CYBERSECURITY

ThreatWatcher

Continual visibility into your digital attack surface and supply chain

LRQA

Contents

What is ThreatWatcher?

Are you looking to discover unknown threats lurking within your internet attack surface and strengthen your external threat management programme?

LRQA
THREAT
WATCHER

LRQA's Cyber Threat Intelligence (CTI) Service, ThreatWatcher, scours millions of digital data points to identify and alert you to risks in the wild so you can take action before they have the chance to impact your business.

ThreatWatcher is a fully tailorable modular-based managed CTI service, which utilises our mature and unique capabilities to deliver detailed insights into the risks and impacts of cyber threats for your organisation. By design, ThreatWatcher is an extension of your organisation, providing situational awareness and contextual information.

When combined with our intelligence analysts, it enables your organisation to make informed decisions, maintain its desired security posture, and effectively employ its technologies to prevent and detect attacks.

Why use ThreatWatcher?

With 70% of breaches originating outside your company's network, organisations are struggling to understand what they own, where it is, the risk it presents and how to protect it.

Attacks on internet-exposed assets often circumvent traditional security tools and place an enormous burden on information security organisations. ThreatWatcher scours over a million digital channels, taken from the surface, deep and dark web, and specific mobile and social platforms to identify and assess risks in the wild, meaning you can action them before they impact your business.

Gain visibility into your digital attack surface through the lens of an attacker

The task of trying to keep pace with the cyber threat landscape, not to mention the challenges of having and maintaining an in-house intelligence capability are not easy nor financially insignificant.

ThreatWatcher is a service which allows us to share our expertise and insight with you by allowing you to have an intelligence-driven and operational approach to cybersecurity which is holistic and specific to your organisation. Alternatively, ThreatWatcher can supplement your existing capabilities, providing in-depth expertise and availability when you need it the most.

Cyber-attacks are not isolated spontaneous events

CTI is necessary to understand the cyber threat landscape and what is required to protect your environment and your people.

When your data is protected by your firewalls and internal security, understanding where it is and who is accessing it is sometimes easy, but when the data is on the internet it is nearly impossible to build an accurate picture. That is where ThreatWatcher comes in. It leverages both proprietary and commercial security intelligence platforms which aggregate data from the largest set of surfaces, closed, and technical sources to provide visibility and context of data which could be used in an attack against your organisation. This is indexed and made available for our CTI analyst team.

ThreatWatcher is about providing you with an understanding of your organisation's specific cyber threat landscape and how it relates to your critical assets.

ThreatWatcher is delivered by our team of highly skilled and experienced CTI analysts and delivers timely intelligence which is the combination of knowledge, data, and context. All designed to help you prevent or mitigate cyber attacks.

How does ThreatWatcher work?

Previous Next

Identify external threats and prevent an attack

Imagine an attacker has just cloned your employee benefits portal and hosted it under a new domain, similar to the original. Would you know how to spot it? What if your employees have been using the same work email and password combination to sign up for eCommerce or online fitness services and those services were compromised? Would you know which users had been affected?

These examples of external threats are commonplace in the digital age and are constantly changing. It is time to take an attacker's view of your organisation through ThreatWatcher.

Security intelligence is the combination of knowledge, data, and context that allows you to prevent or mitigate cyber-attacks. ThreatWatcher is delivered by our team of highly skilled and experienced CTI analysts, using proprietary and commercial security intelligence platforms. This powerful combination leverages CREST-certified analysts and a combination of over one million data sources analysed and contextualised for the following threat categories, culminating in a detailed report with full details of the findings and recommendations.

Domain threats

Domain threats involve registering, trafficking, or using an internet domain name previously used or very similar to a corporate online business identity or website. Domain Squatting is often a precursor to email-based attacks and can trick users into surrendering credentials via phishing attacks.

Credential threats

Credentials are gold for an attacker. The current rise in credential 'dumps' (valid passwords, usernames, e-mail addresses) making their way online or for sale lowers the bar for a would-be attacker gaining access to your corporate systems.

Deep and dark web monitoring

The Deep and Dark Web is where hackers and threat actors trade information on corporate targets for malicious purposes. Dark Web monitoring searches terms and keywords relevant to your company and identifies potential threats facing your brand, suppliers, and employees.

Social brand threats

Monitoring internet resources and identifying content and logo abuse helps organisations to take action on controlled usage of their corporate brand. This helps prevent malicious use by third parties and individuals, which may lead to reputational and loss of trust with consumers.

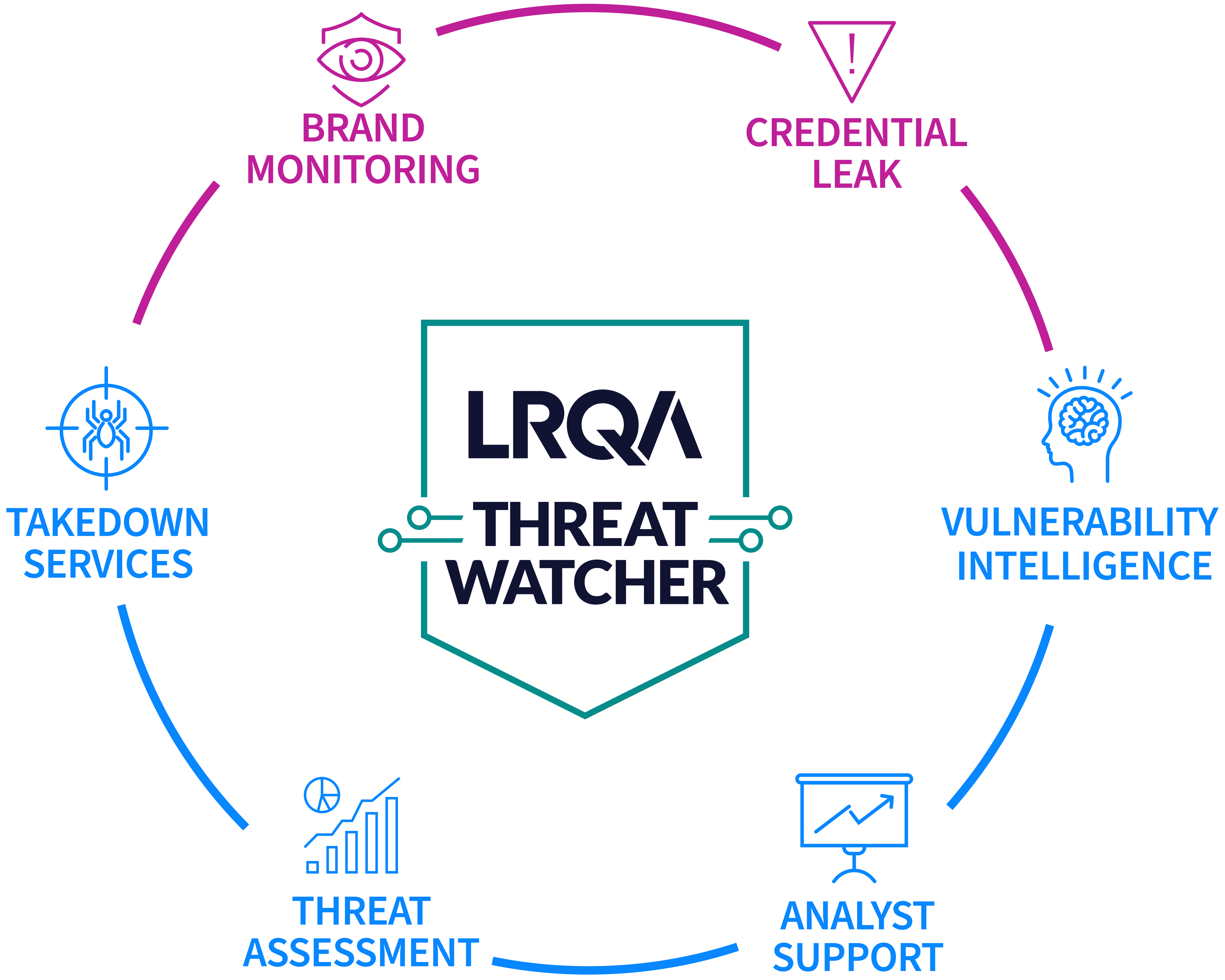
Threat actors assessment

When organisations build their cybersecurity capability understanding adversaries is essential. Knowing and tracking threat actors targeting your industry becomes an essential part of managing your threat landscape.

Data leakage threats

Paste sites and code repositories can sometimes disclose a treasure trove of details relating to your organisation, the way it operates or sensitive information such as certificates, passwords, and keys to your most critical assets.

What are the benefits of ThreatWatcher?



ThreatWatcher reduces the time between known and unknown threats, helping you identify risks presented by your organisation and assessed through the lens of an attacker.

If you are looking to discover unknown threats and strengthen your external threat management programme, then ThreatWatcher is the solution. It provides situational awareness and contextual information to enable informed decision-making and maintain security posture.

Our intelligence analysts look to identify similarities and differences in vast quantities of information and detect deceptions to produce accurate, timely and relevant intelligence.

We ensure ThreatWatcher outputs are a customised solution for you, enabling your organisation to make informed decisions, maintain its desired security posture and effectively employ its technologies to prevent and detect attacks.

ThreatWatcher provides access to our industry insights with a deep analysis of the specific tools, techniques, and threat actors. This helps your organisation answer the key questions:

- Who are my real adversaries?
- What are their tactics, techniques, and procedures?
- How do I defend against them?
- Where do opportunities lie?
- Is my security posture proportionate with my threat profile?
- What threats are of significance to my industry vertical?

How ThreatWatcher is delivered and what you get

Whether you require a full CTI service or a combination of modules, you choose what is right for you. ThreatWatcher can be customised to ensure you get your desired level of situational awareness and contextual information.

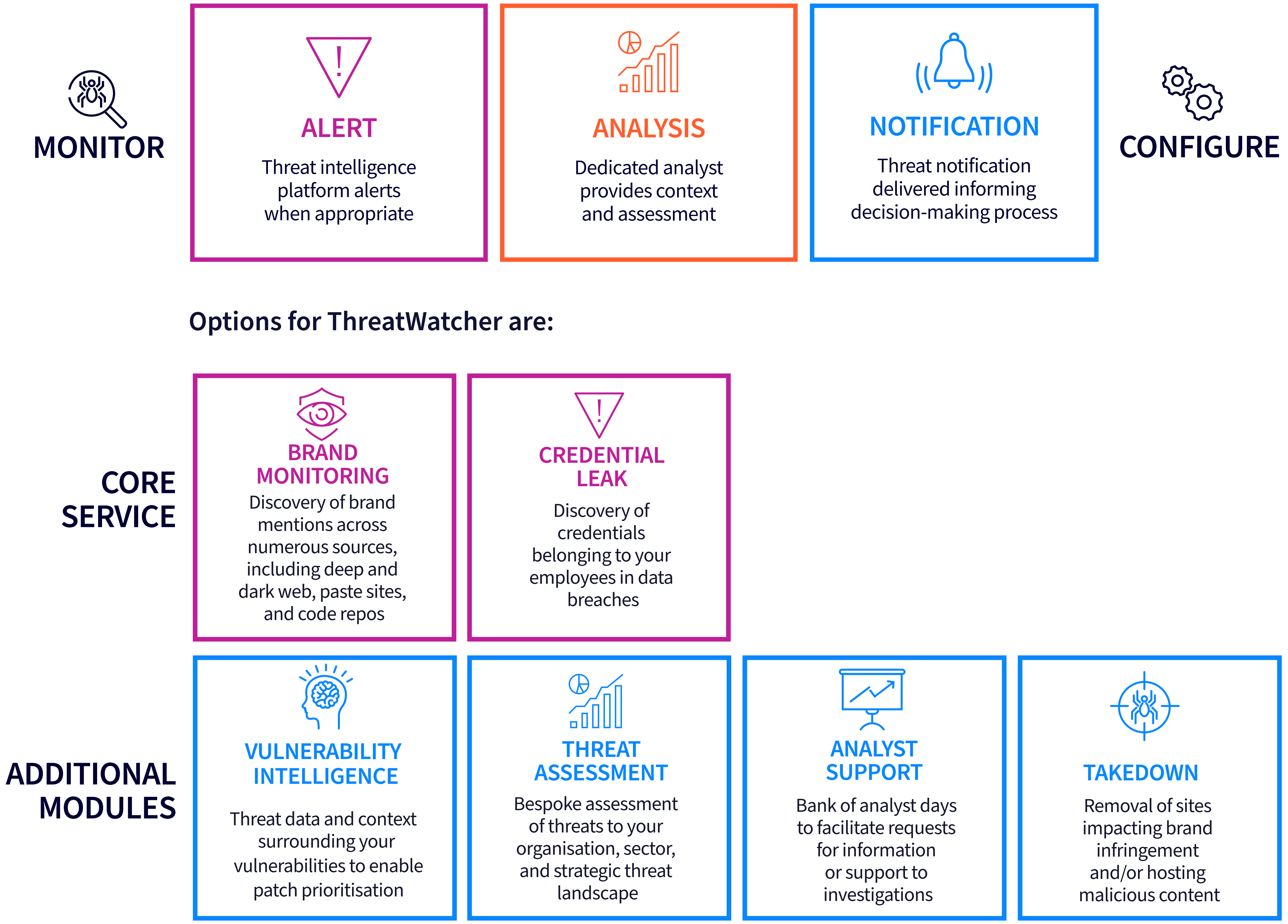
ThreatWatcher provides access to the most highly accredited expertise, combined with leading security technology, to capture your intelligence requirements. ThreatWatcher's advanced reconnaissance and analytics help identify previously unknown threats that could be used against your organisation in a cyber-attack, spanning people, processes, and technology.

Our CTI capabilities allow us to execute broad, intelligence-based exercises, of the kind typically undertaken by real-world threat actors as they prepare for their attack. The objective is to draw a picture of the organisation, through the lens of an attacker, this is key for adding contextualisation.

Our CTI will provide value add, by reducing uncertainty, while aiding in identifying threats and opportunities, reducing the risk of a real attack.

ThreatWatcher outputs are specific to your organisation and can be consumed at all business levels, tactical to strategic, allowing you to maintain optimal defences appropriate to your threat and risk profile.

Once you are onboarded onto the service our analysts will work with you to establish the correct watchlists within our Threat Intelligence Platform. Once these are live, alerts will fire when any of the target entities have been matched. Our analysts will then review this alert and establish its veracity before then looking for contextual information to support the finding. Finally, an assessment will be made of the findings before forwarding them to the predefined contacts. If required and necessary, we also can support 24/7 threat notification delivery.



MONITOR

ALERT
Threat intelligence platform alerts when appropriate

ANALYSIS
Dedicated analyst provides context and assessment

NOTIFICATION
Threat notification delivered informing decision-making process

CONFIGURE

Options for ThreatWatcher are:

CORE SERVICE

BRAND MONITORING
Discovery of brand mentions across numerous sources, including deep and dark web, paste sites, and code repos

CREDENTIAL LEAK
Discovery of credentials belonging to your employees in data breaches

ADDITIONAL MODULES

VULNERABILITY INTELLIGENCE
Threat data and context surrounding your vulnerabilities to enable patch prioritisation

THREAT ASSESSMENT
Bespoke assessment of threats to your organisation, sector, and strategic threat landscape

ANALYST SUPPORT
Bank of analyst days to facilitate requests for information or support to investigations

TAKEDOWN
Removal of sites impacting brand infringement and/or hosting malicious content

How ThreatWatcher is delivered and what you get

The core service focuses on answering key questions likely to be present in any organisation's intelligence collection plans. Common questions that will trigger an alert, assessment and notification include:

- Has there been any mention of your brand(s) identified on the dark web? And in what context?
- Are any credentials belonging to your employees identifiable online?
- Is it possible to identify potential typo-squatting domains about your portals and websites?
- Has your website been cloned during the coverage?
- Are your brands or employees mentioned on paste sites?
- Are your brands or employees mentioned within code repositories?

Additional modules can include:

Vulnerability intelligence module

This module provides organisations with context and real-world threat data associated with their vulnerability exposure. The end state is to provide additional context around vulnerabilities present in the network to enable a prioritised patch remediation effort. The module is seeded with a recent vulnerability scan (covering the appropriate business units in scope) and is repeated monthly.

Threat assessment module

This module would provide a monthly analysis of the threat landscape that's directly relevant to your organisation, the industry vertical you operate in and any strategic observations that are likely to be of interest to the organisation.

Analyst support module

Throughout the life of the service, you can call upon our team of CTI analysts to provide intelligence on specific matters or provide additional context into threats discovered in the service. This key component means you have access to your intelligence capability or, where one already exists, additional capacity and capability. This provides you with the opportunity to reach out to our analysts and task them to deep dive into threat topics of your choosing.

Takedown services

Any infrastructure or service deemed to be impeding your brand or hosting malicious content can also be requested for takedown through this service. This important capability ensures that assets that are identified as being malicious can be actioned using the takedown service.

Other additional reporting methods for the service include:

Weekly briefs

If chosen, this reporting option provides the opportunity for the threat notifications to be supported by a weekly briefing from the analysts to talk through the pertinent issues of the week and will be supported by additional departments and expertise throughout LRQA (if needed).

Monthly summary

If chosen, this reporting option provides a thorough output of the results from the prior month's activity and takes the opportunity to provide any retrospective analysis that could not be developed at the time. Intelligence Summaries (INTSUMS) authored by LRQA will also be included when appropriate.

ThreatWatcher and ISO/IEC 27001:2022

On the 25 October 2022, a revised version of ISO 27001 was published - marking a new era of information security best practice.

The major changes in ISO 27001:2022 that organisations need to be aware of are the updates to Annex A controls in alignment with ISO 27002:2022, which includes the restructuring of the original 14 control domains into four categories and the total number of controls being reduced from 114 to 93 – due mainly to the merging of 57 controls into 24 controls. 58 controls remain mostly unchanged, with minor contextual updates, and 11 controls are brand new to ISO 27001:2022.

ISO 27001:2022 Organisational control: Threat intelligence

One of the new organisational controls, A.5.7 Threat intelligence, requires organisations to collect, analyse and produce threat intelligence regarding information security threats.

The goal of this new control is to provide organisations with a deeper understanding of cyber threats by collecting, analysing, and contextualising data about current and future cyber attacks. The new control is also designed to help organisations understand how they might be hacked and inform companies about what types of data attackers are seeking.

ThreatWatcher provides these exact solutions, helping organisations demonstrate compliance with the new threat intelligence control.

Contact our experts for more information about ThreatWatcher and how it can help demonstrate compliance with the new requirements and controls introduced in ISO 27001:2022.

CONTACT US

About LRQA:

LRQA is the leading global assurance partner, bringing together decades of unrivalled expertise in assessment, advisory, inspection and cybersecurity services.

Our solutions-based partnerships are supported by data-driven insights that help our clients solve their biggest business challenges. Operating in more than 150 countries with a team of more than 5,000 people, LRQA's award-winning compliance, supply chain, cybersecurity and ESG specialists help more than 61,000 clients across almost every sector to anticipate, mitigate and manage risk wherever they operate.

In everything we do, we are committed to shaping a better future for our people, our clients, our communities and our planet.

Get in touch

Visit **www.lrqa.com** for more information or email **cybersolutions@lrqa.com**

LRQA
1 Trinity Park
Bickenhill Lane
Birmingham
B37 7ES
United Kingdom

Care is taken to ensure that all information provided is accurate and up to date; however, LRQA accepts no responsibility for inaccuracies in or changes to information.