

## AGREEMENT FOR THE PROVISION OF CYBER SECURITY SERVICES

This Agreement is made the    day of    2020 (“**Effective Date**”) between Cybanetix Limited whose registered office is at Tintagel House, 92 Albert Embankment, London, SE1 7TY, United Kingdom (“**Cybanetix**”) and [ ] whose registered office is at [ ] and whose company registration number is [ ] (“**Customer**”) of the other part.

### NOW IT IS HEREBY AGREED as follows:

#### DEFINITIONS

“**Affiliate**” means in relation to a body corporate, any other entity which directly or indirectly Controls, is controlled by, or is under direct or indirect common control with, that body corporate from time to time;

“**Confidential Information**” means trade secrets, confidential or proprietary information including but not limited to information concerning products, Customers, business accounts, financial or contractual arrangements or other dealings, transactions or affairs, reports, recommendations, advice or tests, source and object program codes, software, generic business objects, tools, techniques, development plans, frameworks, standards, methods, procedures, documentation, data or materials;

“**Charges**” means the fees and charges as set out generally in Schedule 2 or in an Order;

“**Customer**” means the registered business named in the contract and all Affiliates and/or subsidiaries thereof.

“**Critical Alerts**” means security related alerts in the form of logs which are generated by any security technology that is sent to the SIEM service. For clarity these logs could be named high severity, security, threat or similar names by different security vendors.

“**Emergency Change Request**” means a change arising as a result of a security breach, security incident or service impacting issue;

“**Force Majeure**” means accidents, natural disasters, fire or water, act of war, riot, strikes, lightening, electrical disturbance, damage during transportation by the Customer, local, national or global pandemic or epidemic, quarantine or health related lockdown, work performed by personnel other than the contracting party’s employees, sub-contractors or licensors or any other event beyond a party’s reasonable control;

“**Initial Term**” means the term set out in the Order and in default of such will be 36 months;

“**Intellectual Property Rights**” means patents, rights to inventions, copyright and related rights, trade marks, trade names, domain names, rights in get-up, rights in goodwill or to sue for passing off, unfair competition rights, rights in designs, rights in computer software, database rights, topography rights, moral rights, rights in confidential information (including know-how and trade secrets) and any other intellectual property rights, in each case whether registered or unregistered, and including all applications for, and renewals or extensions of, such rights, and all similar or equivalent rights or forms of protection in any part of the world;

“**Login Credentials**” means the URL, account name and password supplied by Cybanetix to the Customer that provides access to the Services;

“**Managed SIEM Service**” means the Cybanetix managed Security Information and Event Management service, providing setup, configuration and management of the SIEM Service, as may be more specifically defined in Schedule 1;

“**Order**” means the agreement entered into by Cybanetix and Customer incorporating these terms and conditions through which the Customer orders any part of the Services from Cybanetix, and

for the avoidance of doubt, should there be any conflict between terms of the order and this agreement, this agreement shall prevail;

**"Project Manager"** means the Cybanetix nominated point of contact for the Customer;

**"Service Level Agreement"** means the performance standards to which the Services are to conform, as notified from time to time by Cybanetix to the Customer;

**"Services"** means the services to be provided by Cybanetix, as described in Schedule 1;

**"SIEM Service"** means the Cybanetix basic in-house Security Information and Event Management service, that provides the technology but not setup, configuration and management, as may be more specifically defined in Schedule 1;

**"SOC Service"** means the Cybanetix Security Operations Centre service, providing incident and event monitoring of the Customer's IT infrastructure, as may be more specifically defined in Schedule 1;

**"Software"** means software which is pre-installed on the Cybanetix Private Cloud Service as part of the Services.

**"Specification"** means any specification or documentation supplied by Cybanetix from time to time detailing the functionality of the Service;

**"UEBA"** means user entity behavioural analytics, which included the behavioural monitoring of both users and devices.

## **1. PROVISION OF SERVICES**

- 1.1. Cybanetix shall supply to the Customer the Services in accordance with these terms.
- 1.2. Cybanetix shall ensure that the Services conform to the Service Level Agreement.
- 1.3. Cybanetix shall provide the Customer with the Login Credentials.
- 1.4. Cybanetix's personnel shall make reasonable efforts to adhere to any and all rules and regulations which the Customer applies to its employees and/or contractors and that are notified to Cybanetix in advance.
- 1.5. If performance of the Services is delayed or hindered for any of the following reasons the relevant Cybanetix obligation/s shall be deemed to be suspended until the delay or hindrance is removed:
  - 1.5.1 Force Majeure;
  - 1.5.2 any requested change in the Services;
  - 1.5.3 unreasonable delay on the part of the Customer or any person employed or engaged by the Customer;
  - 1.5.4 any delay or failure by the Customer to perform any of its obligations hereunder or otherwise caused by any act or omission of the Customer.

## **2. SOFTWARE**

- 2.1 The Software shall be pre-installed by Cybanetix on private cloud servers.
- 2.3 All Intellectual Property Rights in the Software, and any modifications or copies thereof, are and shall remain vested in Cybanetix or its licensors.
- 2.4 Subject to payment of the Charges by the Customer in accordance with the payment terms specified herein, Cybanetix grants to the Customer a non-exclusive, non-transferable licence to use the Software in object code form for the purpose of using the Services for the normal business purposes of the Customer while this Agreement remains in full force and effect.

Customer acknowledges that the provision of Software is made by Cybanetix strictly for use in conjunction with the Services and Customer agrees not to reproduce, copy, alter, modify, or add to the Software or any part thereof, nor to attempt or to allow a third party to attempt to reverse engineer, translate or convert the Software from machine readable to human readable form, except as permitted by applicable law or the terms under which the Software is licensed.

### **3. CYBANETIX RESPONSIBILITIES**

6.1 Cybanetix undertakes:

- 3.1.1 to use reasonable endeavours to deliver the Services in accordance with this Agreement;
- 3.1.2 to appoint a Project Manager as soon as possible;
- 3.1.3 to use reasonable endeavours to ensure that Cybanetix staff will obey the reasonable instructions and disciplines of the Customer's authorised representatives while on Customer's sites;
- 3.1.4 to use reasonable endeavours to employ competent staff to deliver the Services. Such staff shall remain under the direct control of Cybanetix whilst such staff are on Customer premises;
- 3.1.5 to use reasonable endeavours to prevent the passing of software viruses to Customer.
- 3.1.6 to maintain appropriate quality accreditation for the applicable services defined within schedule 1 and schedule 2 and provide certification upon request of the Customer.

### **4. THE CUSTOMER'S RESPONSIBILITIES**

4.1 The Customer undertakes:

- 4.1.1 to appoint a Project representative to liaise with Cybanetix in relation to the implementation of the Services;
- 4.1.2 to provide Cybanetix promptly with such information advice and assistance relating to the provision of the Services, including information relevant to applicable health, safety and security regulations. This information shall, at least, include a copy of the Customer's health and safety policy, relevant risk assessments associated with any aspects that may affect Cybanetix employees whilst on the Customer's premises, provide any appropriate training relating to health and safety and the name of the person appointed by the Customer to whom Cybanetix employees shall report any health and safety issues that may arise whilst employed on the Customer's premises;
- 4.1.3 to use reasonable endeavours to prevent the passing of software viruses to Cybanetix;
- 4.1.4 in the event that the delivery of the Services requires the attendance of Company staff on the Customer's premises or any other premises over which the Customer has control, to allow at no cost to Cybanetix such access as is necessary for Cybanetix to perform its obligations under this contract. During such attendance,

the Customer shall make available reasonable office accommodation including the use of desks, telephone, fax and copying services;

- 4.1.5 that any property supplied to Cybanetix by or on behalf of the Customer, including any items listed in the Order, shall be held and worked upon by Cybanetix at the Customer's risk. Cybanetix shall not be liable for any loss or damage to any such property except to the extent such loss or damage was caused by the negligence of Cybanetix or its employees or agents;
- 4.1.6 to keep the Login Credentials confidential and to only log in with the same, to ensure that it exits from its account at the end of each session, and to immediately notify Cybanetix in writing of any unauthorised use of its Login Credentials. The Customer is fully responsible for all activities that occur using its Login Credentials. Cybanetix will not be liable for any loss or damage arising from the Customer's failure to comply with these requirements;
- 4.1.7 to indemnify and keep indemnified Cybanetix its employees or agents against all claims, actions, losses, damages, costs and expenses which may be brought against or incurred or suffered by Cybanetix its employees or agents in connection with the use of the Services, unless these claims, actions, losses, damages, costs or expenses have been caused by the negligence of Cybanetix employees or agents.

## **5. WARRANTY AND LIMITATIONS**

### **5.1 Cybanetix warrants that:**

- 5.1.1 it has received all necessary consents, licences and permissions required to perform its obligations under this contract;
- 5.1.2 it will use reasonable care and skill in providing the Services but does not warrant that such provision will achieve any result other than as may be expressly specified by Cybanetix in writing.

### **5.2 Cybanetix shall not be responsible for products or services supplied which incorporate or are based upon information or materials supplied by the Customer or third parties. Responsibility for decisions taken on the basis of advice given by Cybanetix will remain with the Customer.**

### **5.3 Cybanetix warrants that:**

- 5.3.1 it is entitled to sell and license the Software and that it has received all necessary consents, licences and permissions required to perform its obligations under this Agreement;
- 5.3.2 the Software shall, for a period of ninety (90) days from the date of its delivery to Customer ("**Warranty Period**"), be capable of performing the functions described in the Specification in all material respects.

However Cybanetix does not warrant that the use of the Services or Software will be uninterrupted or error-free.

### **5.4 The Customer acknowledges that in providing the SOC Service Cybanetix cannot guarantee that viruses, worms, trojans, bots or other critical security events will be detected through Cybanetix's monitoring, although Cybanetix will use its reasonable endeavours to do so. Accordingly Cybanetix cannot accept any liability to the extent that such security events occur notwithstanding the provision of the SOC Service and monitoring by Cybanetix.**

- 5.5 Where the Customer receives the Managed SIEM Service the Customer is responsible for the monitoring of its IT infrastructure and acknowledges that Cybanetix cannot therefore prevent or detect viruses, worms, trojans, bots or other critical security events. Accordingly Cybanetix cannot accept any liability to the extent that such security events occur. The same is true of the SIEM Service.
- 5.6 The Customer accepts responsibility for the selection of the Services to achieve its intended results.
- 5.7 If, within the Warranty Period, the Customer notifies Cybanetix in writing of any defect or fault in the Software in consequence of which it fails to conform in all material respects to the Specification, and such defect or fault does not result from the Customer, or anyone acting with the authority of the Customer having amended the Software or used it outside the terms of the licence granted, for a purpose or in a context other than the purpose or context for which it was designed or in combination with any other software not provided by Cybanetix, Cybanetix shall, at Cybanetix' option, do one of the following:
  - 5.7.1 repair the Software; or
  - 5.7.2 replace the Software,provided that the Customer provides all the information that may be necessary to assist Cybanetix in resolving the defect or fault, including sufficient information to enable Cybanetix to re-create the defect or fault.
- 5.8 Cybanetix shall not be liable for any breach of warranty if caused by neglect, improper installation or testing of the Services (other than by Cybanetix), attempts by the Customer to modify the Services, or any use of the Services other than as advised by Cybanetix.
- 5.9 Cybanetix shall ensure that it (and its officers, employees, directors or any other person acting on its behalf) will comply with all applicable local and international anti-corruption legislation from time to time in force, including but not limited to the United Kingdom Bribery Act 2010.
- 5.10 In performing its obligations under the agreement, Cybanetix shall and shall ensure that it and each of its subcontractors shall: (a) comply with the Modern Slavery Act 2015; and (b) take reasonable steps to ensure that there is no modern slavery or human trafficking in the Cybanetix's or subcontractors' supply chains or in any part of their business.
- 5.11 EXCEPT AS EXPRESSLY PROVIDED IN THIS AGREEMENT ALL WARRANTIES, CONDITIONS, UNDERTAKINGS OR TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, INCLUDING WITHOUT LIMITATION ANY IMPLIED CONDITION OR WARRANTY OF SATISFACTORY QUALITY OR FITNESS FOR PURPOSE, ARE EXCLUDED.

## 6. INTELLECTUAL PROPERTY RIGHTS INDEMNITY

- 6.1 Cybanetix shall defend, indemnify, and hold harmless Customer against any third party claim, suit, or proceeding ("**Claim**") arising out of, related to, or alleging infringement of any Intellectual Property Rights resulting from Customer's use of the Services or exercise of its rights to the Software granted in this Agreement. Customer shall give Cybanetix sole control of the defence and settlement of any Claim and provide all necessary assistance and support.

- 6.2 If any part of the Software is, or may become, the subject of any Claim or in the event of any adjudication that any part of an item of Software does so infringe, Cybanetix may at its expense elect to do either one of the following: (i) procure for Customer the right to use the Software or the affected part thereof; (ii) replace the Software or affected part thereof with other suitable products; (iii) modify the Software or affected part thereof to make it non-infringing; or (iv) if none of the foregoing remedies are commercially feasible, refund to Customer an amount equal to a three year straight line depreciation of the Charges paid for the Software.
- 6.3 Cybanetix shall have no obligations under this Clause 6 with respect to any Claim to the extent it is based upon (i) the use of any version of the Software other than a current release of the Software; (ii) the use of any version of the Software which has been altered other than by Cybanetix; (iii) the combination, operation or use of the Software with software, hardware or other materials other than as specified by Cybanetix; (iv) use of technology, technological information, designs, plans or specifications furnished by Customer; or (v) use of the Software for a purpose other than that for which it was designed or contemplated. This Clause 6 states the entire liability of Cybanetix with respect to the infringement of the Intellectual Property Rights of third parties.

## 7. CHARGES

- 7.1 In consideration of the provision of the Services by Cybanetix, the Customer will pay to Cybanetix the Charges.
- 7.2 Unless otherwise specified in an Order all Charges are payable within 30 days of receipt of Cybanetix's invoice.
- 7.3 If there is any delay in payment Cybanetix shall be entitled (without prejudice to any other right or remedy, and as well after as before any judgment):
- 7.3.1 to suspend any further performance of the Services after giving Customer 5 days' written notice for such period as Cybanetix feels is appropriate but no longer than payment is received by Cybanetix, and
  - 7.3.2 to charge interest on all outstanding monies due whether before or after judgement at the rate of 2% above the base rate of The Royal Bank of Scotland PLC from the date of the invoice to the date of payment.
- 7.4 If Cybanetix incurs further costs in addition to the Charges whether in respect of time or materials as a result of any events listed below, Cybanetix shall be entitled to charge the Customer in respect of such time and materials and the Customer shall pay such charges within 30 days of receiving the invoice for the same:
- 7.4.1 where a change is requested or sanctioned by the Customer;
  - 7.4.2 where delay in the delivery of the Services has arisen and is attributable to the fault of the Customer or any person employed or engaged by the Customer (other than Cybanetix);
  - 7.4.3 where the Customer following a written request by Cybanetix has not delivered by the agreed time, suitable information or agreement of documents.
- 7.5 Cybanetix shall be entitled, upon giving the Customer 30 days prior written notice to that effect, to vary the Charges as may be fair and reasonable to reflect (i) a material, unavoidable increase in the cost of Software charged by licensors, or (ii) where a key supplier to Cybanetix invoices in a currency other than UK Pounds Sterling, a material adverse change in the exchange rate of UK Pounds Sterling against such currency.

- 7.6** The provisions of this Clause 7 are without prejudice to any other rights and remedies which Cybanetix may possess.
- 7.7** Cybanetix may apply surcharges, as specified in the Charges, should any portion of delivery of the Services be scheduled outside of normal local working hours at the request of the Customer.
- 7.8** All cost and fees are exclusive of any applicable taxes. Customer agrees to pay and bear the liability for such taxes that include, but are not limited to, Value Added Tax.
- 7.9** The currency in which the Charges are to be paid will be UK Pounds Sterling.

## **8. CHANGE CONTROL**

- 8.1** The Customer's Project Representative and the Cybanetix Project Manager shall meet regularly to discuss matters relating to the delivery of the Services. If either party wishes to change the scope of the Services, it shall submit details of the requested change to the other in writing.
- 8.2** If either party requests a change to the scope or execution of the Services, Cybanetix shall, within a reasonable time, provide a written estimate to the Customer of:
- 8.2.1** the likely time required to implement the change;
  - 8.2.2** any variations to the Cybanetix's fees and charges arising from the change;
  - 8.2.3** the likely effect of the change on the estimated timescales; and
  - 8.2.4** any other impact of the change on the terms of this Agreement or any applicable Order.
- 8.3** If Cybanetix requests a change to the scope of the Services, the Customer shall not unreasonably withhold or delay consent to it.
- 8.4** If the Customer wishes Cybanetix to proceed with the change, Cybanetix has no obligation to do so unless and until the parties have agreed in writing on the necessary variations to its charges, the estimated timescales and any other relevant terms of this Agreement and any applicable Order to take account of the change.

## **9. DATA PROTECTION**

- Both parties will comply with all applicable requirements of the Data Protection Legislation. This Clause 8 is in addition to, and does not relieve, remove or replace, a party's obligations under the Data Protection Legislation.
- The parties acknowledge that for the purposes of the Data Protection Legislation, the Customer is the data controller and Cybanetix is the data processor (where Data Controller and Data Processor have the meanings as defined in the Data Protection Legislation).
- Without prejudice to the generality of Clause 8.1, the Customer will ensure that it has all necessary appropriate consents and notices in place to enable lawful transfer of the Personal Data to Cybanetix for the duration and purposes of this Agreement.
- Without prejudice to the generality of Clause 8.1, Cybanetix shall, in relation to any Personal Data processed in connection with the performance by Cybanetix of its obligations under this Agreement:

- process that Personal Data only on the written instructions of the Customer unless otherwise required under the Data Protection Legislation;
  - ensure that it has in place appropriate technical and organisational measures to protect against unauthorised or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data, appropriate to the harm that might result from the unauthorised or unlawful processing or accidental loss, destruction or damage and the nature of the data to be protected, having regard to the state of technological development and the cost of implementing any measures (those measures may include, where appropriate, pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of its systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the technical and organisational measures adopted by it);
  - ensure that all personnel who have access to and/or process Personal Data are obliged to keep the Personal Data confidential; and not transfer any Personal Data outside of the UK or the European Economic Area unless the prior written consent of the Customer has been obtained and the following conditions are fulfilled:
    - the Customer or Cybanetix has provided appropriate safeguards in relation to the transfer;
    - the data subject has enforceable rights and effective legal remedies;
    - Cybanetix complies with its obligations under the Data Protection
    - Legislation by providing an adequate level of protection to any Personal Data that is transferred; and
    - Cybanetix complies with reasonable instructions notified to it in advance by the Customer with respect to the processing of the Personal Data;
  - assist the Customer in responding to any request from a Data Subject, at the Customer's cost, and in ensuring compliance with its obligations under the Data Protection Legislation with respect to security, breach notifications, impact assessments and consultations with supervisory authorities or regulators;
  - notify the Customer without undue delay on becoming aware of a Personal Data breach;
  - at the written direction of the Customer, delete or return Personal Data and copies thereof to the Customer on termination of the agreement unless required by Applicable Law to store the Personal Data; and maintain complete and accurate records and information to demonstrate its compliance with this Clause 8.
- Where the Customer consents to Cybanetix appointing a third-party processor of Personal Data under this agreement, Cybanetix confirms that it has entered or (as the case may be) will enter with the third party processor into a written agreement incorporating terms which are substantially similar to those set out in this Clause 8. As between the Customer and

Cybanetix, Cybanetix shall remain fully liable for all acts or omissions of any third-party processor appointed by it pursuant to this Clause 8.

- The Customer agrees and acknowledges that Cybanetix is reliant upon the Customer for direction as to the extent to which Cybanetix is entitled to use and process Personal Data disclosed by Cybanetix. Accordingly, Cybanetix shall not be liable for any claim brought by a data subject arising from any act or omission by Cybanetix, to the extent that any such act or omission results from the Customer's instructions.
- In this Clause, the following definitions shall apply:

“Data Protection Legislation” means the General Data Protection Regulation ((EU) 2016/679), as implemented by the Data Protection Act 2018, as amended or updated from time to time;

“Personal Data” and “Data Subject” have the meanings ascribed in the Data Protection legislation.

- **CONFIDENTIALITY**

- Each party shall, during the term of this Agreement and for a period of 12 months thereafter, keep confidential all, and shall not use for its own purposes nor without the prior written consent of the other disclose to any third party any, information of a confidential nature (including, without limitation, trade secrets and information of commercial value) which may become known to such party from the other party and which relates to the other party or any of its Affiliates, unless such information is public knowledge or already known to such party at the time of disclosure, or subsequently becomes public knowledge other than by breach of this licence, or subsequently comes lawfully into the possession of such party from a third party.
- The terms of this Agreement are confidential and may not be disclosed by a party without the prior written consent of the other party.
- The provisions of this Clause 9 shall remain in full force and effect notwithstanding termination of this licence for any reason.

- **NON-SOLICITATION**

Each party agrees not to directly solicit the services of any employee of the other party who has been assigned to performing services under this Agreement during the term of the Agreement and for six months after the last services are provided under the Agreement.

- **SURVIVAL OF TERMS**

The provisions of this Agreement that by their nature extend beyond the termination of the Agreement will survive termination or expiration of the Agreement.

- **LIABILITY**

- Neither party shall be liable to the other party whether in tort (including negligence or statutory duty), contract or otherwise for any financial, special or consequential loss (including any loss of revenues, anticipated savings, profits, business or contracts) arising from the provision of the Services or any defect therein or the delayed performance thereof.
- A party (“liable party”) will be liable to the other party for direct damage or injury to the other party's property or person to the extent that such damage or injury is directly caused by the negligence of the liable party's employees or agents. Except as otherwise set out in this

Clause and subject to Clause 13.3, a party's total liability for damages (including damage caused by breach of contract, tort and breach of statutory duty) shall not exceed the total Charges paid under this Agreement in the period of 12 months before the event giving rise to the liability.

- Cybanetix's sole liability in respect of defective or delayed performance of the Services shall be limited to making good at its own expense such as defect or delay.
- Save as expressly stated in this contract, all warranties, conditions, terms, undertakings and representations including but not limited to those implied by statute, common law, custom, course of dealing or otherwise are hereby excluded to the fullest extent permitted by law.

- **NO PARTNERSHIP OR AGENCY**

Nothing in this Agreement, and no course of dealing between the parties, shall be construed to create an employment or agency relationship or a partnership, or joint venture between Cybanetix and the Customer or between a party and the other party's employee, agent, or representative. Neither Cybanetix nor the Customer has the authority to bind the other, to incur any liability or otherwise act on behalf of the other.

- **FORCE MAJEURE**

No party shall be liable to the other for any delay or non-performance of its obligations under this licence arising from Force Majeure. For the avoidance of doubt, nothing in this Clause 13 shall excuse the Customer from any payment obligations under this Agreement. The party affected by the Force Majeure shall give written notice to the other party on its occurrence along with the estimated duration. If the force majeure persists for a period of 60 days or more, the Customer may terminate this agreement by giving written notice to that effect.

- **ASSIGNMENT**

Either party may assign all of its rights and obligations under this Agreement to its owner or successor in business by giving notice in writing to the other party. This Agreement may not be assigned or otherwise transferred by a party, except to an Affiliate, without the prior written consent of the other party, which consent shall not be unreasonably withheld. Subject to the foregoing, this Agreement shall be binding upon and inure to the benefit of the parties hereto and their respective successors and permitted assigns.

- **TERM AND TERMINATION**

- This Agreement becomes effective from the Effective Date and except as may be terminated hereunder, will continue in full force and effect for the Initial Term.
- This agreement provides a continuous service and will automatically enter successive 12-month rolling contract periods (each a "Renewal Term") at the expiry of the Initial Term unless terminated by the Customer. Any notification of termination of the agreement must be given by Customer in writing to Cybanetix at least 60 days prior to the expiry of the Initial Term or each relevant Renewal Term. For the avoidance of doubt if such notice is not given in the correct manner and by the required date this Agreement will continue in full force and effect for the full duration of the Renewal Term and any further Renewal Term that is commenced. Excluding termination by the Customer pursuant to Clause 17.3, termination of this Agreement before the expiry of the Initial Term or any Renewal Term will render the

Customer liable to pay all Charges up to the end of the relevant term, unless otherwise agreed by Cybanetix.

- Either party shall have the right, without prejudice to its other rights or remedies, to terminate this contract immediately by written notice to the other if the other party:

17.2.1 is in material or persistent breach of any of its obligations under this contract and either that breach is incapable of remedy or the other party shall have failed to remedy that breach within 30 days after receiving written notice requiring it to do so;

17.2.2 is unable to pay its debts (within the meaning of Section 123 of the Insolvency Act 1986) or becomes insolvent or an order is made or a resolution passed for the administration, winding-up or dissolution of the other party (otherwise than for the purposes of a solvent amalgamation or reconstruction) or an administrative or other receiver, manager, liquidator, administrator, trustee or similar officer is appointed over all or any substantial part of the assets of the other party or the other party enters into or proposes any composition of arrangement with its creditors generally or anything analogous to the foregoing occurs in any applicable jurisdiction.

#### 17.3 Upon expiry or termination of this contract:

17.3.1 all rights and obligations of the parties under this contract shall automatically terminate, except for such rights of action as shall have accrued prior thereto and any obligations which expressly or by implication are intended to come into or continue in force after such expiry or termination;

17.3.2 the Customer shall pay all monies due under the contract up to and including the date of termination;

17.3.3 Each party shall, at the request of the other party, return any materials and Confidential Information provided to it by that other party.

### 18. NOTICES

18.1 All notices to be given under this Agreement to Cybanetix shall be addressed to the Managing Director at the address given at the first page of this Agreement.

18.2 All notices to be given under this Agreement to the Customer shall be sent to Customer at the address given at the first page of this Agreement.

18.3 All communications sent by prepaid post to the last given address of the addressee shall be deemed to have been given when in the ordinary course they would be delivered.

### 19. SEVERABILITY

If any condition or provision or any part of this Agreement shall be declared void or unenforceable or become void unenforceable invalid or illegal for any reason whatsoever then the other conditions and provisions of the Agreement shall remain in full force and effect

insofar as the offending condition or provision can be severed and the remainder of the Agreement can properly continue to operate.

## **20. DISPUTE RESOLUTION**

- 20.1 The parties will attempt in good faith to resolve any dispute or claim arising out of or relating to this Contract promptly through negotiations between the respective senior executives of the parties who have the authority to settle the same.
- 20.2 If the matter has not been resolved by the negotiations referred to in Clause 20.1 within 30 days of the initiation of such procedure (or such other period as the parties may agree), the dispute shall be referred to the English Courts.

## **21. WAIVER**

No forbearance or indulgence by either party in enforcing any condition of this Agreement shall prejudice or restrict that party's rights or powers under this Agreement and no waiver of any breach shall operate as a waiver of any subsequent or continuing breach.

## **22. COUNTERPARTS**

This Agreement may be executed in counterparts, each of which shall be deemed to be original, but all of which together shall constitute a single instrument.

## **23. THIRD PARTIES**

A person who is not party to this Agreement has no rights under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of this Agreement.

## **24. STATUS OF PRE-CONTRACTUAL STATEMENTS**

Each of the parties acknowledges and agrees that in entering into this Agreement it does not rely on any undertaking, promise, assurance, statement, representation, warranty or understanding (whether in writing or not) of any person (whether party to this Agreement or not) relating to the subject matter of this agreement other than as expressly set out in this Agreement.

## **25. GOVERNING LAW AND JURISDICTION**

This Agreement shall be governed by and construed in accordance with the Laws of England and the parties agree to submit to the exclusive jurisdiction of the English Courts.

SIGNED FOR AND ON BEHALF OF CYBANETIX LIMITED

BY \_\_\_\_\_

NAME: Martin Jakobsen

TITLE: Director

DATE [ ]

SIGNED FOR AND ON BEHALF OF [ ]

BY \_\_\_\_\_

NAME \_\_\_\_\_

TITLE \_\_\_\_\_

DATE \_\_\_\_\_

## SCHEDULE 1 Description of Services

### 1. Service Outline

The SOC is an 'all inclusive' managed SIEM and outsourced Security monitoring solution comprising Centralised log aggregation and management, 24x7x365 security monitoring, threat detection, alerting, investigation, and response.

The SOC service requires a Security Information and Event Management (SIEM) and log storage platform for the collection of security related logs from devices, systems, applications, and cloud services consumed by the customer. Cybanetix partners with, and utilises the Exabeam Security Intelligence Platform, a market leader in SIEM and User Behaviour Analytics.

The Exabeam SIEM technologies ingest live data feeds from collector agents, syslog services and APIs, and is complementary to a layered cyber security strategy. The service enables customers to log and alert on events from all their data sources such as servers, desktops and security technologies etc.

The SOC provides a managed 'service wrap' which utilises the Exabeam SIEM technologies to monitor, identify, classify and verify cybersecurity threats and malicious activities, and to support Incident Management processes and remediation of events and incidents through log analysis on behalf of the customer. The SOC is also responsible for maintaining/managing the SIEM platforms functionality and configuration. SIEM Platform hosting is provided by Exabeam as part of their SaaS Cloud service. The Cybanetix SOC includes:

- A fully managed suite of SIEM Technologies (SaaS hosted).
- Outsource of Incident Management processes, i.e. Monitoring, Detection, Identification, Classification and Verification of cyber security threats and malicious activity, to the Cybanetix 24x7x365 SOC.
- Remedial recommendations provided to the customer as a result of investigative processes.

The Cybanetix SOC comprises a team of skilled Security Analysts working around the clock to monitor, investigate and respond to cybersecurity incidents and events that may take place within the customers' network. Threats can happen at any time, night, or day. It is critical that such events can be detected at the earliest opportunity and notified to the customer, allowing them to take the necessary actions to kill/mitigate/contain such threats and minimise any damage their systems, data, business, and reputation.

Please note that threat remediation activities performed by the Cybanetix SOC are out of scope of this service, however the SOC will advise customers on appropriate actions for containment and remediation in the event of a security incident.

### 2. The SOC Service

The SOC is underpinned by the following Exabeam SIEM technology stack. Licensing for the Exabeam technology components can either be procured via Cybanetix as part of the SOC service, or via alternative means.

#### Licensing requirements

1. SIEM technology licensing as defined and agreed based on customer requirements.
  - a. Exabeam Advanced Analytics

- b. Exabeam Entity Analytics
- c. Exabeam Data Lake
- d. Exabeam Cloud Connectors
- e. Exabeam Incident Responder
- f. Exabeam Case Manager
- g. Exabeam SaaS Cloud storage (Frozen/Archive)

## Hosting

The SOC Service utilises Exabeam SIEM technologies hosted and delivered from within Exabeam's SaaS Cloud environment (located within Google Cloud Platform). Exabeam SaaS includes the full breadth of Exabeam's collection, detection, investigation, and response capabilities as a cloud-based service. It should be noted that SIEM platform availability and technical support for the hosting environment is subject to the Service Levels provided by Exabeam as part of the SaaS cloud licensing.

## SIEM Setup & Deployment

1. Joint completion of SIEM cloud on-boarding form
2. On-site engineering support for the customer setup of log sources
3. Setup of IPSEC VPN to one or more customer access points
4. Setup of Exabeam component platform instances
5. On-boarding of log sources to Exabeam Data Lake
6. Import log parsers
7. Write new log parsers
8. Setup of dashboards
9. Setup of alerting
10. Setup user control/access
11. Setup processing pipelines
12. Define retention policies
13. Setup log back-up
14. Test alerts and dashboards
15. Setup and integration of Exabeam components:
  - a. Advanced Analytics
  - b. Entity Analytics
  - c. Case Manager
  - d. Incident Responder
  - e. Cloud Connectors

## SIEM Platform Management

1. Moves, Adds and Changes ('MACs\*') for new and decommissioned log sources
  - a. MACs for inputs
  - b. MACs for grok pattern
  - c. MACs for log parsers
2. MACs for Dashboards
3. MACs for Alerts
4. MACs for new event processing

5. MACs for threat feeds and threat correlation
6. MACs for correlation rules
7. SIEM platform/systems faults, P1-P3 (see service KPI's)
8. Ensure continuous compliance with relevant compliance schemes

\*A MAC is limited to service requests not exceeding 5 individual changes and is not time limited or specific. Any request that does not meet this limitation, will be dealt with as a project and may result in additional professional service charges.

## SOC Service Setup

1. SIEM Support
  - a. Agree communication matrix for service requests, faults, and escalations
  - b. Agree standard/pre-approved configuration tasks/categories (e.g. new dashboard or log source)
  - c. Agree a change control process for complex/non-standard configuration changes to the SIEM platform
2. Security Incident Handling
  - a. Agree communication matrix for security incident notification, management, and investigation
  - b. Setup and agree any remedial requirements where Cybanetix are partly managing, co-managing or fully managing service for the customer
  - c. Agree a customer change control to avoid false event identification and escalations
  - d. Define security log sources in use by the customer ('this may have been done as part of SIEM setup')
  - e. Agree alerting conditions
  - f. Setup reporting for customer compliance requirements
  - g. High Priority users' needs to be defined\*

## Security Monitoring:

1. Cybanetix will process all events in the SIEM platform and all eligible events will be investigated by a Cybanetix SOC analyst. Events that are eligible for investigations are:
  - a. Critical alerts from security log sources
  - b. High severity threats identified by threat intelligence feeds
  - c. Notable users identified by Exabeam Advanced Analytics
  - d. High profile users exhibiting 30+ threat score in Exabeam Advanced analytics
  - e. Alerts on all predefined alerting criteria
  - f. Customer reported incidents
2. Incidents will be investigated, and an incident analysis and remedial recommendation will be supplied in line with SLA
3. Cybanetix will provide reporting on security events
  - a. Automated compliance reporting
  - b. Monthly Security and incident reporting

\*The number of high priority users is limited to 3% of the licensed user base

## Incident Response:

The Cybanetix SOC will setup and run automated Incident Response actions for mutually agreed SOC use cases/playbooks. Examples include (but not limited to):

- Automated containment/quarantine
  - Achieved through integration with customers' existing security enforcement toolsets, e.g:
    - Endpoint Protection
    - Next Generation Firewalls
    - Email Security
    - Active Directory (account disablement)
- Threat verification/enrichment
  - Integration with external intelligence platforms:
    - 3<sup>rd</sup> Party Sandbox
    - Vendor published CVEs
    - External Intelligence feeds

Where a Major Incident is declared, the incident will immediately be escalated to the operational management of Cybanetix who will instigate and orchestrate the MI process. When working with a customer, Cybanetix can either manage the incident response or support the incident response, representing the SOC and proving the telemetry, reporting and remedial recommendation for the incident management process and a management teams.

The SOC service includes the orchestration of the MI and the interface to the SOC, however any human input required for remedial response such as re-configuration of customer infrastructure is subject to consultancy and engineering charges which are charged on a time and materials basis.

## SOC Service KPI's

Service Metric	Service Criteria	Target Service Level
Time to notify the customer of an event classified as critical by customer designated method	Less than 15 minutes	99%
Time to complete first triage playbooks for critical incidents	Less than 1 hour	99%
SIEM Platform faults – P1 Service down/unavailable/no ingestion of logs	Response within 30 minutes	99.5%
SIEM Platform faults – P2 Reduced service/performance	Response within 2 hours	99.5%
SIEM Platform faults – P3 Minor/isolated issues not affecting the main service, e.g. single Log source not working (during standard hours only)	Response within 8 hours	99.5%
Service Requests response (during standard hours only)	Response within 8 hours	99.5%

## SOC Service Hours

Security Incidents are responded to 24x7x365.

P1/P2 SIEM Platform faults are responded to 24x7x365.

P3 SIEM Platform faults are responded Mon-Fri 9am-5:30pm (GMT), excluding bank holidays.

Service requests are responded to Mon-Fri 9am-5:30pm (GMT), excluding bank holidays.

## Identification of events of interest

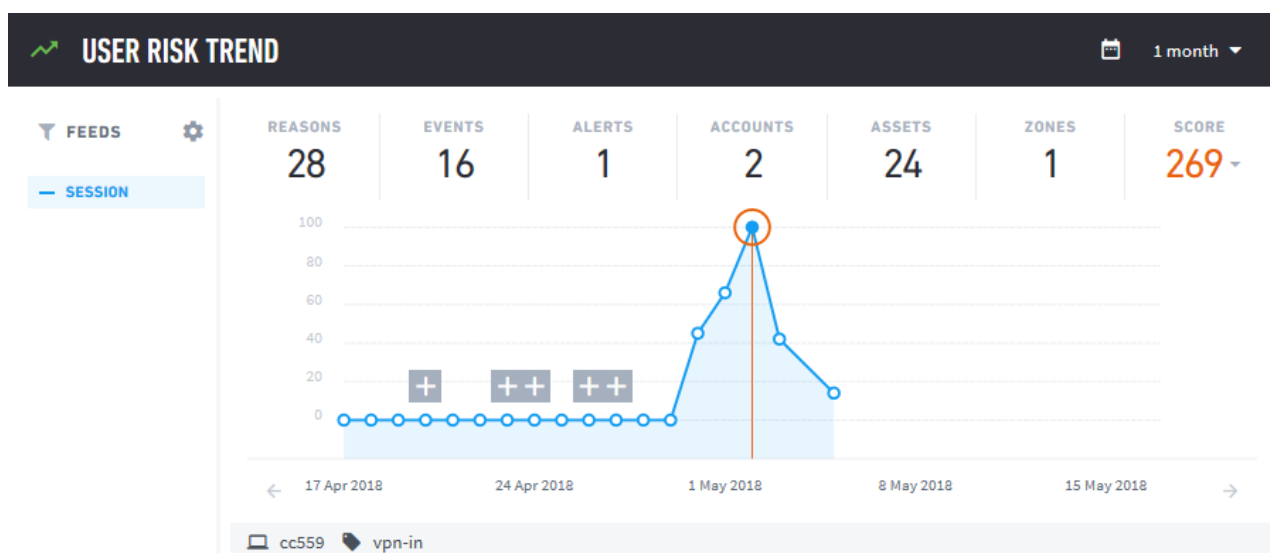
The following table lists the potential sources of information the SOC may use to identify events of interest.

#	Name	Description
1	SIEM monitoring	The SOC may detect issues through continuous monitoring of information security tools including, but not limited to, the Exabeam Data Lake platform If an incident is detected through this channel, please refer to SOC process flow for SIEM step 1 "Validate received alert and notification".
2	Other internal services	The SOC may become aware of issues reported through other functions within the organisation (e.g. issues identified by IT which have gone through the standard troubleshooting process and are believed to be security related). If an incident is detected through this channel, please refer to SOC process flow for SIEM step 1 "Validate received alert and notification".
3	External parties	There may be cases when the SOC is notified of issues by external parties – e.g. vendors, government agencies. If an incident is detected through this channel, please refer to SOC process flow for SIEM step 1 "Validate received alert and notification".
4	User	The SOC may become aware of issues reported by our Client's staff through various channels – e.g. Help Desk If an incident is detected through this channel, please refer to 2.2 SOC process flow for SIEM step 1 "Validate received alert and notification".

## User Entity and Behaviour Analytics

All non-explicit correlations across multiple systems are identified through the Exabeam UEBA software which overlays the SIEM platform. Rather than binary pattern matching the UEBA platform looks at trended activity over time. The Platform references normalised data within the SIEM platform and correlates activity against time, communication channel (e.g. port, application signature or interface), common usage pattern to define a baseline of "normal" activity.

All behaviours are presented in a graphical user interface that outlines deviation from baseline against timeline activity and presents a risk score for each abnormal activity.





While statistical information, even when correlated against a baseline, must be considered subjective – the platform allows data miners or security analysts to interrogate data against either threshold changes in user or entity scoring or alerts against a pre-defined risk score, irrespective of the duration taken to reach that value.

Unless predefined during scoping the alerting criteria is as follows:

- UEBA Risk Score >90 is considered a high priority incident for all high and low priority systems
- UEBA Risk Score change of >30 points for high profile users and a medium priority incident for all other devices.

When incidents are identified the UEBA platform arranges data in a format that can be easily interrogated by both SOC personnel and customer incident handlers to identify inappropriate behaviour in advance of a breach or to analyse the forensics of an event post breach.

Remote access to [src\\_o118\\_dev](#) 

TIME	USER	ACCOUNT
17:50:00	hosborne	 merickson
SOURCE IP	SOURCE HOST	SOURCE ZONE
10.111.122.22	sky-eefile-wp1	los angeles office
DEST. IP	DEST. HOST	DEST. ZONE
10.17.77.34	src_o118_dev	—
DOMAIN	REPORTING HOST	EVENT CODE
ktenergy	src_o118_dev	4624
PROCESS	LOGON TYPE	EVENT SUBTYPE
—	3 - Network	Windows

Abnormal access to [src\\_o118\\_dev](#) for [Howard Osborne](#) +10

DESCRIPTION

Abnormal for this user to access this asset

CONFIDENCE

99%

ANCHOR SCORE

10



X

ANOMALY FACTOR

1.0

=

+10

 Rule Definition  Data Insight

Abnormal access to [src\\_o118\\_dev](#) for group [Sales Representative](#) +2

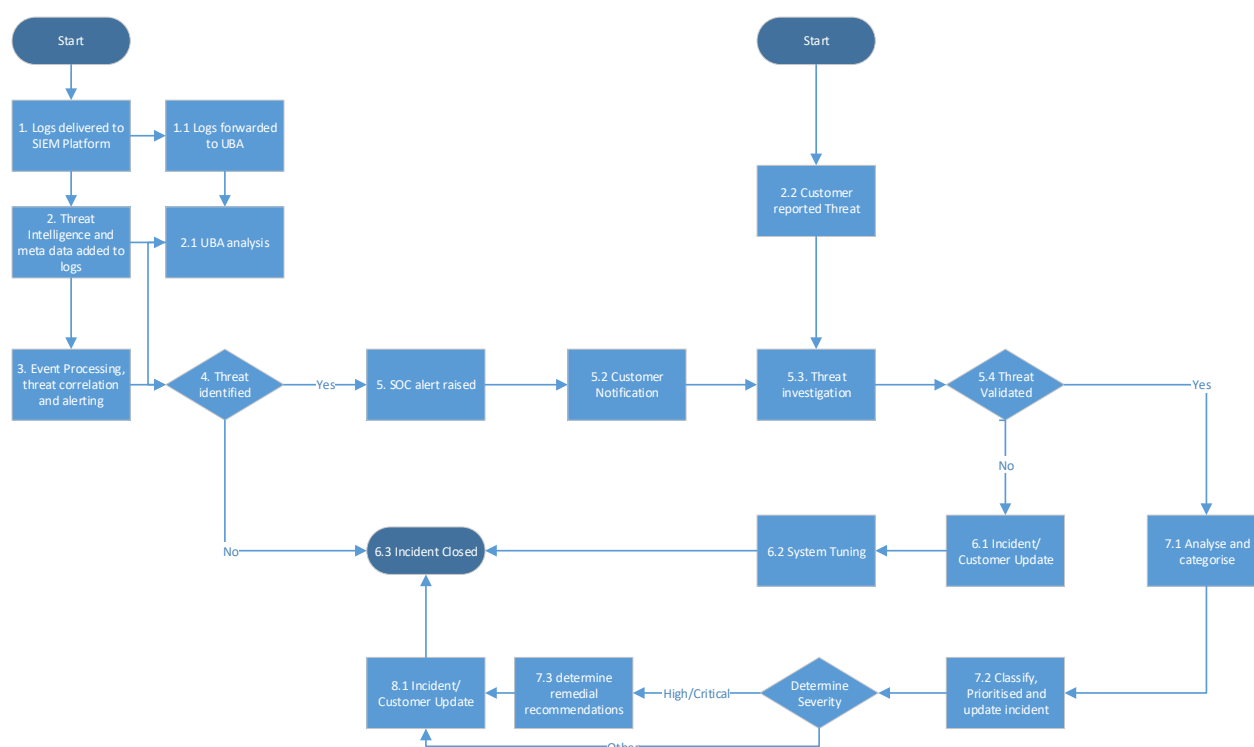
Supported log formats that can be integrated to provide analytics includes but is not limited to:

- Authentication Events – Domain controller logs
- VPN Events – VPN access gateway logins for remote workers, home offices and mobile devices
- Windows Server logs – local account logins, process logs, object access activities
- Unix system logs – user account logs including origination of connection and user changes

- Account creation logs – both domain and local login creation across Unix and Windows systems and directories
- Badge logs – correlation of physical security badges correlated with user account to identify anomalous behaviour and locations or tailgating
- Cloud application logs – Office365, Google apps, Salesforce.com, connecting users against their authentication domains and activities
- Web activity – proxy logging and firewall data transfer correlation for abnormal activity or data exfiltration attempts
- File and database access logs – tracking access to files to prevent ransomware, malware, data exfiltration and malicious insider threats
- Security events – events from malware, anti-virus, firewall and end-point protection incorporated into user timeline
- DLP intelligence – DLP results monitoring to reduce false positives and simplify detection or risky behaviour (this integration may require custom SIEM data normalisation activity on a professional services T&M basis)
- Email Activity – Analysing user email activity such as volume of data, volume of emails, abnormal numbers of CC or BCC recipients, or large volumes of emails delivered to specific accounts

## SOC process flow for SIEM and UEBA incident classification

The following process flow diagram describes the end to end process flow for the SOC from incident identification to closure.



#	Name	Description
---	------	-------------

1.	Logs Delivered to SIEM	<ul style="list-style-type: none"> <li>□ All log sources identified as “interesting” are delivered to the SIEM platform</li> <li>□ Logs are ingested using either Beats agent or Syslog with common event formatting</li> </ul>
2.	Threat intelligence	<ul style="list-style-type: none"> <li>□ All ingress logs are enriched using Threat Intelligence data from several open source and proprietary threat intelligence feeds</li> <li>□ Data such as malware/virus signature, command and control network source addresses, phishing hosts</li> <li>□ Enriched log information is scored High, Medium, Low or Informational/Unclassified based on Threat Intelligence feeds</li> </ul>
2.1	UEBA Analysis	<ul style="list-style-type: none"> <li>□ User and Entity Behaviour is analysed (consider contacting asset owner to gain a thorough understanding of asset’s native behaviour)</li> <li>□ Analyse trended behaviour of known activities to alert against deviation (abnormal login activity, abnormal traffic pattern, first file executions, new connection activity)</li> <li>□ UEBA scoring of 90 or above, will be classified as High priority</li> <li>□ UEBA threshold changes of risk score of greater than 30 points within 30 minutes will also be classified as a potential threat</li> </ul>
2.2	Customer reported threat	<ul style="list-style-type: none"> <li>□ Customers can report a potential threat to the SOC. This will kick off an investigation in the same way of a system generated threat alert.</li> </ul>
3.	Event Processing, threat correlation and alerting	<ul style="list-style-type: none"> <li>□ Corroborate an alert by cross-referencing using data sourced from the SIEM platform.</li> <li>□ Alerting of high threshold activity such as dictionary/brute force attacks, excessive traffic, extensive file changes</li> <li>□ Raise internal ticket logging event of interest.</li> </ul>
4.	Threat Identified	<p>The system will generate an alert based on the following conditions:</p> <ul style="list-style-type: none"> <li>□ Threats identified by correlating logs with known threats from the threat intelligence platform</li> <li>□ Threat identified by the UBA platform</li> <li>□ Critical alerts raised by customer security devices</li> <li>□ Alerts triggered by processing rules, correlation rules and configured alerts</li> </ul>
5.	SOC Alert Raised	<p>If the incident has been confirmed based on procedures performed in step 4, alerting will take place.</p> <ul style="list-style-type: none"> <li>□ High Priority incidents will be raised with a call and an email within an hour of log ingestion. Customer must either allocate resource to receiving phone calls or must accept a lower priority behaviour outside of working hours.</li> <li>□ Medium Priority Incidents will be raised via email only along with an open online service ticket</li> <li>□ Low and informational logs will be made visible via dashboard and custom reports tickets will only be raised against these logs for the purposes of system tuning requirements with suggested actions to reduce false positives or increase severity ratings.</li> </ul>
5.2	Customer Notification	<p>Where a security incident has been confirmed, the customer will be notified in line with the customer communications matrix.</p> <p>This communication will differ depending on time of day, severity and customer preference.</p>

5.3	Threat investigation	<p>Once a threat alert has been triggered or a customer reports a threat, this will initiate an investigation, which will include but not be limited to:</p> <ul style="list-style-type: none"> <li>- Validation of threat</li> <li>- Users impacted/involved</li> <li>- Devices impact involved</li> <li>- Threat and incident type</li> <li>- Severity</li> <li>- Inherent customer protection</li> <li>- Remedial actions and recommendations</li> </ul>
5.4	Threat validation	Depending on the validity of the alert or customer reported threat an incident will be closed or have an extended investigation.
6.1	Notify customer of non-threat	Where an investigation has determined that a reported threat is false positive, the customer will be notified.
6.2	System Tuning	Upon receiving confirmation through the ITSM toolset that threats are not considered a risk or are thought of as a false positive, system tuning will take place where possible to reduce future noise.
6.3	Incident Closure	Following confirmation of incident acknowledgement and subject to customer validation the ITSM ticket will be closed.
7.1/2	Analyse and reclassify	<p>Where an incident has been classified as either High or Medium severity and threats may still be identified as known behaviour or non-malicious.</p> <p>Following the creation of an investigation ticket for either High or Medium risk activities, SOC personnel will endeavour to enrich the ticket with supplemental satellite information to allow customer Incident Response personnel to confirm the impact of such threats.</p> <p>Input from the Business must be solicited whenever possible when attempting to understand the business impact of an incident. Immediate attention must be given to identifying the type of asset affected in the incident.</p> <p>IMPORTANT NOTE: Incident severity ratings derived based on the Incident Severity Assessment Guidelines should never be solely relied upon by the incident response team. When in doubt severity ratings must be discussed between SOC personnel and customer incident handlers to verify legitimacy and less tangible risks:</p> <ul style="list-style-type: none"> <li>□ Company brand and reputation</li> <li>□ Financial standing</li> <li>□ Compliance status</li> <li>□ Intellectual property</li> <li>□ Operations</li> </ul> <p>Professional judgment and due diligence must be exercised throughout the entire incident management lifecycle. The incident severity level must be re-assessed based on any new information that comes to light and may potentially shift current incident classification to a higher or lower tier.</p>
7.3	Identify remedial recommendations	For Critical and high severity incidents the SOC will provide a recommendation for remedial action. This will be based on the prior investigation and knowledge of threats along with the security technologies available to the customer.

8	Critical or high Severity incident?	<p>If the incident has been categorised based on procedures performed in step 7.1/2 please proceed to step 8.1 “Route to Customer incident response team”.</p> <p>If received alert or notification meets the criteria for a Major or Critical Alert the client incident response team will dictate the closure of the ticket. Should further supplemental information be required beyond the data supplied up to this point, or interrogation of affected systems, then professional services may be required on a time and materials basis.</p>
8.1	Customer notification of threat	<p>If the incident has been classified as Critical or Major Severity based on procedures performed in step 7.2 a phone call with customer incident response team will be carried out. At this point the customer may choose to begin a major incident process.</p> <p>Cybanetix are required to supply the following information:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Incident category</li> <li><input type="checkbox"/> Indicators of compromise</li> <li><input type="checkbox"/> Impacted systems</li> </ul> <p>Following this telemetry, the client Incident Response Team will be required to enrich the ticket with the following details:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Actions taken</li> <li><input type="checkbox"/> Impacted systems and data</li> <li><input type="checkbox"/> Confirmation of remediation</li> </ul>

## Categories of Incidents

Information security incidents vary in objective, pattern, techniques, impact, etc. In order to effectively detect information security incidents, the SOC will monitor for activity, where the customer solutions allow, that falls into the following categories:

- Reconnaissance – attacker’s activities focused on gathering insight about the target (e.g. internal PING sweeps, port scans).
- Active Malicious Code – Malware of any type present on an information asset connected to our Client’s network (e.g. viruses, worms, Trojans, botnets).
- Vulnerability exploitation – Active exploitations happening in infrastructure
- Denial of service – An interruption or significant degradation in the performance of an information asset or its availability.
- Unauthorised access attempt – An attempted compromise of an information asset by an attacker performed through interactive hacking techniques.
- Unauthorised access success – A successful compromise of an information asset by an attacker accomplished through interactive hacking techniques.
- Network Defence Testing – Controlled testing activities of a system or networks defences.
- Data loss – An indicator that a user or a malware is exfiltrating or destroying data
- User threats – An indicator that a user is exhibiting abnormal behaviour
- Privilege escalation – escalation of privilege to non-approved users
- Scans/Probes – Any activity that seeks to access or identify any open ports, protocols, services or any combination for exploit.

## Incident Severity Assessment Guidelines

Incident severity level and prioritisation is an important decision point in the initial steps of the incident

response process. Due to resource limitations, incident response efforts need to be prioritised based on the level of impact the incident poses to the organisation. Some events are detected and categorised by the SIEM platform directly, other events of interest are only categorised after an initial triage.

Guidelines to assist with the severity assessment process have been provided below and consider the following factors:

- Incident category
- Value of asset impacted by the incident (system, data, account).

	Scans/Probes	Privilege escalation	Data loss	Reconnaissance	Active Malicious Code	Denial of Service	Unauthorised Access – Attempt	Unauthorised Access – Success	Network Defence Testing	UEBA Threshold >30 Points <30 minutes	UEBA Score >90 risk points
High value Assets	Low	High	High	High	High	High	High	High	Medium	High	Medium
All other assets	Low	Medium	Medium	Medium	Medium	Medium	Low	High	Low	Medium	Medium

## Incident Severity Assessment Guidelines - Asset Classification

To assess the criticality of an asset (generically describing systems, data and accounts), consider the criteria listed in each cell. Note that this assessment is not always linear in nature. For example, initial investigation can point to the compromise of a single non-privileged user account which would rank as “Low” importance. Further investigation, however, could reveal that the individual user had access to sensitive financial data, which would rank as “High”. Highest level of importance in any consideration will override all other factors; so in this case, the overall asset importance rating will be “High”. The asset importance levels listed above are described in the following table.

IMPORTANT NOTE: The table below is to be used as general guidance only. Professional judgment must always be applied.

Asset Importance	Systems	Accounts
High	<ul style="list-style-type: none"> <li>• Core Firewalls</li> <li>• Switches and Routers</li> <li>• Security Technologies</li> <li>• Servers</li> </ul>	<ul style="list-style-type: none"> <li>□ Administration accounts</li> </ul>
All other Assets	<ul style="list-style-type: none"> <li>• Any other account</li> </ul>	<ul style="list-style-type: none"> <li>□ Any other account</li> </ul>

## Incident Severity Rating

Incident severity level	Priority	Initial Customer Contact	Status tracking and communication	Support team response time expectation if part of managed service
Critical & High	<ul style="list-style-type: none"> <li>• Service provider ticket type – P1</li> <li>• Information Security Incident Response support team mobilised as required</li> <li>• 24/7 response</li> </ul>	1 hour following detection / reporting via customers preferred contact method	<ul style="list-style-type: none"> <li>• Response actions documented in incident ticket</li> <li>• Out-of-band communications, if necessary</li> <li>• Where managed under another service provider server, hourly Milestone updates to stakeholders and Information Security Incident Response team members</li> </ul>	Immediate upon notification by SOC
Medium	<ul style="list-style-type: none"> <li>• Service provider ticket type – P2</li> <li>• Information Security Incident Response support team mobilised as required</li> <li>• Standard working day response</li> </ul>	1 Hour following detection / reporting via customers preferred contact method	<ul style="list-style-type: none"> <li>• Response actions documented in incident ticket</li> <li>• Out-of-band communications, if necessary</li> <li>• Where managed under another service provider server, 2 hourly Milestone updates to stakeholders and Information Security Incident Response team members</li> </ul>	Immediate upon notification by SOC (priority always given to critical incidents)
Minor	<ul style="list-style-type: none"> <li>• Service provider ticket type – P3</li> <li>• Support functions engaged as required</li> <li>• Standard working day response</li> </ul>	Notification as required during standard hours.	<ul style="list-style-type: none"> <li>• Response actions documented in incident ticket</li> </ul>	None
Events of Interest	<ul style="list-style-type: none"> <li>• Service provider ticket type – P4</li> </ul>	Email only	<ul style="list-style-type: none"> <li>• Tracked in Exabeam Data Lake</li> <li>• Response actions documented in incident ticket</li> </ul>	Dependent on eventual classification

## Alert Tuning

The SOC will periodically review existing SIEM rules and security alerts to continue effective detection of activity that introduces risk to our client's environment.

## False Positive Alerts

All events that are categorised as false positives should be reviewed for correctness. The analyst that reviews the rule should evaluate not only the logic of the rule but any thresholds that are associated with the rule. Changes to rule logic or thresholds should be proposed to the SOC Manager, who will retain approval authority for any modifications to rule logic.

## SOC Onboarding process

The onboarding process will gather all the information required for service management from the customer and will include, but not be limited to, the following:

- Server list with services provided.
- Workstation lists.
- Network diagrams and location of equipment.
- Customer contacts as well as escalation matrix and out of hours contact requirements.
- Patching schedules.
- Change control and other process details.
- Agreements of the logs to be collected.
- Classification of devices by type and criticality.
- Communication matrix for notifications and escalations
- The customer will be supplied settings and agents for installation on all endpoints as well as details on how each end point should be configured.

## Initial 3-month service period

In order to reduce the impact on the SOC team and the customer response team due to incorrectly classifying false alerts and tuning issues due to standard customer working practices, the following incident severity table will be used for an initial period of up to three months.

	Scans/Probes	Privilege escalation	Data loss	Reconnaissance	Active Malicious Code	Denial of Service	Unauthorised Access – Attempt	Unauthorised Access – Success	Network Defence Testing UEBA	Threshold >30 Points <30 points	UEBA Score >90 risk points
High value Assets	Low	High	High	High	High	High	High	High	Medium	High	Medium
Other Assets	Low	Medium	Medium	Medium	Medium	Medium	Low	High	Low	Medium	Medium

## Service Reporting

Cybanetix will produce a quarterly service report, which will be reviewed with the Customer in a subsequent service review. The service report will as a minimum include:

- Number of incidents in the service period
  - Type of incidents
  - Time of incidents
  - Severity of Incidents
  - Average Response times
  - False Positives
  - SLA against KPIs
- Use case statistics
  - Volume
  - Time of day
- Platform Performance
  - Service Outages
  - Data volumes
  - Platform performance
- Change management
  - Changes for the period (please note that changes are not tracked in the first 3-month period)

As part of reviewing the report, the technical correctness and the SIEM alerting rules pertaining to monitored use-cases will be assessed. Any anomalies or identified gaps will be actioned following the review.

## Exclusions and Limitations

- The Service Provider reserves the right to review the volume of service requests being requested on a weekly basis and charge for excessive usage.
- In the event of a breach to a customer service or site, then this service will support, through information gathering from captured event logs, the remediation of the event, but this service does not include implementing remediation activities.
- The Service Provider reserves the right to review the number of investigations requested by a customer and, if found to be excessive, will charge accordingly.
- Log handling and subsequent investigations by the service supplier are not carried out in a manner to maintain the chain of evidence.
- The agents are supported by best endeavours on any end of line systems and operating systems.
- The Service Provider is not responsible for log enrichment failing due to the customers patching processes and subsequent changes in vendor log messages. The Service Provider will review log collection on a monthly basis to confirm that the logs are being ingested as expected and will resolve issues that may have arisen by patching/firmware etc. to that log inspection.

## Customer Responsibilities

- The customer is to provide a complete list of the equipment and services that are required to be monitored, with a network map and a list of services per endpoint.
- The customer is to manage changes to the list via its own change control procedures and to inform the service provider.
- The customer is to provide relevant contact details, along with escalation paths to facilitate event alerting.
- The customer is to provide the tools capable of capturing the events required. For example, in the event of a firewall port scan, either the firewall must be capable of detecting and alerting against the event, or the firewall must log and report all deny events.
- All logs to be collected and analysed are to be in English.
- The customer is responsible for providing VPN end points, where required, to maintain the security of the logs gathered.
- The customer will ensure that there is a common time source that is used by all devices covered by the service to ensure time synchronisation across all logged events.
- The customer is to make modifications to services identified in order to optimise the data being captured. For example, the Service Provider may notice excessive broadcast on a LAN segment and will attempt to identify the source and recommend to the customer the changes that may be required to reduce such traffic.
- Unless the endpoint is covered by a Service Provider's managed service contract, the customer is responsible for resolving issues with the collection of logs, with the service providers assistance, where identified by the service provider as resulting from an issue with the end point device.
- Unless the endpoint is covered by a Service Provider's managed service then the customer is responsible for ensuring all end points required are sending the required log data. The Service Provider will make available to the customer upon request, a report of total events collected from each endpoint in order that the customer can confirm that log collection is occurring from each end point required.
- The customer is to make the Service Provider aware in advance and in writing (email is acceptable) of any penetration tests and of any vulnerability scanning that may be undertaken. Failure to do so may subject the customer to charges for any time taken to investigate incidents caused by such activity.
- The customer is responsible for implementing basic preventative security measures such as regular patching of all endpoints, managing anti-malware products, removal of unnecessary services from end

points, using host-based firewalls, using IDS or IPS systems etc.

## Service Provider Responsibilities

- To provide and manage the SOC toolset, including, processes, procedures and skills to ensure the effective and efficient handling of incidents.
- Hosting, Storage and SIEM platform availability is subject to Exabeam SaaS Service Levels.
- Cybanetix SOC licensing will be maintained and supported throughout the contract.
- Security of Customer data within the SIEM toolset is subject to the security controls applicable to Exabeam SaaS.
- The Service Providers agents will use encryption techniques to ensure the integrity of data captured by that agent.
- Access to the log store is provided to the customer through a web interface.
- The Service Provider will manage all security events through its incident management process.
- Through Threat Intelligence gathering and analysis, the service provider will frequently review and revalidate the SIEM rules.
- The Service Provider will maintain a list of log sources it can ingest and process.
- The default dashboards provided by the Service Provider may be modified by the Service Provider to reflect changes in the service and/or changes to the logs gathered on behalf of the customer. The customer may request changes to the default dashboards, however these may be rejected by the Service Provider. Changes may be subject to an administration charge.
- The service provider will confirm at the time of on boarding that all customer logs are ingested and enriched. The service provider will review log collection on a monthly basis to confirm that the logs are being ingested as agreed and will resolve issues that may have arisen by patching/firmware etc. changes that arise from that log inspection.
- Where the Service Provider also provides other managed services, then the Service Provider will maintain a Computer Incident Response Team to assist the customer with any Cyber Security related incident

## SCHEDULE 2 Charges and Term

Service: [ ]

User Number: [ ]

Entity Number: [ ]

Log Storage: [ ] TB ("Storage Allowance")

The Term of this Agreement is [36] months commencing on the Effective Date.

### Charges

Item	Description	Qty	Unit Price	Total Price
[ ]	[ ]	[ ]	£[ ]	£[ ]
[ ]	[ ]	[ ]	£[ ]	£[ ]
[ ]	[ ]	[ ]	£[ ]	£[ ]
<b>Total (excluding VAT)</b>				<b>£[ ]</b>
<b>VAT</b>				<b>£[ ]</b>
<b>Total (including VAT)</b>				<b>£[ ]</b>

- Cybanetix SOC service is paid annually in advance
- Payment terms strictly 30 days on invoice.

### Additional Charges

Item	Description	Qty	Unit Price
[ ]	[ ]	[ ]	£[ ]
[ ]	[ ]	[ ]	£[ ]
[ ]	[ ]	[ ]	£[ ]

If Customer exceeds the Storage Allowance stated above by more than 10%, then additional log storage charges will apply in respect of such excess storage, charged as follows:

Charges per 1 TB of excess storage £1500 per annum

The charges will be invoiced after 30 days after the first notification to the customer of the excess storage use. The over usage is charged in whole 1TB increments which is calculated as the lowest number whole 1 TB increments which exceeds the current usage at the point of invoice.

Customer may also reduce its excess storage charges by purchasing additional storage upfront in 3TB and 10TB increments. The applicable charges are as follows:

Charges per 3 TB of additional storage £3500 per annum

Charges per 10TB or additional storage £6000 per annum

Cybanetix' records in respect of log storage used by the Customer will be deemed final and conclusive.