Integrity360

your **security** in mind

Managed Digital Risk Protection Service

Service Description

Version: V0.1

integrity360.com

Table of Contents

1. Service Overview

1.1. Introduction

Many organisations have good exposure management and threat monitoring, detection and response across their own environment. However, this is only half the picture, as threats and exposures are not only internal, and it is equally vital to understand the external security posture of your organisation and how it may be viewed and exploited by an external actor.

Integrity360's Managed Digital Risk Protection Service (DRPS) provides highly tailored and relevant threat intelligence information along with 24/7 continuous monitoring of digital risks and other external threats facing today's organisations. Powered by the Integrity360 SOC team and a marketing leading Digital Risk Protection Platform, an organisation's external attack surface, brand use and misuse, and adversary intelligence is continuously monitored across the open, deep and dark web.

When an external threat is observed, the exposure, the context about who is planning or attempting to exploit the customer, what their motivation and capabilities are, and indicators of compromise to look for are presented by Integrity360, along with recommended response actions to take.

In addition to continuous monitoring, the service includes 24x7 access to a rich set of up-to-date threat intelligence information, and the ability to raise threat intelligence "Incidents", or specific "Service Requests" to receive guidance and advice about threats or threat actors of particular concern or that are in the news.

Integrity360 will also layer proactivity across the service to optimise digital risk detection. In addition to triaging, investigating & containing alerts generated by Integrity360's threat intelligence sources, customers will receive "Major Cyber Threat Advisory" assistance when major threats relevant to the client's environment are identified.

1.2. Service Objectives

The objectives of Integrity360's Managed Digital Risk Protection Service are to provide continuous monitoring and ability to rapidly respond to external exposures and threats to the organisation as follows:

1. Ongoing and continuous monitoring of the External Attack Surface of the customer to identify any exposures that could be exploited by a threat actor, whether vulnerabilities, misconfigurations, rogue assets, weak or expiring certificates, and leaked credentials to name but a few.

2. Monitoring for any misuse of the organisation's brand on the open, deep or dark web, to include impersonating / phishing domains, copycat websites, social media misuse and impersonation of brand or VIPs, fake mobile applications, and so forth, and ability to respond and take down such misuse.

3. Ongoing monitoring and review of adversary-centric threat intelligence, to understand and be able to react to threats manifesting against an organisation's name, industry, geography, supply chain, or infrastructure profile, including ability to investigate indicators of compromise.

1.3. Service Overview

The Integrity360 service is designed to take the load of the customer and

- Ensure the platform is configured and operating optimally
- Reduce noise and provide high-fidelity alerting - Monitor the alerting and conduct triage and investigation to only report threats or exposures that represent a material risk
- Manage the takedown process to ensure malicious websites, accounts, applications and other infrastructure are removed as soon as possible
- Provide support and advice on any digital risk exposure or threat concerns of the customer and provide investigative support
- Curate threat intelligence so that tailored insight is regularly provided to inform strategic planning and investment prioritisation

2. Solution Architecture - Digital Risk Protection Platform

Depending on the license level chosen, the following modules will be managed under DRPS:

Features	External Attack Surface Management (EASM)	Brand Protection (BP)	Adversary Centric Intelligence (ACI)
Asset Discovery	✓		
Security Issues	✓		
Asset Reports	✓		
Weekly Asset Identification	✓		
Leaked Credentials	✓		
Merger Acquisition Risk Asses	✓		
Subsidiary Risk Management	✓		
Domain Threats - Typosquatting, Phishing, Brand Impersonation		✓	
Data Leakage - Source Code Repo, Cloud Storage,		✓	
Rogue Mobile Application		✓	
Executive Monitoring		✓	
Social Media Monitoring – Fraudulent Accounts		✓	
Intel Gathering – Darknet, OSIT, TI, TA			✓
Darknet Marketplace Monitoring- Stealer Infections & Credit Card Fraud			✓
Supply Chain - Vulnerability & Ransomware Intel, Vendor Risk Assessment			✓
IoC Reputation Lookup (IP/Domain/Hash/CVE)			✓

The underlying platform for DRPP offers an extensive library of up-to-date threat intelligence information. Key features include:

- Threat Profiles (Actor, Campaigns, Criminal Locations)

- MITRE ATT&CK Profiles: Detailed description of attacker MITRE tactics and techniques and ability to drill into associated industry targets and related intel updates
- Threat Intel queries and briefings
- Threat intel portal used in a variety of different ways:
    - **IOC Investigation:** Gain additional context on Indicators of Compromise (IOCs), which can be useful to SOC teams during investigations. It can also be used to uncover further IOCs linked to malicious actions helping triage, and in configuration updates.
    - **CVE Tracking:** When clients are faced with many Common Vulnerabilities and Exposures (CVEs) which require patching, they use information within the platform to help prioritise – such as gaining an understanding of when exploits have been made public.
    - **Enrich Investigations:** Used within tactical investigations of technical indicators used in cyber-attacks such as business email compromise, phishing attempts, or denial of service attacks.
    - **Identify Supplier Risks:** Used by security teams to monitor potential third-party risks, such as vulnerabilities found in outsourced IT suppliers, or breaches of companies holding their sensitive data.
    - **Track Industry News**: Use to understand quickly whenever there's a new development related to their industry.

Whilst full customer access to the portal is available, Integrity360 will distil and tailor the most relevant threat intelligence information and provide curated intelligence.

Within package, the following monitoring, alerting and notification functionality is included:

2.1. External Attack Surface Management

External Attack Surface Management (EASM) provides an external outside-in view of the organisation and its subsidiaries, to identify exposed known and unknown enterprise assets and associated vulnerabilities to help prioritize the remediation of most critical issues. EASM helps to identify servers, credentials, public cloud service misconfigurations and third-party affiliate software code vulnerabilities potentially exploited by malicious actors.

2.1.1. Attack Surface Monitoring

Attack surface is a set of external (or Internet-facing) digital assets that contain, link or process corporate data that can be potentially exploited by an attacker, to compromise networks or systems. In today's environment it is imperative to have visibility of attack surface to be able to effectively plan defence strategy for all digital assets. Attack surface monitoring provides a realistic picture of exposed digital assets, that include:

- Domains/Subdomains
- IP Addresses / Subnets
- Open Ports
- SSL Certificate Scans
- Services
- Possible Misconfigurations
- Reputation Checks for the network

2.2. Brand Protection

Our service uses proprietary algorithms to detect web-based phishing attacks, typo-squatting, rogue apps, credential leaks and brand impersonation in social media common techniques used by Cyber Threat Actors. By detecting activity early and taking action such as web site or application takedown, Brand Protection helps organisations to protect their brand value, trust, integrity, and reputation.

Brand monitoring & protection services is specifically targeted towards monitoring unauthorized use / abuse / malicious intent against the organisations brand. Threats that are monitored and neutralized as part of Brand Protection services which are listed in subsections below.

2.2.1. Typo Squatting Monitoring

The service platform continuously monitors for “Typo squatting” attacks to detect when a threat actor registers domain names, similar to the monitored organisation, and uses them for malicious activity. These are detected by monitoring domain registration and live web servers to identify domains which are typos (transpositions, character swaps) The Team monitors similar looking domains for stipulated duration to identify if any content damaging the organisation brand is hosted on those domains. When such domain is detected, the organisation’s administrator can initiate the takedown.

2.2.2. Phishing Monitoring & Takedown

The platform and service provide a rich repository of threat Intelligence collections provides unique advantage in detecting and acting on the phishing content. A technical research team with special focus on Phishing uses proprietary algorithms for brand and links detection. Backed upon intelligence from Collections & Research inputs, our Takedown specialists quickly take corrective actions and work with multiple agencies such as Hosting Providers, Registrars and Search Engines to ensure the links are removed in a timely manner

2.2.3. Digital Watermarking

The platform uses digital watermark on official login and sensitive pages to track cloning and rehosting of the web pages as phishing sites on different IP addresses. A small script will be provided to the organisation to be embedded into their website that will help the research team to track the cloning/rehosting of the site. This process will also help customer to identify if any of their users have been in fact phished on the cloned page and take corresponding remedial actions.

2.2.4. Rogue App monitoring

With the critical importance of mobile technologies to organisations and their customers, mobile applications and potential for brand damage if abused, it is important to monitor for rogue applications abusing the organisational reputation. Rogue mobile apps are an evolution of phishing that attackers create by cloning the legitimate mobile apps and adding specific functionality to repurpose it to capture information such as Card details/credentials or install malicious software. There are many tools available on the market which can quickly clone the apps and let user add their own code. With many applications being uploaded daily to Google and Apple, as well as third party stores, it is important to monitor for Rogue/Fake/Malicious applications and prevent them being targeted towards unsuspecting end users to steal data, credit card info or distribute malware. The research team continuously monitors most popular app stores to identify newly created apps that appear similar to the customer's official application. On identification of the rogue app the team will notify the customer and provide an option to initiate the process of takedown of these apps from all the app stores. Upon customer request the research team will also provide detailed analysis of the app functionality along with related threat indicators.

2.2.5. Social Media

The service and platform protect an organisation's social media against Brand impersonation attacks and Malware distribution. Brand impersonation occurs when a page or user is created that has been set up to look like and resemble a business. These accounts are used to gather information on the people that follow or like the pages, or to run fake promotions that will generate activity around the account and help it increase the number of followers. The team continuously monitor the social media if the organisations brand has been impersonated and notify the organisations and help to takedown the content.

2.2.6. Credential Leak Monitoring

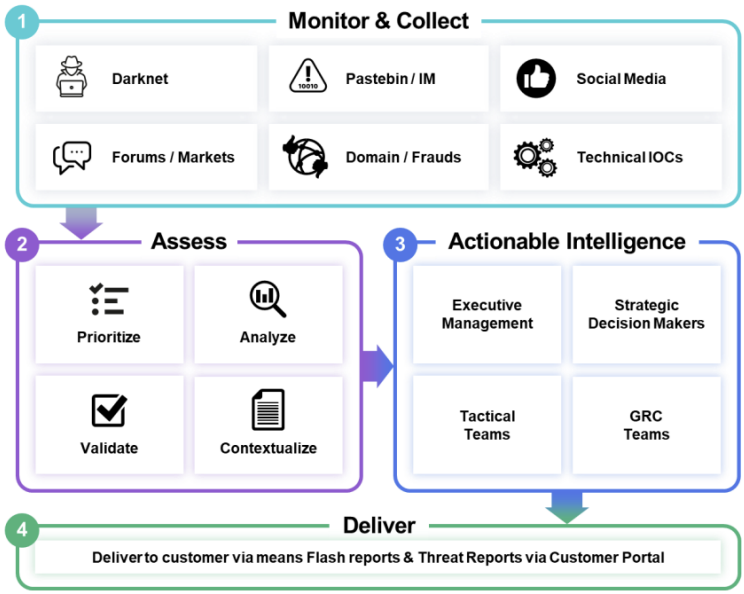
The service and platform continuously monitor for credential leaks and alerts customer via the portal which will be automatically populated if there are any leaked/breached credentials involving email addresses of the organisations or the users of their systems. As part of consolidated collection, the leaked credentials are gathered from multiple sources, including:

- Publicly leaked / breached databases
- Privately shared databases
- Paste Sites
- Malware Infections

The leaked credentials are the primary source of 'Password Re-Use' Attacks. It is important for any organisation to remediate them with highest priority.

2.3. Adversary Centric Intelligence

Adversary Centric Intelligence (ACI) provides contextual insights into imminent threats to organisations and allows them to respond faster to incidents, better understand their attackers and safeguard their assets. ACI provides comprehensive coverage of Dark Web, Open Source and Technical Threat Indicators from dominant and emerging threats. The intelligence includes threat actor insights to help organisations proactively assess risks, look for vulnerabilities in the existing setup and increase the security awareness of their staff.



2.3.1. Dark Web Monitoring

Dark Web monitoring includes carefully collecting, categorizing and disseminating all threat related information based upon customer profile and relevance from various Forums/sites/IRC/I2P sites. Human Intelligence is the activity involving human interaction and engagement with threat adversaries to extract relevant organisation information which would not be posted by threat actor on any Dark Web forum.

2.3.2. Technical Intelligence

The service and platform have strong technical intelligence (TECHINT) capabilitie allowing us to continuously monitor various campaigns and reports detailed IOCs and technical information via reports and customer portal. The technical research team will provide research outputs on regular intervals about technical research based upon:

- Phishing Campaigns
- Malware
- Phishing Kits
- Domain Squatting

In addition to this the service provides an option to investigate any observables within the platform, including:

- IP Address
- Malware Hash
- URL

- Domain

To facilitate understanding of attacker tools, tactics and procedures, the findings in TECHINT reports are mapped to MITRE ATT&CK Framework.

2.3.3. Open Source Intelligence

Open-Source Intelligence (OSINT) as it is commonly referred is method of gathering threat intelligence from publicly available sources. Initially OSINT covered simple sources such as blogs, news, business websites, social networks. Over time OSINT coverage has changed to a great extent. Researchers have years of experience in collecting and prioritizing intelligence with OSINT and then verifying it with all possible contextual information collected via other private sources. This allows organisations to correlate the information which is being spoken in public media with solid context. Following is the sample list of OSINT collection sources; this list is updated regularly as new sources appear:

- Social Media
- Instant Messaging (IRC/Jabber)
- Paste Sites (like Pastebin)
- GitHub Repositories
- Blogs & News sites

2.4. Managed Takedowns

Requests for Managed Takedowns are done via our Service Request portal. The service uses proprietary DMCA process to carry out the takedowns, which includes notices to the offending parties, hosting providers and registrars with provisions of local and international laws to demand the takedown on account of impersonation/phishing etc.

The current types of takedowns covered, and evidence required are included below:

Type of Incident	Sub-types	Typical Evidence Required
Phishing	**Hacked Website:** Phishing content on a compromised site **Malicious Domain:** Domain registered imitating a trademark (must be evidence of phishing) **Redirect:** A URL that is redirecting to a phishing site **Subdomain:** A phishing domain hosted on a subdomain **Pharming IP:** An IP or Server that serves phishing pages **Free Hosting:** Phishing domain registered with free hosting providers **URL Shortener:** Infringing sites that are hosted/redirect from shortened URLs **Post Target:** Domains where criminals post stolen information	Live URLs Email Samples
Mobile App	**Copy of Legitimate App:** URL on third party store advertising a clone of a client mobile app **Adware:** Branded APK or IPA files used to install adware on a	Link to URL Link to Original Content

	mobile device **Mobile Malware:** Malicious mobile app using company branding to malware, such as for credential theft **Redirect:** A redirect that will send users to a malicious mobile app link **Mobile Brand Abuse:** A third party mobile app listing that is not malicious, nor advertising a direct download, but is making money off listing company's legitimate app	Letter of Authorisation
Brand Abuse	**Profile:** Malicious profile on social media impersonating brand of individuals (excluding negative sentiment) **Page:** Malicious page on social media impersonating brand or individuals (excluding negative sentiment) **Group:** Malicious group on social media impersonating brand or individuals **Post:** Malicious post spread on social media that seeks to damage brand or spread false information **Event:** Malicious event on social media that lists business' premises as location without permission **Fake Survey:** Fake survey distributed without consent, often offering free prize giveaways **Gambling Site:** Fake gambling sites impersonating casinos **Fake News:** Fake articles about an individual or business **Data Leakage:** Confidential information leaked online **Pornography:** Brands posted to pages with pornographic content **Job Ads:** Fake job ads for companies **Marketplace:** Marketplaces using company brand or intellectual property for monetary gain **Paid Search:** Malicious links promoted via paid search engine **General Trademark:** Trademarks infringed or posted without consent	Direct link to offending content Trademark information Copy of Government-issued ID Letter of authorisation
Malware	**Redirect:** URL redirecting a user to a malware distributing URL **Command and Control:** Malware command and control centre **Dropzone:** Publicly writable directory on a server owned by a criminal as is used to capture stolen information **Pharming DNS:** Malicious DNS server that accepts traffic and redirects them to a Pharming IP address	Copy of malicious DNS server, malware or redirect
Messaging and Communications	**Email (Malicious):** An email impersonating an individual or organisation **Unified Communications:** Account on messaging network (i.e., Skype) impersonating name **SMShing:** Malicious SMS sent to customers, directing to phishing or malware sites **Vishing:** A number used for malicious activity or impersonating brand **Mobile Brand Abuse:** A third party mobile app listing that is not malicious, nor advertising a direct download, but is making money off listing your legitimate app	Copy of original email/SMS Copy of Account Handle/Phone Number

2.5. Asset Types Collected and Monitored

The following table lists the asset information to be collected and monitored.

Asset Type	Description
Access Key	Access keys are a type of security credential, similar in principle to user credentials, that allow authentication to systems, be they third parties or your internal systems. Generic access key names, e.g., “Admin”, should be avoided, and we advise against the submission of secret keys.
Brand	An example would be the company logo, images or marketing images with a colour scheme and hex code Company logo images should be attached as a .PNG file and the name of the file added to the list of assets along with the specific HTML colour hex code contained within brackets e.g. (Logo1.png IndianRed #CD5CfC LightCoral#F08080)
Company	Any Company names owned by the client and any additional logos or images that should be monitored
Domain	List of any company owned domains
Key staff member	Full names of key members of staff e.g. CEO, CFO etc.
IP address	CTR TIPS accepts IP addresses or ranges in CIDR, e.g., 1.2.3.0/24, or netblock, e.g., 1.2.3.4 - 1.2.3.56, formats. Ranges larger than /16 (IPv4) or /112 (IPv6) cannot be accepted due to their size
Server format	CTR TIPS uses server format assets to detect sensitive code or technology that has been exposed online. Server format assets should be regular expressions or text strings that can be used to identify your servers. For best results, only add assets that can uniquely identify your servers. Generic server formats should be avoided where possible.
Server name	CTR TIPS uses server name assets to detect sensitive code or technology that has been exposed online. Server names should be text strings that refer to internal servers used by your organisation. To ensure the best results, server names should uniquely identify a server that belongs to your organisation. Generic or short server names should not be added.
Allowed port	List of expected open ports
Code format	CTR TIPS uses code format assets to detect sensitive code or technology that has been exposed online.

	Code format assets should be regular expressions or text strings that uniquely identify strings contained within your code base. To ensure best results, regular expressions should not match any generic libraries, or publicly available code. Generic code formats should be avoided where possible.
Code repository	CTR TIPS can use your public GitHub and GitLab code repositories to attribute potentially sensitive data leakage to your organisation. To add all code repositories belonging to a user or group, enter the profile URL. Individual repositories can be removed from the list at the next step.
DLP identifier	A machine-readable marking, DLP identifiers are used as a unique identifier of a marked document. CTR TIPS will raise alerts for all detected documents containing the DLP identifier asset within the document or metadata.
Document marking	A human readable marking used to classify the sensitivity of company documents, e.g., “Confidential - Not for Distribution”.
General keyword	A general keyword search that when seen together with another asset, may indicate a data leak
IIN/BIN	Issuer identification numbers (IINs), also known as bank identification numbers (BINs), are 6- or 8-digit numbers at the start of payment card numbers that are used to identify the institution that issued the card to the card holder. If your organisation uses IINs/BINs then adding these as assets enables CTR TIPS to detect exposed payment cards.
Mobile app	Any mobile app created by your organisation
Mobile app keyword	CTR TIPS uses mobile app keywords to identify mobile applications that are impersonating your organisation within the app title or description text. Mobile app keywords can be app names or app description text that uniquely identifies a mobile app as being associated with your organisation.
Phone number	Sensitive phone numbers are used to detect where company, employee or VIP phone numbers are exposed online. To ensure best results, assets should not be added for phone numbers that are meant to be publicly available, for example customer support or office reception phone numbers. Phone numbers should be prefixed with the country calling code. Whitespace is optional and will be ignored.

Package name	CTR TIPS uses package name assets to detect sensitive code or technology that has been exposed online. Package name assets should be text strings that refer to a package name that is unique to your company. Examples of package names could be mobile applications, or internally developed packages that are not publicly available. Package name assets should follow the standard naming conventions where possible, e.g., “com.example.package” for Java packages.
Sensitive code identifier	CTR TIPS uses sensitive code identifier assets to detect sensitive code or technology that has been exposed online.
Sensitive keyword	Sensitive code identifiers should be text strings that uniquely identify your codebase. Example code identifiers can be references to internal domains, code comments, or any other code strings that are unique to your organisation. To ensure best results, sensitive code identifiers should indicate code that is only used by your organisation and that is not intended to be publicly available.
Social media hashtag	
Social media profile	
Supplier	Assets are used in a pre-set intel update subscription to notify you when your suppliers are mentioned in intel updates.

Solution Architecture description

3. Managed Service Details

3.1. Service Features Overview

Managed DRPS is available in three service tiers, aligned to the platform licensing feature tiering as outlined in section 2 Solution Architecture - Digital Risk Protection Platform, otherwise the features are common across all tiers.

1. Managed DRPS – Includes support and management of External Attack Surface Management (EASM)
2. Managed DRPS+ - Includes support and management of EASM and Brand Protection (BP)
3. Managed DRPS Complete – Includes support and management of all features of the platform including EASM, BP, and Adversary Centric Intelligence (ACI)

See below the features of the Managed Digital Risk Protection Service (DRPS):

Managed Service Features	Managed DRPS	Managed DRPS+	Managed DRPS Complete
External Attack Surface Management (EASM) support and management	✓		
Brand Protection (BP) support and management	✓	✓	
Adversary-Centric Intelligence (ACI) support and management	✓	✓	✓
Platform configuration setup and management	✓	✓	✓
Continuous maintenance to monitor for agreed digital risks associated with defined customer assets and asset identifiers	✓	✓	✓
Online Portal Customer platform access and ad-hoc searches	✓	✓	✓
Centralised ticketing - email, phone and portal	✓	✓	✓
24x7x365 monitoring of threats	✓	✓	✓
Threat triage analysis & prioritisation	✓	✓	✓
Elimination of false positives	✓	✓	✓
Response alerting and remediation recommendations	✓	✓	✓
Curated, tailored actionable insight to inform security strategy and investment	✓	✓	✓
Major and vertical specific threat advisories	✓	✓	✓
Daily threat intel digest	✓	✓	✓
Weekly alert summary reporting	✓	✓	✓
Monthly report and service review	✓	✓	✓

Quarterly strategic review	✓	✓	✓

3.2. External Attack Surface Management (EASM) support and management

Feature Overview	Overview text
Feature Details & Deliverables	Details text

3.3. Brand Protection (BP) support and management

Feature Overview	Overview text
Feature Details & Deliverables	Details text

3.4. Adversary-Centric Intelligence (ACI) support and management

Feature Overview	Overview text
Feature Details & Deliverables	Details text

3.5. Platform configuration setup and management

Feature Overview	Overview text
Feature Details & Deliverables	Details text

3.6. Continuous maintenance to monitor for agreed digital risks associated with defined customer assets

Feature Overview	Overview text
Feature Details & Deliverables	Details text

3.7. Online Portal Customer platform access and ad-hoc searches

Feature Overview	Overview text
Feature Details & Deliverables	Details text

3.8. Centralised ticketing - email, phone and portal

Feature Overview	Overview text
Feature Details & Deliverables	Details text

3.9. 24x7x365 monitoring of threats

Feature Overview	Overview text
Feature Details & Deliverables	Details text

3.10. Threat triage analysis & prioritisation

Feature Overview	Overview text
Feature Details & Deliverables	Details text

3.11. Elimination of false positives

Feature Overview	Overview text
Feature Details & Deliverables	Details text

3.12. Response alerting and remediation recommendations

Feature Overview	Overview text

Feature Details & Deliverables	Details text

3.13. Curated, tailored actionable insight to inform security strategy and investment

Feature Overview	Overview text
Feature Details & Deliverables	Details text

3.14. Major and vertical specific threat advisories

Feature Overview	Overview text
Feature Details & Deliverables	Details text

3.15. Daily threat intel digest

Feature Overview	Overview text
Feature Details & Deliverables	Details text

3.16. Weekly alert summary reporting

Feature Overview	Overview text
Feature Details & Deliverables	Details text

3.17. Monthly report and service review

Feature Overview	Overview text
Feature Details & Deliverables	Details text

3.18. Quarterly strategic review

Feature Overview	Overview text
Feature Details & Deliverables	Details text

4. Reporting

Reporting overview

Commented [BM1]: Describe the reports that are produced part of the service, the frequency (on demand, daily, weekly, fortnightly, monthly, quarterly, annually, etc.) Include any report also mentioned in the Feature Descriptions above.

Heading	Description	Cadence	Applicable Tier
Proactive IOC Review and Report (Daily)	Report Description	Frequency	
Monthly 24-point Health Check	Report Description	Frequency	
Report name	Report Description	Frequency	

Reporting detail.

Commented [BM2]: Include details for every report as to wh content is included in each.

Commented [BM3]: Provide information on the service port what is available, dashboards, and any customer self-service opti that are available.

5. Portal

Service portal / dashboard details

6. Service Level Agreements (SLAs)

Commented [AA4]: Added the standard SLAs - may need to remove irrelevant SLAs from the service, e.g. if the service doesn have security monitoring, remove the security SLAs.

6.1. Availability and Service Window

The service window is 24/7/365 (24 hours a day, 7 days a week, 365 days a year). In this context the service window means the operation of the SOC and Service Desk to monitor the customers estate, respond to events, and respond to tickets logged. The response, in terms of engagement to investigate an issue or fulfil a request, is dependent on the time of day and the priority of the item.

6.2. Definitions

- The alert acknowledgement SLA: the time between a new alert being received into SOAR (Case Stage: New) and Integrity360 beginning triage activity (Case Stage: Triage). Triage activity may be automated for alerts with playbooks or manual.
- The triage SLA: the time between the alert being received (Case Stage: New) and triage completing (either Case Stage: Incident or Case Closed: False Positive), with the alert being either correlated to an existing incident, marked as a false positive or notified to customers as an incident.
- The investigation target: the intent for incidents to be fully investigated, customer notified, and response actions proposed. This is defined as the time between an alert moving to a security incident and the security incident management stage completing. This does not include the execution of response actions, which may require additional analysis/planning and/or customer approval. The investigation time is only a target and not a contractual obligation, as the effort and time involved will vary depending on the nature of the incident.
- The implementation time: the estimated effort to implement a change.
- The implementation period: the elapsed time from the approval of the change to change completion.
- Business days: normal working days in the country of contract, excluding bank/public holidays and weekends. Integrity360's normal working days are Monday - Friday 09.00 – 17:30, excluding bank/public holidays.
- Non-security incident priorities are defined as follows:

Priority	Severity	Description
Priority 1 (P1)	Critical	Operations or business is severely impacted due to the supported products not adhering to its specified agreed function.
Priority 2 (P2)	High	Group/department operations or business is severely impacted due to the supported products not adhering to its specified agreed function.
Priority 3 (P3)	Medium	Less than ten users impacted due to the supported products not adhering to its specified agreed function.
Priority 4 (P4)	Low	Minor degradation of service due to the supported products not adhering to its specified agreed function.
Service Request	N/A	A request from a user for information, or advice, or for access to an IT service.

6.3. (Non-Security) Infrastructure/Platform Incident SLAs

Priority	Service Window	Target Response	Target Resolution
P1	24x7	15 minutes	4 hours
P2	24x7	1 hour	8 hours
P3	8x5	8 working hours	16 hours
P4	8x5	16 working hours	40 hours

6.4. Security Incident SLAs

Incident Severity	Service Window	Acknowledgement SLA	Triage SLA	Investigation Target SLA
Critical	24x7	15 minutes	1 hour	2 hours
High	24x7	30 minutes	2 hours	4 hours
Medium	8x5	2 hours	4 hours	8 hours
Low	8x5	24 hours	24 hours	16 hours

6.5. Change Management SLAs

Change Type	Change Classification	Approval period	Implementation Time	Implementation Period	Service Window
Standard Change	Minor	Pre-approved	2 hours	2 days	Normal Business Hours
Normal Change	Minor	Up to 5 days	3 hours	3 days	Normal Business Hours
Normal Change	Moderate	Up to 5 days	4 hours	5 days	Normal Business Hours
Normal Change	Major	Up to 15 days	Subject to separate scoping and not included in the managed service		
Emergency Change	N/A	Emergency approval or retrospective approval	N/A	4 hours	N/A

7. Appendices

Commented [BM5]: For detailed reference information relat to the service, please use the Appendices to present it to avoid breaking up the flow of the main body of the document

7.1. Appendix 1.

7.1.1. Sub section

7.2. Appendix 2.

7.2.1. Sub section

integrity360.com

8. Tables

Table heading

Heading	Heading	Heading
Text should be left aligned	Text should be left aligned	Text should be left aligned
Text should be left aligned	Text should be left aligned	Text should be left aligned
Text should be left aligned	Text should be left aligned	Text should be left aligned

Title	Text should be left aligned
Title	Text should be left aligned
Title	Text should be left aligned