Managed Cyber Security Service

Threat Intelligence

Service Description

Secure, Integrated Cloud Services

Table of Contents

1. Service Overview 3
   1.1. Brand and Identity Alert 3
   1.2. Managed Brand and Identity 4
   1.3. Managed Brand and Identity and Vulnerability 4
2. Service Features 5
3. Intelligence Reporting 6
   3.1. Monthly Alert Reporting 7
   3.2. Quarterly Threat Landscape Report and Briefing 7
4. Service Implementation 8
   4.1. Phase 1 – initiation 8
   4.2. Phase 2 - Planning and configuration 8
   4.3. Phase 3 – Staging and live 8
   4.4. Ready for Service 9
5. Billing 9
6. Exit Assistance 9
7. Client Obligations 9
8. Service Dependencies 10

1. Service Overview

Our Threat Intelligence Service provides you tactical intelligence as well as operational and strategic intelligence reports by monitoring known criminal forums and the dark web.

We offer different modules for our Threat Intelligence Service:

(a) Brand and Identity Alerts;

(b) Managed Brand and Identity;

(c) Manged Brand, Identity and Vulnerability

Your Service module and the associated Fees will be detailed in your Order Form and/or Statement Of Work.

1.1. Brand and Identity Alert

This module focuses on your organisation's reputation, data and people, and is designed to give you visibility on attempts to steal your data, falsely represent your business and undermine your employees, managers and directors. As part of this module, we will provide actionable, analytical insights to assist you with the proactive defence against new and emerging threats. We will provide you with alerts where we identify threats and include details of such alerts in your weekly and/or monthly reports which you can use for your own strategic decisions around mitigating your risks. As a standard, the key elements of this module include the below:

(a) Monitoring for domain abuse detection – we will monitor websites and social media accounts to attempt the identification of fake websites and accounts used to impersonate your organisation or employees which could be used for fraud and phishing attacks;

(b) VIP monitoring – we will monitor your VIP accounts to mitigate the risk of your key business leaders being targeted or misrepresented;

(c) Intellectual property monitoring - we will monitor your intellectual property as agreed with you to minimise the risk of your information and data being stolen, leaked or sold on to your competitors;

(d) We will monitor your organization for malicious content and false information which may damage your brand and reputation;

(e) We will monitor the threat landscape for counterfeit products and software offered in digital marketplaces and app stores which may damage your brand and reputation;

(f) We will monitor your environment for broader data leaks and leaked credentials from employees and executives which may compromise the security of your organisation.

1.2. Managed Brand and Identity

This module provides all the elements covered under Brand and Identity Alerts module, plus additional managed support for your Service. As a standard, we will provide the Managed service support below:

(a) Our analysts will review the information gathered by the platform and create intelligence reports for you;

(b) The availability of Threat Intelligence analysts to you for any questions or additional information relating to the intelligence reports.

1.3. Managed Brand and Identity and Vulnerability

This module is designed to give you an understanding of your technical security posture and visibility on emerging threats, based on the ever-changing tools, techniques and tactics used by threat actors. This module includes all the elements covered under Managed Brand and Identity module plus the following additional features:

(a) We will provide you visibility into the likelihood of a known vulnerability being exploited;

(b) We will investigate multiple sources to gather visibility on risk milestones such as Proof of Concept (“PoC”), dark web references, exploited in-the-wild;

(c) We will provide you context around the common vulnerability scoring system (“CVSS”) on risks identified that we think may be relevant to your organisation;

(d) We will help you understand your exposure to threat actors based on their capability to exploit vulnerabilities;

(e) We will provide visibility into the likelihood of exploitation, by using a risk milestone structure and reviewing attributes such as PoC, dark web references, exploited in the wild.

2. Service Features

Feature	Brand and Identity Alert	Managed Brand and Identity	Managed Brand, Identity and Vulnerability
Support for compliance with industry regulations	●	●	●
Threat landscape intelligence report	●	●	●
Brand and identity focussed intelligence requirements	●	●	●
Dark web monitoring	●	●	●
Actionable technical intelligence	-	●	●
Tailored reporting of threat landscape and attacker behaviour	-	●	●
Analysis based on critical assets	-	●	●
Information on the evolving threat landscape	-	●	●
Quarterly strategic intelligence	-	●	●
Custom intelligence requirements	-	●	●
Monthly alert reporting	-	●	●
Quarterly threat landscape report and briefing	-	●	●
Vulnerability prioritisation	-	-	●
Custom guidance	-	-	●

Service Feature	Description
Support for compliance with industry regulations.	Our Service is aligned with ISO 27001:2022 (Annex A 5.7) and PCI DSS v4.
Threat landscape intelligence report	We will provide you daily updates on significant events identified in the wider threat landscape via the Client portal.
Brand and identity focussed intelligence foundations	Our service includes a foundational set of intelligence capabilities tailored to safeguard your organization's brand integrity and identity security. This baseline coverage addresses common security intelligence use cases, which allows you to assess the security of your brand and identity assets against emerging threats.
Dark web monitoring	We will monitor the dark web to understand if your credentials, secret key or code may have been leaked, if you may have any

	malicious traffic in your IP ranges, and if there may be a risk of impersonation of your VIPs or other organisational defamation.
Actionable technical intelligence	We will provide you with detections, detection rules, and security control suggestions.
Tailored reporting of threat landscape and attacker behaviour	We will provide you regular reporting, both monthly and quarterly, to give you insight on the reasons why a certain threat actor may be targeting your organisation or organisations like yours.
Analysis based on critical assets	When performing analysis, we can change the priority of the alerts generated by the Service to provide you with alerts relevant to your business.
Information on the evolving threat landscape	We will perform monthly review of top actors and their tactics related to your organisation, and we will provide you guidance on how to mitigate the relevant threat vectors.
Quarterly strategic intelligence	We will provide you quarterly strategic reports. The report will include our analysis of the trends that we have identified in the previous quarter based on certain validated attacks. This report is aimed at giving you insight in the longer-term cyber threat landscape, which you can use as an internal guidance for the security posture of your organisation.
Vulnerability prioritisation	With vulnerability intelligence we will provide alerts that allow you to understand the threats to your technology stack in line with the vulnerability exploitation lifecycle, so that relevant and applicable patches can be prioritised with the resources you have available.
Monthly alert reporting	See the Intelligence Reporting section for more details.
Quarterly threat landscape report and briefing	See the Intelligence Reporting section for more details.

The table above describes the features included in the scope of our Service as a standard. If you have any bespoke requirement or would like us to implement custom intelligence, we will review your request and advise whether our Service can be customised in accordance with your requirements. Please follow the change enablement process set out in the Operations Manual if you require an operational change, or the process set out in your MSA if you require a change to the scope of your Service.

3. Intelligence Reporting

We will provide intelligence reporting as part of our Threat Intelligence Managed Brand and Identity or Managed Brand, Identity and Vulnerability modules. Please note that Intelligence reporting is not included in our Threat Intelligence *Brand and Identity Alert* module.

3.1. Monthly Alert Reporting

We will electronically provide you a monthly report including analysis and review on the previous month's threats. This report will include information from alerting, research, and vendor reporting. Where new data and information is available to provide further contextualisation, the report will also include a retrospective review of the alerts and the application of such analysis.

The monthly alert report will include a threat map of actors related to your organisational vectors and based on intent and opportunity of attack. The report will also include a review of the most active actors over the previous month, which can help you understanding the background on infrastructure, high fidelity indicators, hunting packages, and tactics, techniques and procedures that can be used.

Where you have procured the *Managed Brand and Identity and Vulnerability* module, your monthly alert report will include an additional threat exposure summary, brand exposure summary and vulnerability exposure summary:

- The threat exposure summary will provide a contextual review of the most active actors over the previous month, including background, high fidelity indicators, and any hunting packages that can be used.
- The brand exposure summary is a review of alerting and analysis on the trends related to brand and credential which may increase the risk of exposure of your organisation.
- The vulnerability exposure summary is a review of any as Proof of Concept ("PoC"), recently exploited, or malware-linked vulnerabilities related to your organisation's technology stack.

3.2. Quarterly Threat Landscape Report and Briefing

We will provide you a strategic report which includes an overview of the cyber threat landscape in the context of your organisation to assist you with your security posture over the next quarter.

The report and briefing will include analysis on threats over the previous quarter specific to your organisation. The report will be based on the most common techniques used in the previous quarter and will include, where available, advice on how you could potentially mitigate the risk based on the threats that we have observed.

The report will cover the whole cyber threat landscape and include information on industry, technology, people, and geopolitical vectors.

4. Service Implementation

After order acceptance, we will implement the Service in three phases:

(a) Phase 1 – initiation;

(b) Phase 2 - planning and configuration;

(c) Phase 3 – staging and go live.

4.1. Phase 1 – initiation

The key activities performed during this phase are the following:

(a) We will provide you an on-boarding form which you must complete with all information reasonably required by us to complete the onboarding;

(b) We will review the documentation that you have provided and confirm whether you have met all requirements for commencement of the implementation activities;

(c) We will provide you details of your Account Manager and where relevant, the Service Delivery Manager;

(d) We will schedule and conduct a kick-off meeting with you to discuss the transition process, project tasks, roles, and responsibilities, and to introduce the key stakeholders. You must ensure that all your relevant stakeholders attend this kick-off meeting;

(e) We will provide a copy of the SoW, which will include details of your monitored assets.

4.2. Phase 2 - Planning and configuration

The key activities performed during this phase are the following:

(a) We will jointly hold a kick off meeting, with a walk through of the onboarding document;

(b) Our threat analysts will configure the Threat Intelligence platform based on the onboarding document and the information that you have provided;

(c) We will configure the Service based on your requirements as agreed with you.

4.3. Phase 3 – Staging and live

The key activities performed during this phase are the following:

(a) We will confirm whether all brand, technology, and people within your organisation that you require us to monitor are in the Threat Intelligence platform;

(b) We will perform tuning of alerts where needed;

After completion of the activities listed above, we will confirm that the Service is live and operating correctly. Our threat analyst will review the onboarding documentation with you on a quarterly basis and update it as necessary for the correct performance of the Service. Please note that this quarterly review will be performed remotely.

4.4. Ready for Service

The Ready for Service Date is the date when we, acting reasonably and properly, notify you that the implementation steps are complete. This date could be specified to occur at a later date, if mutually agreed to be so. If you consider that the Service is not ready for service on the date notified, you must notify us within two (2) weeks of our notification, after which the Ready for Service date will be deemed to have occurred regardless of issues or defects of which you could later become aware and notify us about (which will then be dealt with as faults or service issues but will not change the Ready for Service Date).

5. Billing

The Service will be billed as a Recurring Fee on or shortly after the Ready for Service Date as described in the Billing Guide.

Details of the applicable Fees and billing frequency will be included in your Order Form.

6. Exit Assistance

As a standard, we will perform the following activities shortly before or upon termination of your Service:

(c) Cease all connectivity to our systems;

(d) Remove your users and watch list data from our systems;

(e) Cease the service you have procured from us and the access to the solution.

Please note that it is your responsibility to provide a valid termination notice in accordance with the terms of your MSA. We reserve the right to charge additional Fees for the performance of the activities listed above if you fail to provide such notice.

Please note that this Service is not transferable in whole or in part to an alternative supplier.

7. Client Obligations

(a) You will provide us reasonable assistance in the performance of the Service, including, but not limited to, providing all technical and monitoring information that we require for performing the Service;

(b) You will provide a service contact email address which we can use to send notifications and communications to you. It is your responsibility to ensure that this email address is active and that emails sent to this address are received by the appropriate recipients;

(c) You will work closely with our threat intelligence team during the tuning of alerts and implement recommendations provided;

(d) You will inform us of any internal changes, including changes in identities, software versions and locations or changes to your monitored assets or components;

(e) You will interact with us and provide updates and information to tickets via the IMS system only;

(f) You are responsible for following the correct change process as described in the Operations Manual;

(g) You will notify us of any change that may affect the operation of the Service. We will not be responsible for any detrimental impact on your Service and/or adverse consequences of changes implemented by you where you have failed to notify us of such changes or, where relevant, to implement the changes in accordance with our guidance;

(h) You will identify the correct systems/assets and components to be monitored;

(i) You will provide us with accurate and up-to-date information, including name, email, landline, and mobile numbers (if applicable) for all your authorised points of contact and your head office or contact address.

8. Service Dependencies

We will provide monthly alert reporting and quarterly threat landscape reports and briefings as described in Sections 3.1. and 3.2. only if you have procured our Managed Brand and Identity module, or our Managed Brand, Identity and Vulnerability module.

Six Degrees

For more information

Tel – 0207 858 4935

Email – info@6dg.co.uk

www.6dg.co.uk

Secure, Integrated Cloud Services