat hunting initiative.</p> <p>Talanos has also regularly invoked its BCP for testing and in real life scenarios and customers have often noted how seamless the transition was. A session is held with the customer upon resuming normal operations to share lessons learnt and to update and improve the plans for future scenarios.</p>	<p>PM-14 Testing, Training, and Monitoring</p> <p>IR-3 Incident Response Testing</p> <ul style="list-style-type: none"> • IR-3(2) COORDINATION WITH RELATED PLANS • IR-3(3) CONTINUOUS IMPROVEMENT
PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	Informational regarding Talanos stance on HR screening.	<p>COMPLIANT</p> <p>All Talanos employees and contractor’s employment is subject to there being no adverse findings during:</p> <ul style="list-style-type: none"> • Criminal record checks • Fraud and credit checks • Education background checks • Identity Verification 	<p>PS-3 Personnel Screening</p> <ul style="list-style-type: none"> • PS-3(4) CITIZENSHIP REQUIREMENTS

<p>PR.IP-12: A vulnerability management plan is developed and implemented</p>	<ul style="list-style-type: none"> The management plan must include the operation of schedule scans, including how failed or incomplete scans are managed The management plan must include how vulnerabilities are identified, alerted and responded to The management plan should include vulnerabilities identified through other sources 	<p>COMPLIANT</p> <p>Talanos will work with the customer to develop a (or augment an existing) vulnerability management program that includes the requirements raised.</p> <p>AlienVault can be configured to regularly schedule vulnerability scans to identify known vulnerabilities on assets across your environments. Continuously updated threat intelligence ensures that the USM platform is operating with the latest correlation directives, vulnerability signatures, reports, guided responses, and indicators of compromise. It will also identify recommended patches for discovered vulnerabilities.</p> <p>External vulnerability scans (such as from Nessus for example) can be imported into AlienVault to provide single vulnerability views or perform cross-platform correlation.</p>  <p>Raised vulnerabilities may be automatically logged to Jira so that the issue can be tracked through to remediation, but this will be determined by the service management design (also an early stage Talanos deliverable).</p> <p>Vulnerabilities are then considered remediation when subsequent scans can no longer detect the previously raised vulnerability or if the risk has been accepted for the vulnerability. The trends on</p>	<p>RA-5 Vulnerability Monitoring and Scanning</p> <ul style="list-style-type: none"> RA-5(1) UPDATE TOOL CAPABILITY RA-5(2) UPDATE VULNERABILITIES TO BE SCANNED RA-5(3) BREADTH AND DEPTH OF COVERAGE RA-5(4) DISCOVERABLE INFORMATION RA-5(6) AUTOMATED TREND ANALYSES RA-5(10) CORRELATE SCANNING INFORMATION
---	--	--	--



		vulnerability remediation are reported in the monthly service review meeting.	
--	--	---	--

Protective Technology	Common Requirement	Talanos Response	Specific NIST SP 800-53, REV. 5 Controls Implemented
PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	An audit policy providing minimum audit levels for each of the devices/nodes in use within the estate must be provided	<p>COMPLIANT</p> <p>PCI-DSS resources have excellent guidance on operating system audit configuration to satisfy the control requirements. Using these as a baseline, Talanos has built up a library of configuration for devices / nodes that would be implemented to bring in the required information to detect incidents in the SIEM. This is tested and tuned through an ongoing threat hunting program that assesses the level of audit information against the indicators of compromise.</p> <p>AlienVault aggregates and normalises log events from across your on-premises and cloud environments and cloud applications, including Office 365 to create customizable and searchable alarm and event views which enable fast and simple review of events and detected incidents.</p> <p>In the Premium instance selected for the customer, 90 days of hot searchable events are made available and the raw logs required for archive or forensics are stored as long as an active subscription is held with AlienVault (unlimited raw log storage). The raw logs can be downloaded at any point for offsite storage – if required.</p>	<p>AU-11 Audit Record Retention</p> <ul style="list-style-type: none"> AU-11(1) LONG-TERM RETRIEVAL CAPABILITY <p>AU-12 Audit Record Generation</p> <ul style="list-style-type: none"> AU-12(1) SYSTEM-WIDE AND TIME-CORRELATED AUDIT TRAIL AU-12(2) STANDARDIZED FORMATS <p>AU-7 Audit Record Reduction and Report Generation</p> <ul style="list-style-type: none"> AU-7(1) AUTOMATIC PROCESSING AU-7(2) AUTOMATIC SEARCH AND SORT <p>AU-8 Time Stamps</p>

Detect

Anomalies and Events	Common Requirement	Talanos Response	Specific NIST SP 800-53, REV. 5 Controls Implemented
----------------------	--------------------	------------------	--

<p>DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed</p>	<p>The services must contribute to the discovery and ongoing management of dataflows</p>	<p>COMPLIANT</p> <p>The most data rich information gathered in any SIEM implementation is network based information. This is done with a NIDS (Network Intrusion Detection System) agent and is typically quite difficult to configure in traditional on-premise network deployments. This feature will absolutely assist the customer in discovering and managing dataflows within the environment and a design for NIDS will be delivered as part of the Talanos engagement.</p> <p>Port Mirroring Requirements for AlienVault can be found here: https://cybersecurity.att.com/documentation/usm-anywhere/deployment-guide/portmirroring/portmirroring.htm</p> <p>Managing data flows on GCP, Azure and AWS however will be much easier to achieve because the network is essentially software defined. AlienVault has a purpose-built sensor for public clouds that will be able to ingest the VPC data flow logs and provide the required insight.</p>	<p>AC-4 Information Flow Enforcement</p> <ul style="list-style-type: none"> • AC-4(13) DECOMPOSITION INTO POLICY-RELEVANT SUBCOMPONENTS • AC-4(15) DETECTION OF UNSANCTIONED INFORMATION • AC-4(26) AUDIT FILTERING ACTIONS
<p>DE.AE-2: Detected events are analyzed to understand attack targets and methods</p>	<p>The solution must ensure that all events recorded are analysed, both individually but also as part of a wider set of events to identify any potential security incident</p>	<p>COMPLIANT</p> <p>AlienVault aggregates events from across your on-premises and cloud environments and cloud applications, including Office 365 and GCP. The raw events and resulting correlation’s area available to search for 90 days before being archived in long term storage.</p> <p>It uses machine learning and state-based correlation capabilities to detect threats and classifies threats across a kill-chain taxonomy to inform the threat risk level. Continuously updated threat intelligence from AlienVault Labs and the Open Threat Exchange (OTX) delivers the latest correlation rules to the USM platform.</p> <p>The tool however only informs the analysts where they need to look and the ultimate responsibility for identifying and contextualising security incidents remains with Talanos people – who will use all the tools at their disposal to better understand the threat.</p>	<ul style="list-style-type: none"> • CA-7(3) TREND ANALYSES • CA-7(5) CONSISTENCY ANALYSIS • CA-7(6) AUTOMATION SUPPORT FOR MONITORING • IR-4(4) INFORMATION CORRELATION • IR-4(8) CORRELATION WITH EXTERNAL ORGANIZATIONS • IR-4(11) INTEGRATED INCIDENT RESPONSE TEAM • IR-4(13) BEHAVIOR ANALYSIS • IR-4(14) SECURITY OPERATIONS CENTER

<p>DE.AE-3: Event data are collected and correlated from multiple sources and sensors</p>	<p>Event data must be collected from all relevant sources, including endpoints, servers, network devices, storage, perimeter devices, security controls, etc</p>	<p>COMPLIANT</p> <p>See Application Support list later.</p>	<p>IR-5 Incident Monitoring</p> <ul style="list-style-type: none"> IR-5(1) AUTOMATED TRACKING, DATA COLLECTION, AND ANALYSIS
<p>DE.AE-4: Impact of events is determined</p>	<ul style="list-style-type: none"> Impacts must be contextualised to enable the customer to prioritise efforts Impacts must include technical and non-technical impacts 	<p>COMPLIANT</p> <p>In terms of the FAIR institute’s taxonomy, Impact is contextualised as Effect. Primary and Secondary losses are determined.</p> <div style="text-align: center;">  <p>Threats > Controls > Assets > Effect</p> </div> <div style="background-color: #2c4e64; color: white; padding: 10px; margin-top: 10px;"> <p style="text-align: center; font-weight: bold; color: yellow;">Effect</p> <ol style="list-style-type: none"> 1. Productivity <ul style="list-style-type: none"> – Generally represents the reduction in an organisation’s ability to generate its primary value proposition. Example: Income, goods, services, etc. 2. Response <ul style="list-style-type: none"> – Expenses associated with managing a loss event (e.g., internal or external person-hours, logistical expenses, legal defense, public relations expenses, etc.). 3. Replacement <ul style="list-style-type: none"> – The intrinsic value of an asset. Typically represented as the capital expense associated with replacing lost or damaged assets. 4. Fines & Judgments <ul style="list-style-type: none"> – Legal or regulatory actions levied against an organisation. 5. Competitive Advantage <ul style="list-style-type: none"> – Losses associated with diminished competitive position. 6. Reputation <ul style="list-style-type: none"> – Losses associated with an external stakeholder’s perception that an organisation’s value proposition is diminished and/or that the organisation represents liability to the stakeholder. </div> <div style="text-align: right; margin-top: 10px;">  </div>	<ul style="list-style-type: none"> RA-3(2) USE OF ALL-SOURCE INTELLIGENCE RA-3(3) DYNAMIC THREAT AWARENESS CP-2(8) IDENTIFY CRITICAL ASSETS
<p>DE.AE-5: Incident alert thresholds are established</p>	<p>The respondent will work with the customer to establish appropriate thresholds and alerts based on incident type and impact</p>	<p>COMPLIANT</p> <p>There will be a product baseline that will be tuned six weeks into the engagement based on the service management and incident response design and behavioural analysis of transactions in the customer environment. This will be reviewed monthly in the service review</p>	

		meeting. Essentially, it's about learning how to work together to achieve common goals and finding effective ways of delivering tasks.	
--	--	--	--

Security Continuous Monitoring	Common Requirement	Talanos Response	Specific NIST SP 800-53, REV. 5 Controls Implemented
DE.CM-1: The network is monitored to detect potential cybersecurity events	Networks and network attached devices will be monitored to identify potential security events	COMPLIANT See response to DE.AE-1.	<ul style="list-style-type: none"> • AU-12 AUDIT RECORD GENERATION • CA-7 CONTINUOUS MONITORING • SC-7(8) RESTRICT THREATENING OUTGOING COMMUNICATIONS TRAFFIC • SI-4 SYSTEM MONITORING
	Events across platforms will be correlated to identify potential security events	COMPLIANT See response to DE.AE-2.	
DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	The respondent should describe any services that may enable the customer to monitor user behaviour, identifying anomalies and integrating this with the core offering	COMPLIANT See response to PR.AC-1. Additionally, AlienVault monitors user and administrator activities, including access and modification of files and content, in cloud applications such as Office 365 and GCP, for example. It also monitors successful and failed logon attempts to external applications through Azure Active Directory, Office 365 and GCP, for example. Talanos have added extensions and reporting that highlight anomalies in the user behaviour that leads to further investigation.	<ul style="list-style-type: none"> • CA-7 CONTINUOUS MONITORING
DE.CM-4: Malicious code is detected	The solution must be able to detect the delivery and execution of malicious code through integration with existing controls	COMPLIANT AlienVault agents and sensors can monitor for indicators of malware-based compromise, such as communication to a known Command & Control (C&C) Server as well as implement File Integrity Monitoring	<ul style="list-style-type: none"> • SI-3(7) NONSIGNATURE-BASED DETECTION

		<p>(FIM) that detects access and modification to files and directories on Windows and Linux systems.</p> <p>The SIEM will also integrate with the customer’s endpoint protection software and Microsoft Defender ATP to centrally monitor and manage incidents raised through these existing controls.</p> <p>Finally, hashes of known malicious code are shared and updated through the OTX threat intelligence platform but this has historically proved a poor detection mechanism and the Talanos team focus rather on the function (and related events) of code being monitored.</p>	
DE.CM-5: Unauthorized mobile code is detected	The solution must be able to detect the delivery and execution of malicious code through integration with existing controls	<p>COMPLIANT</p> <p>If the Mobile Device Management (MDM) tool can already detect this, then the SIEM will be able to integrate with it to centrally monitor and manage incidents raised through this platform.</p>	
DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	The respondent should describe any services that may enable the customer to monitor for rogue personnel, users, connections, devices and software, integrating this with the core offering	<p>COMPLIANT</p> <p>See response to PR-AC.1 as it relates to rogue personnel and privileged access.</p> <p>Regarding assets and software, AlienVault runs regularly scheduled scans to identify new and updated assets and to identify any vulnerabilities on each asset. The delta is highlighted and investigated by Talanos analysts who may upon investigation raise incidents relating to the change.</p> <p>Unauthorized connections are only highlighted when they are connecting to known bad actors (IP addresses on black or grey lists).</p>	<ul style="list-style-type: none"> • AU-12 AUDIT RECORD GENERATION • CA-7 CONTINUOUS MONITORING • CM-8 SYSTEM COMPONENT INVENTORY • SI-4 SYSTEM MONITORING
DE.CM-8: Vulnerability scans are performed	<ul style="list-style-type: none"> • Solution should include discovery, vulnerability scanning, web application scanning, and configuration assessment 	<p>COMPLIANT</p> <p>See response to ID.RA-1.</p>	<ul style="list-style-type: none"> • RA-5 VULNERABILITY MONITORING AND SCANNING

	<ul style="list-style-type: none"> • Unsafe/dangerous scans should be configurable per scan, host, time • Remote and authenticated scans must be supported • Solution must support cloud environments 	<p>Additionally, vulnerability scanning will be performed across a hybrid environment of both cloud and on-premise assets and has in our experience also highlighted deficient or misconfigured assets.</p>	
--	--	---	--

Detection Processes	Common Requirement	Talanos Response	Specific NIST SP 800-53, REV. 5 Controls Implemented
DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability	<ul style="list-style-type: none"> • The respondent must work with the customer to define roles and responsibilities and to identify accountability • The customer will look to the respondent’s expertise to assist in this development 	<p>COMPLIANT</p> <p>See response to PR.IP-9.</p>	<ul style="list-style-type: none"> • PM-14 TESTING, TRAINING, AND MONITORING
DE.DP-2: Detection activities comply with all applicable requirements	Detection activities must comply with regulatory requirements (DPA, FCA)	<p>COMPLIANT</p> <p>AlienVault has recently completed its ISO27001:2013 certification and a 3rd Party assessment of its GDPR Readiness. As part of our efforts to comply with GDPR and to help you to demonstrate your own compliance, we have compiled a Data Processing Addendum (DPA) that provides our customers and partners with a documented summary of the policies and processes we have established to ensure GDPR compliance. This DPA is designed to be mutually executed by AlienVault, Talanos and the customer.</p> <p>AlienVault also has an updated privacy policy that clearly communicates how they collect user data and for what purposes in accordance with GDPR which can be found here: https://cybersecurity.att.com/legal/privacy-policy</p>	

	Detection activities must comply with control framework requirements (e.g. ISO27k, NIST CSF, PCI-DSS, etc)	COMPLIANT Evidenced throughout. Additionally, AlienVault have been ISO27001:2013, HIPAA, SOC2 and PCI-DSS certified.	
DE.DP-4: Event detection information is communicated	<ul style="list-style-type: none"> Stakeholders must be identified for the receipt of event detection information Information must be made available through secure means 	<p>COMPLIANT</p> <p>Together with the customer, Talanos will develop a service management design that will talk to these requirements. Technically however, AlienVault enables creation of different user accounts that grant access to the USM platform console for inspection and review of alarms and events. There are built-in notification capabilities that enable analysts to be alerted to alarms through email, SMS, Datadog, and Slack and Talanos have an additional pre-built Manage Engine integration for our Service Desk.</p> <p>Using the AlienApp for Jira, we provide the ability to manually or automatically generate a ticket within Jira in response to a detected alarm. Managing access to these systems will ensure that event detection information is only ever available through secure means.</p>	<ul style="list-style-type: none"> AU-6 AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING

Respond

Communications	Common Requirement	Talanos Response	Specific NIST SP 800-53, REV. 5 Controls Implemented
RS.CO-1: Personnel know their roles and order of operations when a response is needed	<ul style="list-style-type: none"> The respondent must work with the customer to agree roles and responsibilities The respondent's services must work with and alongside the customer's team and incumbent IT provider 	<p>COMPLIANT</p> <p>See response to PR.IP-9.</p>	
RS.CO-2: Incidents are reported consistent with established criteria	<ul style="list-style-type: none"> The respondent must work with the customer to agree incident reporting 	<p>COMPLIANT</p> <p>See response to PR.IP-9.</p>	

	<ul style="list-style-type: none"> Reporting should include appropriate reports for various stakeholders across the business and management/executive teams 	<p>Additionally, monthly service reviews will be held with management / executive teams where the appropriate business terminology and language will be used to communicate incidents effectively. These sessions will be the best opportunity to share knowledge, intelligence, measure performance and provide feedback.</p>	
RS.CO-3: Information is shared consistent with response plans	The respondent must work with the customer to agree information sharing	<p>COMPLIANT</p> <p>See response to PR.IP-9.</p>	
RS.CO-4: Coordination with stakeholders occurs consistent with response plans	The respondent must work with the customer to agree stakeholder engagement	<p>COMPLIANT</p> <p>See response to PR.IP-9.</p>	
RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	The respondent should describe how they could support the customer in sharing threat information and other useful and relevant information, in a form that does not compromise the customer's security, but provides value to the wider industry	<p>COMPLIANT</p> <p>This will always be client lead and Talanos will never solicit detailed information from the customer to share externally. The high-level TTP may be used to broadly educate external stakeholders using the same language that would be used to educate non-IT executives.</p> <p>Eg. I baked a cake, rather than, I beat eggs with flour and sugar to bake the customer a cake.</p>	

Analysis	Common Requirement	Talanos Response	Specific NIST SP 800-53, REV. 5 Controls Implemented
RS.AN-1: Notifications from detection systems are investigated	Potential security events must be analysed and investigated	<p>COMPLIANT</p> <p>See Incident Response Process below.</p>	
RS.AN-2: The impact of the incident is understood	The impact to the customer's operations must be qualified and quantified, considering all potential impacts	<p>COMPLIANT</p> <p>See response to ID.RA-3.</p>	

RS.AN-3: Forensics are performed	<ul style="list-style-type: none"> • Where required, forensic capabilities should be available to investigate incidents further • Forensic evidence must be maintained to preserve integrity and be suitable as evidence for any potential legal action 	<p>COMPLIANT</p> <p>With the AlienApp for Forensics and Response, AlienVault enables automatic forensics tasks to be executed in response to a detected threat. External forensic examiners are able to perform their investigation with rich filter, search, and reporting capabilities event and log data. Examiners typically require raw logs and these are archived in unlimited long term storage that has its integrity preserved and is always downloadable through the SIEM console.</p> <p>Beyond technically enabling the forensics activity, Talanos DO NOT provide forensic cyber security services as these are highly specialised and typically require the forensic auditor to provide testimony in court during prosecutions.</p>	
RS.AN-4: Incidents are categorized consistent with response plans	The respondent must work with the customer to agree incident categorisation	<p>COMPLIANT</p> <p>See response to DE.AE-5.</p>	
RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)	The respondent must work with the customer to agree and share such information	<p>COMPLIANT</p> <p>See response to PR.IP-12</p>	

Mitigation	Common Requirement	Talanos Response	Specific NIST SP 800-53, REV. 5 Controls Implemented
RS.MI-1: Incidents are contained	<ul style="list-style-type: none"> • The respondent must work with the customer to ensure identified security incidents are contained 	<p>COMPLIANT</p> <p>See response to PR.IP-9 and PR.IP-12</p>	

	<ul style="list-style-type: none"> This may include recommendations, actions and ownership of security controls and configurations 	<p>Generally, Talanos should never own security controls and configuration unless it is related to the SIEM and service management itself. This does not mean that tickets are thrown over the fence and we no longer worry about them. In a RACI model, we can be held accountable for our recommendations, often consulted and should definitely be informed but never responsible for the execution of the control change.</p>	
RS.MI-2: Incidents are mitigated	<ul style="list-style-type: none"> The respondent must work with the customer and the IT provider to remediate identified security incidents This may include recommendations, actions and ownership of security controls and configurations 	<p>The actual process of remediation would be carried out by the customer where the Talanos team would interact directly with the teams to provide analysis, recommendations, playbooks and support. Where the customer have previously approved it, automated remediation and orchestration (SOAR) could be implemented to Cisco Umbrella for example, to immediately block malicious IPs that have triggered an indicator of compromise or security incident on the SIEM platform.</p> <p>Talanos used Manage Engine’s Service Desk for managing all incidents internally and where possible, we integrate with the customer’s ticketing system so that incidents can be automatically raised and tracked on both sides. AlienVault also has a pre-built integration with Jira to add tickets for assets and log vulnerabilities and incidents automatically. The nature of the integration and which systems will be used for managing tasks will be discussed and agreed with the customer.</p>	
RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	<ul style="list-style-type: none"> The respondent must work with the customer and the IT provider to remediate identified vulnerabilities This may include recommendations, actions and ownership of security controls and configurations 	<p>COMPLIANT</p> <p>See response to PR.IP-12</p>	

Improvements	Common Requirement	Talanos Response	Specific NIST SP 800-53, REV. 5 Controls Implemented
RS.IM-1: Response plans incorporate lessons learned And RS.IM-2: Response strategies are updated	Additional Value Added	COMPLIANT A standard part of the ITIL and ITSM process is to continuously improve and sessions are held together with the customer to share our experiences, lessons learnt, honest feedback and focus areas. The customer will benefit from the lessons that Talanos have learnt at other customers and vice versa ensuring that plans and responses are always updated to reflect the latest understanding.	

Recover

Improvements	Common Requirement	Talanos Response	Specific NIST SP 800-53, REV. 5 Controls Implemented
RC.IM-1: Recovery plans incorporate lessons learned And RC.IM-2: Recovery strategies are updated	Additional Value Added	COMPLIANT See response to RS.IM-1.	



Supplier Information

History

Talanos Cybersecurity is the trading name of Prosense Technology Limited, a company registered in England and Wales, in 2016 with Companies House number 10019631.

Talanos specialises in serving the financial services industry and provides the following capabilities, either as a Managed Service or through an implementation:

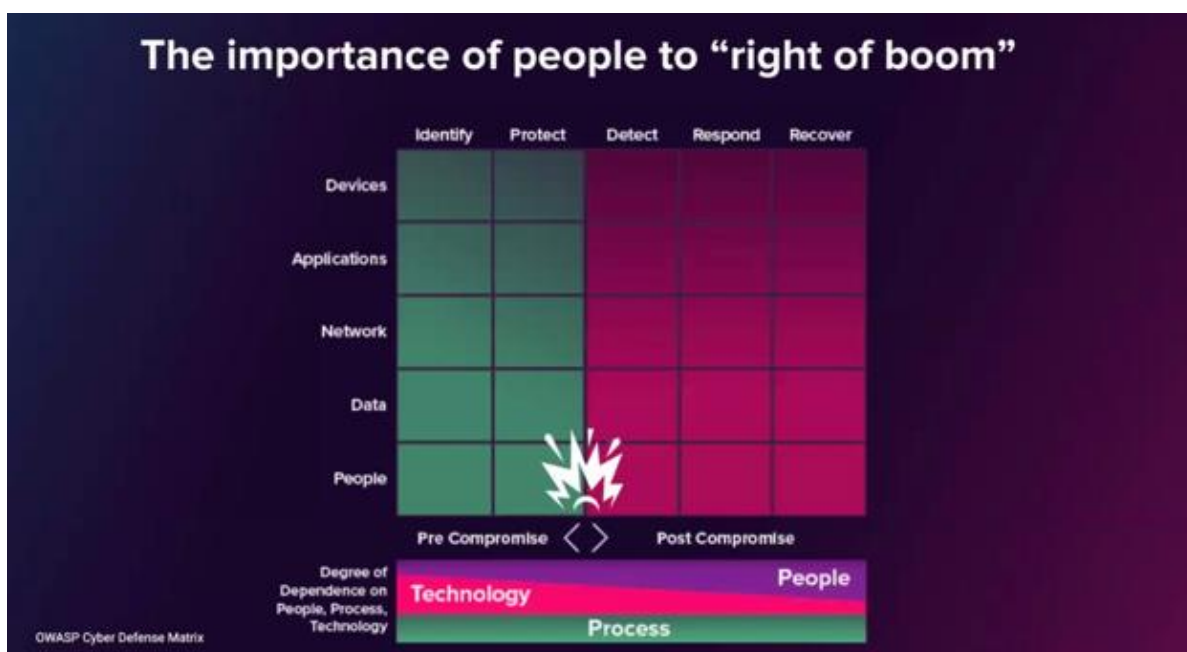
- Identity Governance (Partnerships with Saviynt, Oracle and Sailpoint)
- Access Management (Partnership with Okta, One Identity and Oracle)
- Privileged Access Management (Partnership with Delinea, BeyondTrust, Cyberark and Saviynt)
- Managed Detection & Response (Partnership with AlienVault, SentinelOne)
- Threat Intelligence
- Service Oriented Architecture (Partnership with Oracle)
- eSignatures (Partnership with Impression Signatures)

The team have battled DDOS attacks, worked with police intelligence to uncover syndicate activity and traced individuals complicit in Business Email Compromise.

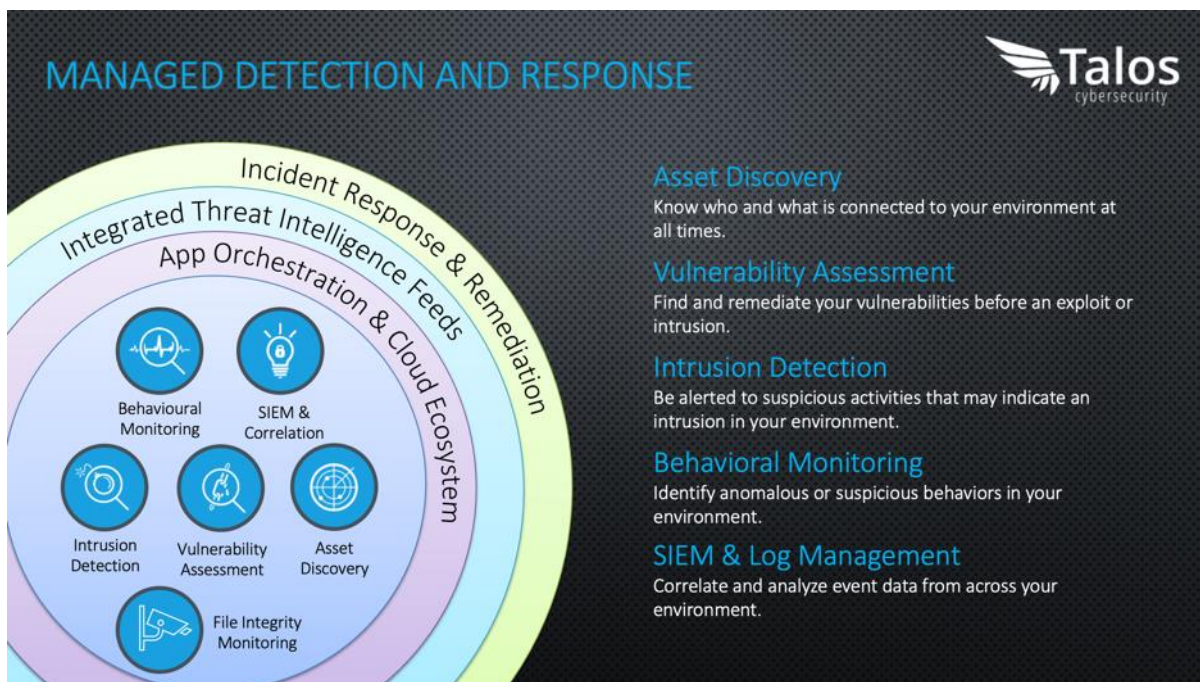
Technology

Overview

In government parlance, Boom is the detonation of an explosive device, initially used in speaking of a nuclear bomb. Those steeped in disaster preparedness and response now speak in terms of “left of boom” and “right of boom”. Technology, although an important component of security operations monitoring is not nearly as important as the people and process component of any Managed Detections and Response service. The technology should therefore support the people and process and should be evaluated in such terms rather than on a product by product basis.



It was this approach that led Talanos to partnering with AlienVault (subsequently acquired by and renamed to AT&T Cybersecurity). The support received from the team and the flexibility in the approach made the AlienVault product an obvious choice for Talanos in becoming an MSSP. Entering our sixth year of partnership, Talanos continues to evaluate its selection of AlienVault’s SIEM against other market offerings and is still convinced that it is the right tool for the job – having successfully delivered the service Talanos was employed to provide. The AlienVault toolset provides the following capabilities:



The AlienVault product suite are composed of an Agent, Sensor, Logger and Server where each component has the following functionality –

Agent: An agent is either a HIDS (hardware IDS) or NIDS (network IDS) agent responsible for forwarding logs and events to a sensor. It can be configured to filter (or include) specific events and is also responsible for file integrity monitoring. Servers (or services) that cannot forward their logs and events to a syslog service can use the agent to do this on their behalf.

Sensor: A sensor receives logs and events in syslog format and uses plugins to normalise the data into a predefined format that is easily interpreted by the logger. The sensor will typically sit in a network segment to capture traffic locally, requiring only a single route of traffic into and out of the sensor. The sensor is also responsible for running the automated asset discovery and vulnerability scans.

Logger: The logger receives normalised logs from the multiple sensors and is responsible for organising the raw logs, running the correlation rules and parsing the raw data into intelligence to raise alarms and incidents. The correlation rules may build across sources to form indicators of compromise that will be mapped to a kill chain taxonomy and raise the appropriate response.

Server: The server is responsible for presenting the information and dashboards to security analysts so that they may investigate incidents, close tickets and perform functions in the SIEM.

Gartner



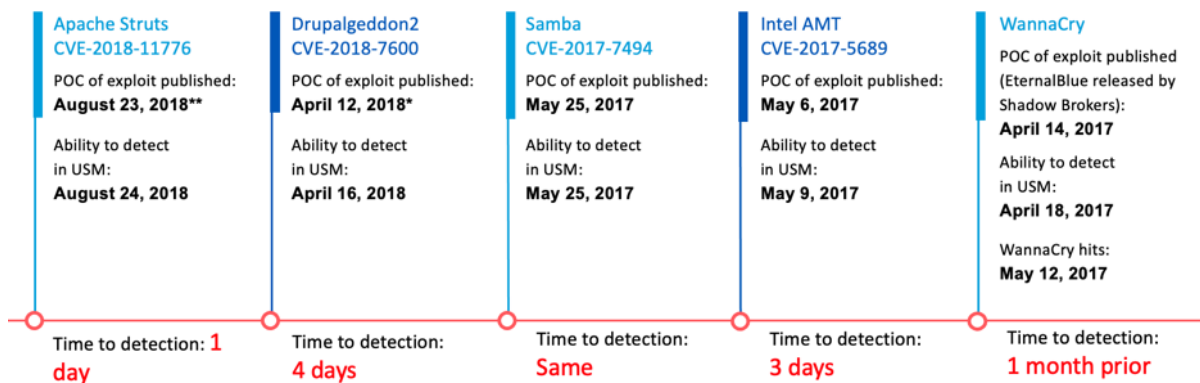
AlienVault features in the Gartner SIEM Magic Quadrant 2020 with the following relevant quotation:

“Small and midsize businesses (SMBs) in financial services and healthcare verticals, which need SIEM as a service (SaaS SIEM) delivery models with bundled security controls that don’t require extensive database or application monitoring or advanced analytics, should consider AT&T Cybersecurity’s USM Anywhere.”

Since Gartner’s report, AlienVault have introduced several new features to address the areas that Gartner felt they could improve, such as User Behaviour Analytics and new AlienApps for automation, orchestration and response – Check Point, MS Defender ATP, SentinelOne and Umbrella.

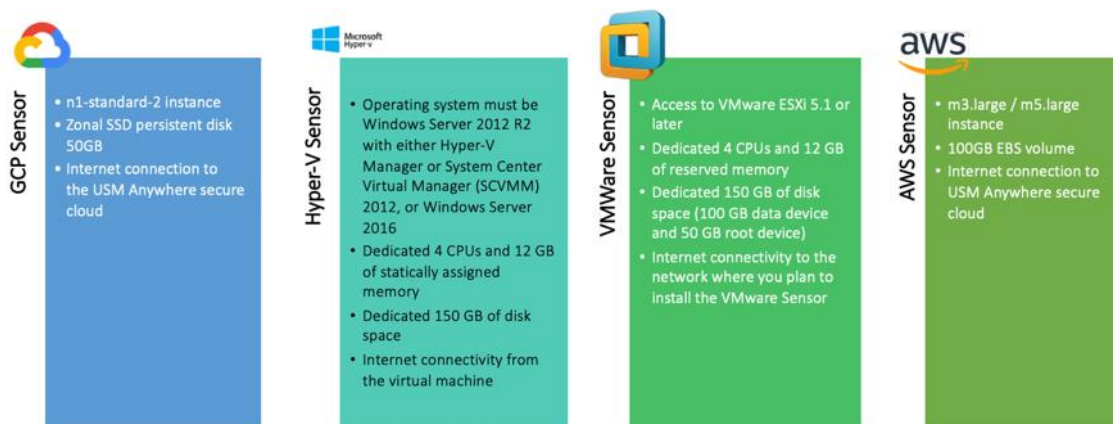
AlienVault’s integrated threat detection that updates indicators of compromise and correlation rules based on the latest exploits is highlighted as a strength:

Early detection



Sensors Requirements

Sensors will have the following technical requirements to be installed in the various environments:



Data Security

As a security-first organization, AT&T Cybersecurity makes your data protection and privacy a top priority. USM Anywhere architecture and processes are designed to protect your data in transit and at rest. USM Anywhere and USM Central have been attested as compliant to PCI DSS, SOC 2, and HIPAA, ensuring confidentiality, integrity, and availability of your data and your customers' data.

All data sent from the USM Anywhere Sensor deployed in your on-premises or cloud environment to the USM Anywhere service in the AlienVault Secure Cloud is encrypted and transferred over a secure TLS 1.2 connection. Each sensor generates a certificate to communicate with the USM Anywhere service. This means that all communication is uniquely encrypted between each sensor and USM Anywhere.

All forensic data (raw logs) is backed up on an hourly basis. The data collected in USM Anywhere is secured using AES-256 encryption for both hot (online) storage and cold (offline) storage.

Your data in USM Anywhere is treated as highly confidential, and only a select few AT&T Cybersecurity staff members have access. This group of employees uses multi-factor authentication (MFA) to access the AlienVault Secure Cloud. Strict internal controls and automation enable support for the service while minimizing administrative access.

AT&T Cybersecurity also has a formal information security program that implements various security controls to the National Institute of Standards Technology (NIST) Cyber Security Framework. Key controls include: Inventory of Devices, Inventory of Software, Secure Configurations, Vulnerability Assessment, and Controlled Use of Administrative Privileges. Additionally, AT&T Cybersecurity conducts security self-assessments on a regular basis.

Unlike other SaaS solutions that use a multi-tenant architecture, AT&T Cybersecurity uses a single-tenant data store architecture to securely store your data. With USM Anywhere, your data is stored in its own dedicated data store, which is completely isolated from other customers' data. Unlike multi-tenancy, which is prone to data leakage and breakage that can affect multiple customer accounts, single-tenancy ensures that all customers' data is kept separate and leak-proof.

USM Anywhere offers secure long-term log retention, known as cold storage. By default, USM Anywhere stores all data associated with a customer's subdomain in cold storage for the life of the active USM Anywhere subscription at no additional charge.

USM Anywhere uses a write once, read many (WORM) approach to log storage to prevent log data from being modified or otherwise tampered with. You can download your raw logs at any time. If you do not renew your subscription, AT&T Cybersecurity will keep the raw logs for 14 days after your subscription expires, giving you a grace period to restart your service. Within the 14 days, no data is collected until your license is reactivated. Therefore, data is lost between license expiration and reactivation. After 14 days, your data will be destroyed.

IT Resilience & Disaster Recovery

To ensure business continuity, USM Anywhere executes a backup procedure 2 times a day, encrypts the data, and stores it for 15 days. The Recovery Point Objective (RPO) is up to 12 hours and the Recovery Time Objective (RTO) is approximately an hour, depending on the size of the data being restored.

The USM Anywhere cloud instance will be deployed in one of the following AWS endpoint regions based on your chosen location. The backup is simply redeployed / migrated to a different region as required. Deployments benefit from all the resilience features available on the AWS public cloud. Historical outages related to the AlienVault service can be found here: <https://status.alienvault.cloud>

The following table lists the code and name of each region:

Supported AWS Regions		
Code	Name	Reserved Static IP Address Blocks
ap-northeast-1	Asia Pacific (Tokyo)	18.177.156.144/28
ap-south-1	Asia Pacific (Mumbai)	3.7.161.32/28
ap-southeast-2	Asia Pacific (Sydney)	3.25.47.48/28
ca-central-1	Canada (Central)	3.96.2.80/28
eu-central-1	Europe (Frankfurt)	18.156.18.32/28
eu-west-1	Europe (Ireland)	3.250.207.0/28
eu-west-2	Europe (London)	18.130.91.160/28
sa-east-1	South America (São Paulo)	18.230.160.128/28
us-east-1	US East (N. Virginia)	3.235.189.112/28
us-west-2	US West (Oregon)	44.234.73.192/28
us-gov-west-1	AWS GovCloud (US-West)	3.32.43.32, 3.32.43.33, 3.32.43.34, 3.32.43.35

Talanos, as an MSSP of AlienVault, providing a USM Anywhere instance to the customer will benefit from the following support SLAs 24x7x365:

Response Times:

- Severity 1: 1 hour during All Coverage Hours
- Severity 2: 2 hours during All Coverage Hours
- Severity 3: 6 hours during All Coverage Hours
- Severity 4: 9 hours during All Coverage Hours

Business Continuity

Talanos Business Continuity Plan (available on request and updated annually) has been tested and executed several times in the last couple of years – from rolling power cuts in Johannesburg to flooding in India and recently to the COVID-19 pandemic. We consistently receive positive feedback from our customers on our handling of a crisis with zero impact to our services. Simply, our approach to business continuity is honesty and transparency.

Our service delivery managers continuously communicate the status and capabilities of the teams throughout the disaster scenario and adapt the approaches as necessary to ensure uninterrupted service delivery. At the conclusion of the disaster and upon resuming normal



services, a review is conducted with the customer to learn from the response and update the BCP. The lessons learnt are shared with the customer.

The ability of Talanos to deliver services from one of three geographic locations differing in timezone, religion and politics has been crucial to our success and our customers have benefitted.

Documentation

Project Documentation

Extensive project documentation will be provided as part of the initial rollout. This documentation includes but is not exclusive to:

- Master Service Agreement and Statement of Work
- High-Level Solution Design
- Sensor Requirements, Network Configuration and Installation Guides
- Service Management Process Design
- High-Level Incident Response Plan
- SOAR Design
- Network IDS Design
- Log Retention Policy
- Service Strategy
- Implementation & Configuration Guide
- Operational Guide

Operational Documentation

Critical to the visibility and measurement of the success of the service is the operational documentation that is delivered throughout the month:

- Major Incident Report - docx (As required)
- Root Cause Analysis - docx (As required)
- Service Review - pptx (Monthly)
 - Vulnerability Management Progress - xlsx
 - Asset Discovery - xlsx
 - Events > Alarms > Incidents Statistics
 - SLA achievement
 - Program and milestones
 - Threat Hunting Progress
- SIEM Update Release Notes & New Features (As required)
- Customer Specific BCP (Annually)
- 3rd Party Risk Assessment (Annually)

Standards

It is important to take a practical stance on the implementation of controls and processes and to remember that the key ingredients of a successful cyber security monitoring and response service are creativity, curiosity and experience.

ITIL & ITSM – As a Managed Service, Talanos MSSP practices are founded in these standards and its Service Delivery Managers have been trained in these procedures to ensure measurable outcomes and continuous service improvement.

MITRE ATT&CK – Talanos uses this framework as a roadmap for threat hunting campaigns to ensure that all known TTPs have been tested against and prepared for.

NIST – Both AlienVault and Talanos have aligned aspects of their services to various NIST frameworks to guide security policy, control implementation and incident response.

Cyber Essentials – Talanos is Cyber Essentials certified.

ISO/IEC 27001:2013 – Talanos has adopted the standard for its information security management and although it has not yet been assessed, AlienVault has been assessed and certified. Talanos will be assessed as part of its CREST accreditation which it plans to undertake in 2023.

FAIR Institute – Talanos uses the FAIR institutes taxonomy for quantifying and communicating risk.

PCI-DSS, SOC 2, HIPAA – Talanos has assisted customers with achieving their PCI-DSS certification, having hosted auditors in the SOC to live test security controls and view the alerts raised. AlienVault has been assessed and certified against PCI-DSS, SOC2 and HIPAA.

Price

Please review the G Cloud 13 Pricing Document.

Implementation & Support

Build

One of the first activities the team would engage the customer in would be a risk assessment workshop to better understand the environment, stakeholders, data flows and areas of concern. Outputs from this session would be used to fine tune a project rollout plan and design that would see the first functional implementation complete in two weeks with the remaining configuration and sensors rolled out over the next few weeks. The major delaying factor in our experience has been the ability for the customer (or outsourced provider) to provision servers, configure networks and make firewall rule changes.

Detailed requirements and dependencies are normally discussed during the risk assessment workshop but can be provided during the contracting phase so as to “shortcut” the process and deliver the service quicker. Higher value integrations, such as into JIRA for ticket management and Cisco Umbrella for orchestration and remediation are introduced later in the process once a solution design has been completed, understanding both the business processes and technical aspects of the integration.

Actions for the AlienApp for Jira

Action	Function
Create a new issue from an alarm	Run this action to generate a new Jira issue directly from an alarm. This action is available when you launch a response action directly from an alarm or a response action in an orchestration rule .
Create a new issue from a vulnerability	Run this action to generate a new Jira issue directly from a vulnerability. This action is available when you launch a response action directly from a vulnerability .
Create a new issue from an event	Run this action to generate a new Jira issue directly from an event. This action is available when you launch a response action directly from an event .
Create a new issue from event based orchestration rule	Run this action to generate a new Jira issue directly from an orchestration rule that triggers from a matching event. This action is available when you launch a response action in an orchestration rule .

As sensors are rolled out and connected into the SIEM, the following process is followed to onboard systems:

- Deployment of HIDS (Hardware Intrusion Detection) agents
- Configuration of servers to forward logs into sensor
- Asset Discovery and Tagging
- Testing
- Vulnerability Scanning
- Event collection to form baseline (4 weeks)

These actions and tasks have been mapped into a high-level project plan broken into four phases that each focus on delivery the following components (the order to be agreed with the customer):

Phase 1 – Platform Go-Live (2 weeks)

1. Risk Assessment workshop (1 day)
2. Procure AlienVault license and configure single tenant for the customer (1 day)
3. Configure threat intelligence feeds (1 day)
4. High-Level solution design and shared requirements (2 days)
5. Provision Sensors
6. Network configuration to allow connectivity between sensors and AlienVault logger (1 day)
7. Configure and tune sensors for log and network data collection (3 days)
8. Go-Live (1 day)

Phase 2 – Service & SLA Go-Live (4 weeks)

1. Asset Discovery & Tagging (1 week)
2. Vulnerability Scan (1 week)
3. Network segment, sensor & agent design (2 days)
4. HIDS Agent Rollout (2 weeks)
5. HIDS Agent Asset Discovery & Tagging (2 weeks)
6. Service management process and incident response design (3 days)
7. AlienApp A configuration (3 days)
8. AlienApp for Dark Web Monitoring (1 day)
9. Global team introduction, sorting access and induction (3 days)
10. First service review (1 day)
11. SLA Go-Live (1 day)

Phase 3 – Services Integration Go-Live (6 weeks) – Defined with the customer

Phase 4 – Finalise strategic service plan (4 weeks) – Defined with the customer

A dedicated project manager will be assigned to manage the rollout of the project.

Run

With the platform and first sensor in place, the service is ready to begin. Talanos has Security Operations Centres (“SOCs”) in the UK, India and South Africa. Each SOC has implemented strict access controls such as, but not limited to:

- CCTV at points of entry and windows
- Security glass and reinforced walling
- 2-Factor biometrically controlled access
- Dedicated business grade fibre service with dedicated failover
- Recording devices such as cameras, phones, personal devices banned from SOC rooms

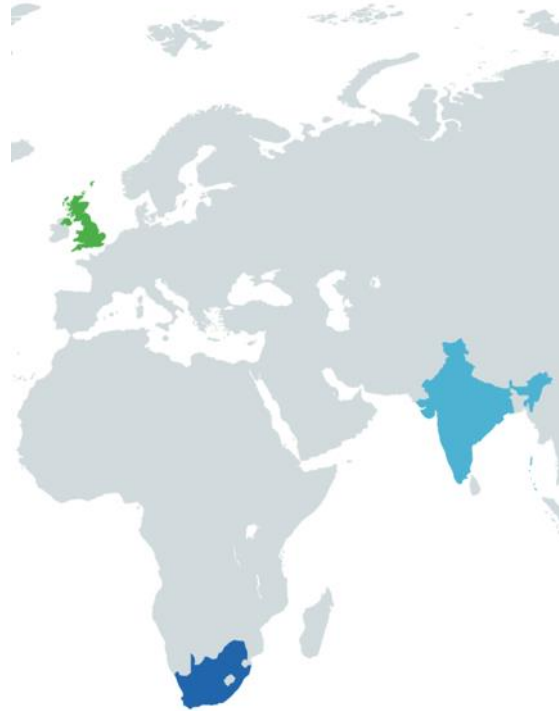
The SOC and team are regularly audited by customers as part of their PCI and SOC audits and customers are also invited to perform site visits (both planned and unplanned). With the teams spread geographically, this allows us to provide 17 hours of standard service coverage throughout the year regardless of bank holidays and religious holidays.

Operating Hours

Talanos teams can provide the following operating hours to UK businesses:

- All P1 requests are raised and incident response is performed on a 24 x 7 x 365 basis.
- The standard service as well as response to P2 – P5 incidents are handled Monday to Friday: 01:00 – 18:00 (UK Local Time) including bank and religious holidays.

Support requests outside of these hours (“Out of Service Support Operating Hours”) can also be pre-arranged with the consent of both Talanos and the customer at least 7 business days in advance. Such escalations for additional support and overtime requests will be made to the Talanos account manager who will coordinate with the relevant resources. Charges for these non-standard requests will be on an hourly Time & Materials basis.



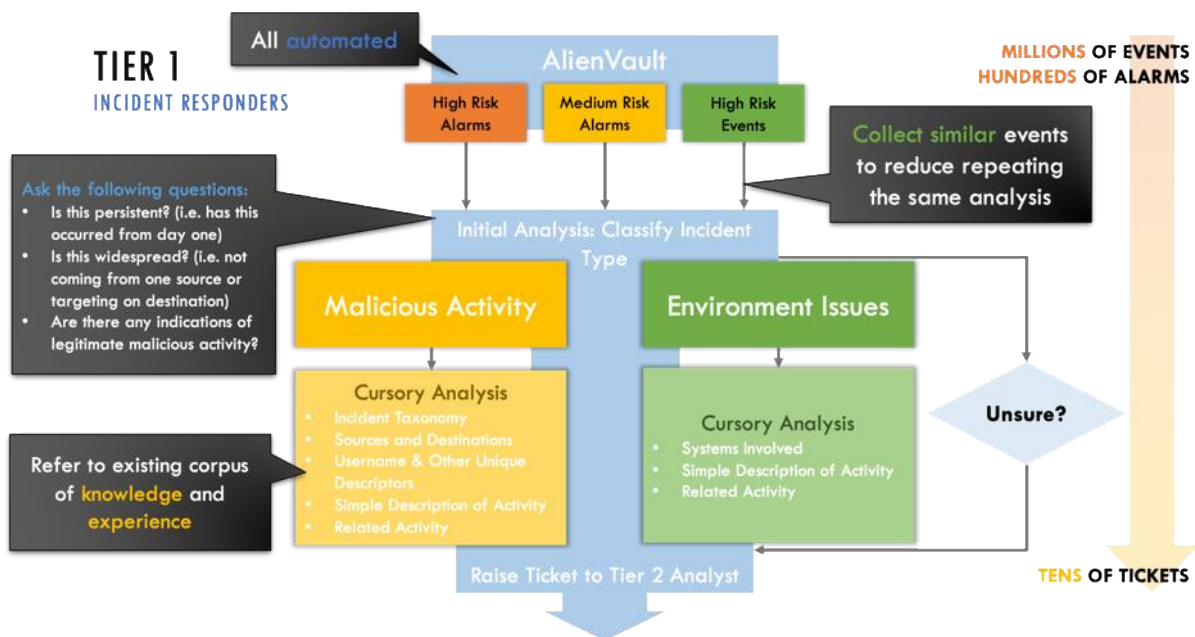
Managed Detection & Response Team

Teams across the UK, India and South Africa will be assigned to the customer account unless the customer requests that the service be run out of the UK only. Account and service management will be performed from the UK, Tier 1 security analysts are available in the UK, India and South Africa and Tier 2 incident responders are available in the UK and South Africa.

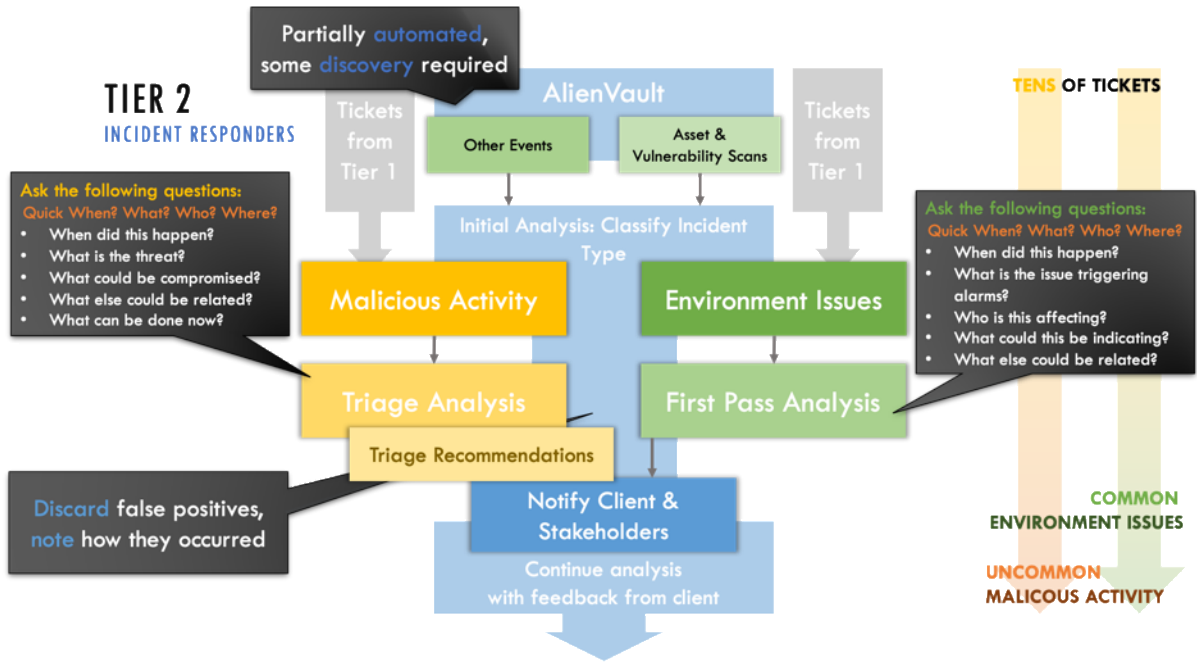
Incident Response Process

Drawing on several frameworks such as NIST SP800 61 Rev 2, Talanos have created a practical incident response procedure which caters for both the real-life operational incidents encountered as well as the advanced persistent threats for which the service was procured. In our experience, the behaviour and security events analysed can also indicate misconfiguration and human error in the administration of services and security appliances. These are just as valuable to highlight because their remediation protects against security incidents before they occur, and our response procedure calls these out separately. Our process also gives the appropriate weighting to the human analysis and intervention because it is our belief that human creativity and curiosity cannot be automated through security toolsets – in 100% of the threats detected and remediated, our toolset has made it easier for us to see deviations in the normal pattern of behaviour but our analysts were the key to understanding and contextualizing the threat.

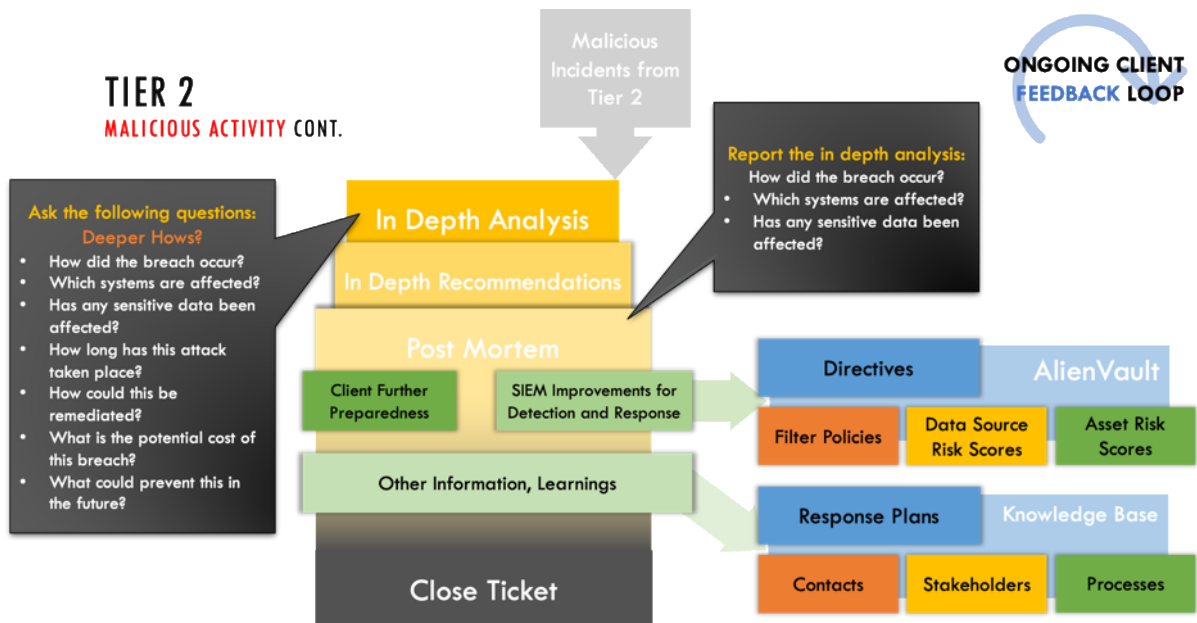
Tier 1 Response Procedure – two streams of incident analysed:



Tier 2 Response Procedure:



Tier 2 Response to Malicious Activity:

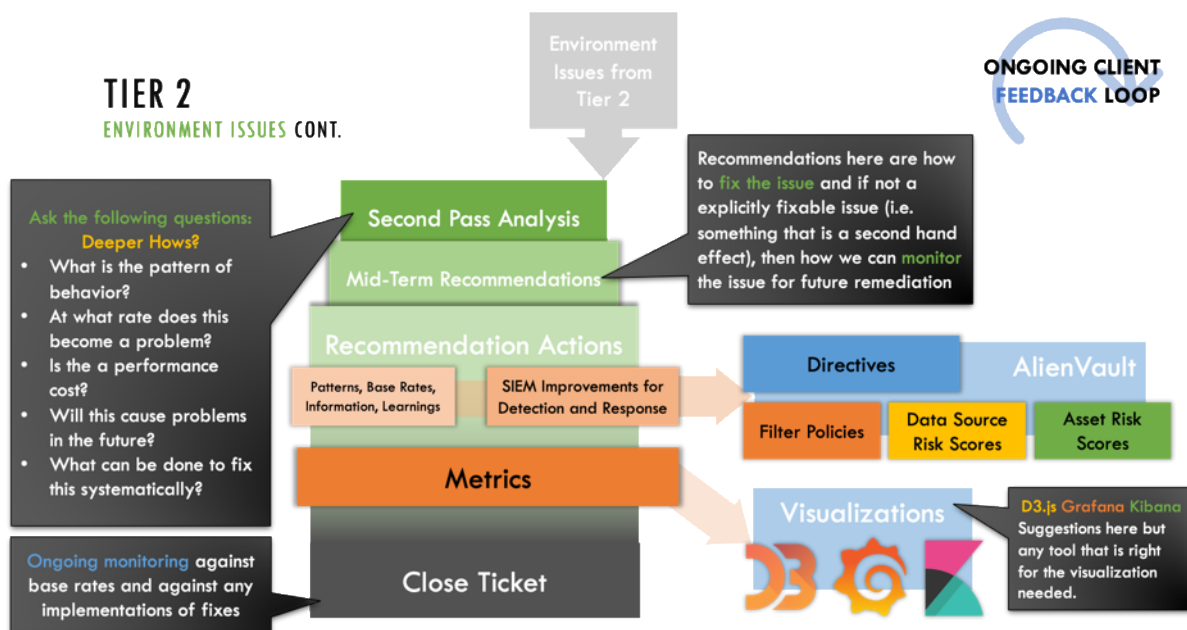


For the customer, the actual process of remediation would be carried out by the customer where the Talanos team would interact directly with the teams to provide analysis, recommendations, playbooks and support. Where the customer have previously approved it, automated remediation and orchestration (SOAR) could be implemented to Cisco Umbrella for example, to immediately block malicious IPs that have triggered an indicator of compromise or security incident on the SIEM platform.

Talanos used Manage Engine’s Service Desk for managing all incidents internally and where possible, we integrate with the customer’s ticketing system so that incidents can be

automatically raised and tracked on both sides. AlienVault also has a pre-built integration with Jira to add tickets for assets and log vulnerabilities and incidents automatically. The nature of the integration and which systems will be used for managing tasks will be discussed and agreed with the customer.

Tier 2 Response to Environmental Issues:



An example of an environmental issue discovered for a customer was that they had misconfigured a particular rule on their firewall that was allowing torrent downloads to their network. The particular employee had discovered this and misused company bandwidth to download many TB of their favourite TV series. Apart from being a misdemeanour, it had exposed the organisation to a potential threat and once the misconfiguration had been discovered, the firewall rule was fixed, and the hole closed.

Monitor

The trickiest part of providing a Cyber Security Managed Service is measuring its value. Nobody wants to experience a security incident and it's a relief when a month passes without one, but it makes it incredibly difficult to motivate for budget to continue monitoring and detecting incidents month after month that aren't there. Like an insurance policy, security monitoring is necessary but it doesn't need to become a grudge purchase. Apart from our daily analysis of security events, the team have other proactive security detection and service improvement tasks such as:

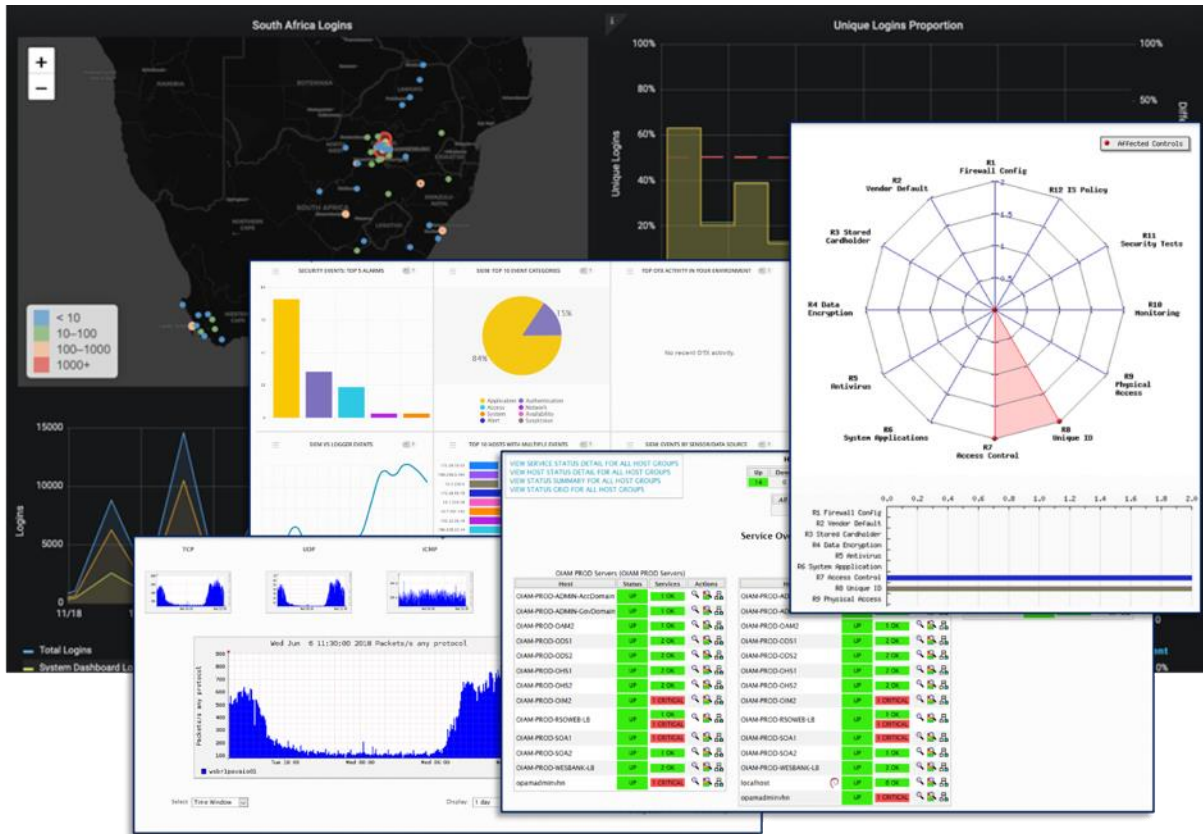
MITRE ATT&CK® Framework Mapping

5+ Users
 2 - 4 Users
 1 User
 0 Users
 No Labs Mapped

Organisation View

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Exfiltration
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable...	Exfiltration
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Exfiltration
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Prot...	Data Exfiltration
Replication Through Removable M...	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Local System	Custom Cryptographic Protocol	Altitude
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Network Shared Drive	Data Encoding	Exfiltration
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Removable Media	Data Obfuscation	Exfiltration
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data Staged	Domain Fronting	Exfiltration

- Threat hunting: Using the MITRE ATT&CK framework and our training partner Immersive Labs, we pick themes for the month focusing on various attack vectors in your organisation. We plan through and test aspects of the attack scenario and determine whether a) we getting the correct logs and event information from your environment to detect such a threat and b) our SIEM rules are tuned correctly to detect this threat. This typically results in the upliftment of audit rules and logging in certain aspects of your environment where we can test that the information we now receive is sufficient. The team also create customised playbooks at the end of the scenario so that a personalised response plan exists when these threats are detected. Mapping our threat hunting exercises in your environment is one of the easiest ways of measuring progress against your security posture and readiness in a practical sense (beyond NIST checkbox exercises).
- Analytics: Custom behavioural reporting and dashboards are developed focusing on the aspects of your environment that matter most to you. These could relate to the detection of new assets, the trends on how vulnerabilities detected are remediated over time as well as usage patterns of key services in your estate.



- Alignment with audit standards and frameworks: Our service is always developing and improving based on the latest frameworks and standards. We encourage formal audits of our environment, people and processes and are passionate about achieving certifications and accreditations (both in our personal capacities and as a business). Having successfully been engaged in a number of PCI audits, we are actively pursuing CREST accreditation which will improve and standardise our service over time. Aspects of the improvements and our journey are regularly mapped and communicated to customers.

Service Levels

For simplicity, Talanos will be adopting the customer’s existing service definitions for ease of management. The Priority Level of a ticket is calculated by assessing the business impact of the Incident or Service Request and the urgency to resolve. Impact and Urgency are classified as High, Medium and Low, and are defined as follows:

Impact Definitions:

- High: A Service has failed or is suffering severe degradation and is affecting a significant proportion of Users, or the Customer is at significant risk of loss of revenue, reputation or security.
- Medium: A Service has failed or is suffering degradation and is affecting a small proportion of Users, or an individual User is unable to work.
- Low: A Service has failed or is suffering degradation and is affecting a single user.

Urgency Definitions:

- High: Critical Customer business processes are at risk, and no workaround is available.
- Medium: No workaround is available but Customer business processes are not at risk, or Customer business processes are at risk but a workaround is available.
- Low: A workaround is available and no Customer business processes are at risk.

Priority Level:

		Impact		
		High	Medium	Low
Urgency	High	Priority 1	Priority 2	Priority 3
	Medium	Priority 2	Priority 3	Priority 4
	Low	Priority 3	Priority 4	Priority 5

Platinum Response SLA:

Talanos core business hours are: 01:00 – 18:00 (UK Local Time) where the following response SLA is provided:

Priority Level	Response SLA
P1	10 mins
P2	1 hr
P3	2 hr
P4	4 hr
P5	4 hr

All calls to the Talanos emergency support hotline are answered within 10 minutes.

Outside of the above Talanos core business hours, the following response SLA is provided:

Priority Level	Response SLA
P1	1 hr

Major Incident Report SLA:

Priority Level	Response SLA
P1	1 Business Day

Root Cause Analysis SLA:

Priority Level	Response SLA
ALL	5 Business Days

Service Credits

In respect of each calendar month, where Talanos fails to meet one (1) or more of the Service Levels, Service Credits shall be payable by Talanos in accordance with the following:

- Incident Response Rate: £200 for each incident that is not responded to within the Incident Response Time.
- Major Incident and Root Cause Analysis Report: £100 for each analysis document not provided within the Root Cause Analysis Time.

The maximum Service Credit that can accrue in any one calendar month is the equivalent of 10% of the monthly charges. If Talanos accrues the maximum allowed Service Credit (10% of the month charges) in 3 consecutive months or any 3 months in a rolling 6 month period then this shall be deemed a Material Breach and the service agreement may be cancelled. To the extent that a Service Credit is caused by an Incident that Talanos, acting reasonably, is required to refer to a third party, that period shall be disregarded, for so long Talanos can demonstrate to the customer's reasonable satisfaction that Talanos is using its reasonable endeavours to ensure that the third party resolves the Incident as soon as reasonably practicable.

Service Credits can be applied to monthly / annual service fees, used to fund non-standard requests or refunded.

Manage

Service Review Meetings

The progress on both SLA managed and non-SLA managed improvement tasks are regularly communicated in monthly review meetings which are an opportunity to share updates on:

- Service rollout against strategic plan
- Incidents raised and managed (measured against SLAs)
- Incidents of particular importance that might trigger strategic projects / improvements
- Threat hunting progress
- Environment analytics
- What works and doesn't work (outstanding dependencies and blockers)
- Feedback on the service and areas of focus
- Threat Intelligence and knowledge sharing

These meetings are scheduled between the customers key security personnel, service sponsor and Talanos project managers, service delivery managers and account manager. The review meetings are delivered in addition to the reporting mentioned in the Documentation section (which are standard service deliverables). Most customers who started on quarterly meetings have requested more frequent meetings (moving to monthly reviews) because of the critical nature and value of information shared in the session.

Key Personnel

Both Parties shall meet to review the Services and Service Levels every month. Talanos shall ensure the following people attend this meeting:

Account Manager

Security Program Manager

Service Delivery Manager
Offshore Service Delivery Manager (if applicable)

Transition

Although an uncomfortable topic and taking into consideration that Talanos wants to pursue a long-term partnership with the customer, we feel it's important that details around transitioning the service away from Talanos be discussed upfront. There may be many reasons why the customer would choose to end the relationship and it is for this reason that Talanos makes commitments around knowledge management, training and exit services – should they ever be required.

Knowledge Management & Training

Nearly all of the SLA and non-SLA managed deliverables under the service result in some form of documentation. This documentation covers the various architecture, design, configuration and operational aspects of the service. This documentation is hosted on the internal Talanos Sharepoint but can also be dropped into a central content management repository of the customer – which is advised. Any intellectual property developed by Talanos as part of the the customer engagement is shared between the customer and Talanos – in other words, both parties may continue to use the developed components for their own purposes even after any contractual engagement ends. The quality and quantity of documentation delivered should be sufficient for handover to another party and should enable the customer to upskill their own cyber security staff as their team grows.

Typically included in the proposal is a training seat on the AlienVault SIEM platform which should enable the customer's security team member to be in a position to navigate, operate and understand the core platform. Further, more detailed technical training can be purchased through Talanos, as required.

AlienVault USM Anywhere: Deploy, Configure, Manage (ANYDC) - Included

This two-day course begins with the deployment of USM Anywhere and walks students through the process of initial configuration of asset discovery, scanning, log collection, events, alarms, and rules. It then takes them through administering and reporting on the USM Anywhere environment and introduces them to the numerous resources available to assist them during and after this course. Our instructor-led courses feature challenging and immersive labs to provide a powerful hands-on learning environment.

AlienVault USM Anywhere: Security Analysis (ANYSA)

The AlienVault USM Anywhere: Security Analysis 2-day course provides security analysts with the knowledge and tools to fully leverage AlienVault USM Anywhere to perform analyst duties. Students benefit from instructor lectures, product demonstration, and hands-on practice labs which make up about 50% of the course. This comprehensive course ensures that you can use all of USM Anywhere's functions and features to detect and respond to security incidents and determine the extent of a compromise.

Launchpad for USM Anywhere – Self Paced Training

This self-paced course gives security engineers, analysts, and project team members an introduction to USM Anywhere. Get an overview of product setup, configuration and functionality so that you can start using USM Anywhere immediately,

Sharing knowledge and intelligence is a key pillar of Talanos partnership with its customers and helps to build a trusted relationship.

Exit Services

If at the end of the agreement, the customer decides to move the Services to another supplier or to an internal team, Talanos will provide all necessary cooperation and information as reasonably required to enable a smooth and orderly transition of the Services.

Such transition activity shall include but is not limited to:

- Provide documentation of systems and procedures used to provide the Service
- Copies of all inflight activity including open incidents and problems
- An up to date inventory of Software licences (licenses can be transferred so that the customer would not need to rebuild or migrate away from their existing SIEM – thus retaining access to the long-term archived log data)
- Access to Talanos staff for planning meetings, knowledge transfer and other transition related activity.

Talanos will attempt, wherever possible, to provide the Exit Services from resources already engaged and paid for under the Service.