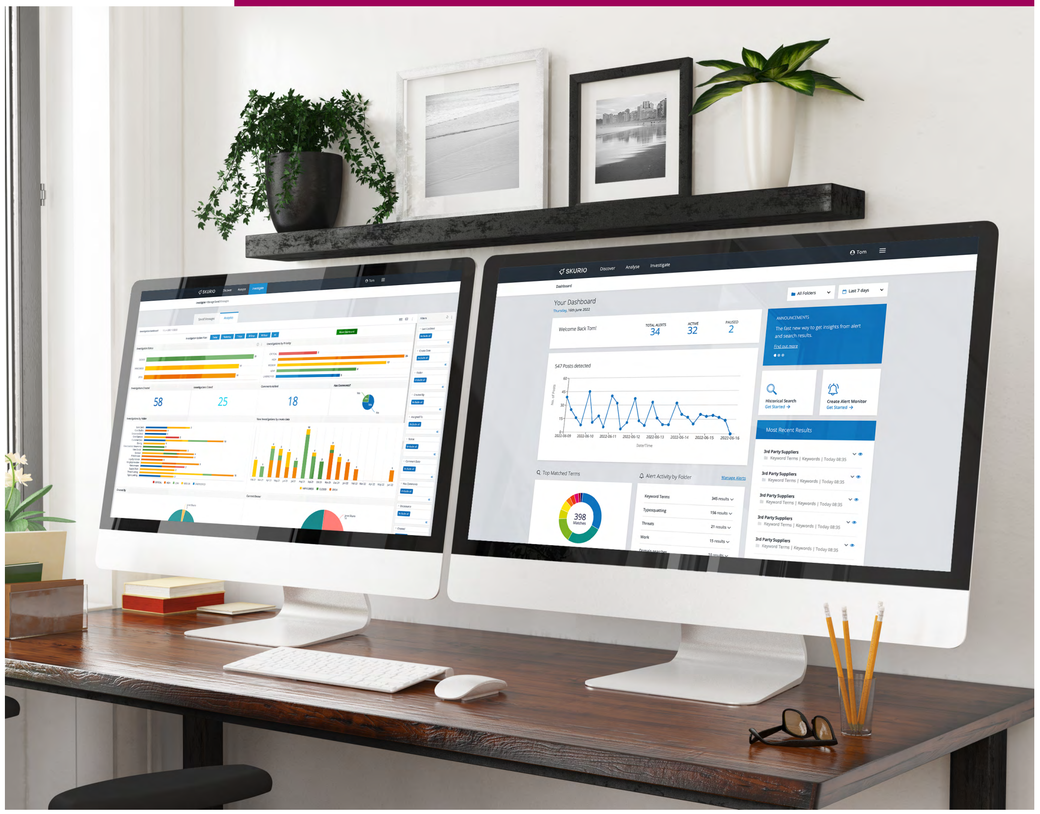
The Skurio tailored threat intelligence playbook

Your guide to efficiently maturing your cybersecurity strategy with tailored threat intelligence.

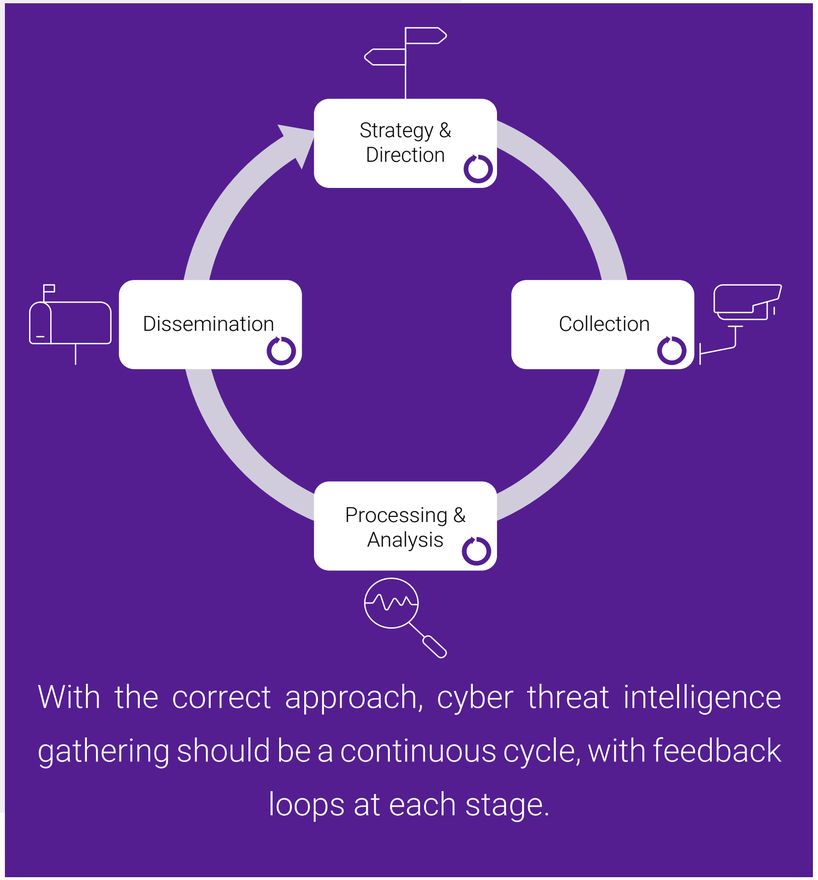
info@skurio.com | skurio.com

Table Of Contents



What is cyber threat intelligence?

and how could your business benefit from it?



With the correct approach, cyber threat intelligence gathering should be a continuous cycle, with feedback loops at each stage.

Your organisation may already be in the cross-hairs of threat actors. Gathering information to understand who is targeting your business, why and how, can help you mitigate such threats. Put simply, this is cyber threat intelligence. Various methods of collecting and processing information are used to produce and disseminate cyber threat intelligence at strategic, operational and tactical levels. Each level has a purpose and stakeholders, but good cyber threat intelligence takes the needs at all levels into consideration, providing *insight and foresight* to create a well-rounded view of the evolving threat landscape.

A stitch in time saves nine

Threat intelligence can be used to prepare for, identify, prevent, and recover from cyber-attacks. But it's worth noting that an organisation is most at risk from a cyber-attack when an incident has already happened. By averting attacks before they happen and resolving incidents quickly, you can use cyber threat intelligence to prevent incidents from snowballing and overwhelming your business.

Why tailored threat intelligence?

One size doesn’t fit all...

Your cybersecurity strategy impacts all stakeholders of your business, from the executive board to staff, customers and partners. You’re probably already facing questions from your senior leadership team about your efforts to keep data safe and prevent cyber incidents. Many IT and security leaders in your position want to improve their security posture by implementing a Cyber Threat Intelligence solution. But, the cost and the impact on resources often prove too much of a challenge. Every department and team require something different from threat intelligence:

Business leaders
want to know you have their back and be able to prove to investors they take cybersecurity defences seriously.

Architects, admins & SOC managers
need tactical advice to help them build and manage robust IT solutions.

Security operations staff
want to know if the business is, or will be, under attack to boost defences where necessary.

Incident response teams
need intelligence on vulnerability exploitation methods to stop attacks and recover smoothly.

That’s a lot of boxes to tick!

Traditional threat intelligence platforms can meet all these demands but come at a hefty price, because they support large enterprises with deep pockets and copious resources, by design. These solutions provide blanket coverage of vulnerabilities, potential threats, zero-days and threat actors - all of which can leave busy teams swamped with interesting but irrelevant alerts.

Cutting your cloth to suit your needs

If your resources are under strain, don’t worry. Tailored threat intelligence could be the answer for you. This type of solution is perfect for organisations looking to establish an intelligence capability or for businesses with a mature team that can benefit from an external threat feed that is less noisy.

Threat intelligence production relies on collecting relevant and timely information from appropriate sources. When done manually, this information gathering is resource-intensive. But, behind the scenes, many cyber threat intelligence platforms rely on teams of analysts doing precisely that. As a result, these solutions come with a designer price tag - but tailored threat intelligence can provide a perfect fit!

The key to this is automation. You wouldn’t hand-stitch a suit if you had a state-of-the-art sewing machine - so why use precious resources on activities like information gathering? Skilled information security staff can better spend their time analysing business needs and the potential threats identified. The next factor is customising your feeds. Your business will have its priorities, and certain types of threats could be specific to your industry. With tailored threat intelligence, you can define alert monitors to scan feeds from the surface, deep and Dark Web for terms specific to your business, so you only get the results that match.

Step one: Getting started

Take some measurements!

If your organisation is new to cyber threat intelligence, you'll need to understand the threats it could face.

- Completing an audit of the software and devices you use is a great place to start. Think about what you need to protect and prioritise
- Consider assets you may already produce that could be included in your intelligence, for example, network logs. Are they sufficient to protect against all the threats you anticipate?
- You could already make changes to lower your cyber risk at this stage. Removing application access for staff or third parties who don't need it or downgrading their access using a "least privilege" model will provide instant benefits.
- Think about who might target your business and why. It's ok if your theories aren't correct, your results will help you to make any alterations necessary.

Skurio Risk Assessment Service

If you're not sure where to start - Skurio can help. Our experts will work with you to assess common threats your business could face. We'll also compile a footprint report based on our database of over 6 billion curated records. With this knowledge, you'll be able to decide the best way forward for your organisation.

Step two: Evaluate your resources

Prioritise based on risk. Being realistic is critical to having an effective cyber threat intelligence strategy. Your team can't hope to cover every base all the time. Focusing resources on the threats that are expected or the most disruptive makes sense.

Choose your tools wisely. Intelligence platforms designed for skilled experts could be hard to implement and use. Ask questions like: is there access to expert analyst advice? How quickly can we get started? Can we expand use cases as we get more confident?

Opting for a managed service could be the answer to resource issues. You'll still have to provide input on your risks, of course. But day-to-day management of your service or incident response won't be a worry.

Step three: Priority use cases

Roll up your sleeves!

Getting three fundamental use cases under your belt will help you quickly improve your security posture and demonstrate to your senior management team that you're taking cyber threats seriously. These use cases will help you protect the three most important aspects of your company's digital presence: your network, your staff and your customers. Your business is at its most vulnerable when an incident has already happened. Early identification of threats will allow you to mitigate them, prevent incidents and lower the chances of criminals targeting your business in the future.

Threats to infrastructure

Staff credentials exposure

Typosquatting

Threats to infrastructure

Your digital infrastructure is made up of many moving parts. Hardware or software vulnerabilities could impact your network, hosting, and wireless equipment. You may already have services set to detect these and patching procedures in place to fix them. But, this is not the whole picture. Further software vulnerabilities could affect the applications and databases you use - even digital assets like document templates could be used in scams if they fall into the wrong hands.

By monitoring for data linked to your infrastructure, you can detect potential attack planning, vulnerabilities or misuse that could lead to an attack. There is no shortage of online tools that can capture details of your public-facing infrastructure. Someone sharing those results online could indicate potential attack planning, however. New vulnerabilities are identified daily, so keeping up can be difficult. The trick is to tailor alert monitors to detect only vulnerabilities relevant to you.

Tailor your alerts

Restrict your searches to specific terms, including:

- Mentions of our infrastructure terms
- Individual IP addresses or ranges
- Domain names
- File names
- Database header details
- Equipment models

Select sources are best to monitor

- Dark Web | Chat Forums | Data Dumps | Social sources

Consider adding suitable risk identifiers, to ensure results are relevant:

- open port
- DDoS/DoS
- vuln/CVE
- bug
- ransomware terms
- known hacker gangs or individuals

Threats to infrastructure

Develop your intelligence

By tailoring your alert monitors, you'll be able to quickly identify which vulnerabilities need to be fixed. Your alert results could also provide evidence of attack reconnaissance or planning. Either way, you can respond swiftly to secure your infrastructure or investigate potential threats further.

Take action

- Initiate a proactive threat hunt where results identify bad actors
- Beef up defences in specific areas, for example, deploy a DDoS mitigation solution
- Patch / close ports etc.
- Request a post takedown
- Engage with a specialist threat intelligence service

Staff credentials exposure

The number of software applications used by businesses these days is startling. Managing access can be a headache, but your security team can't hold your business back by withholding it. Account takeovers can lead to compromised data and put your business operations at risk. Yet, they can be easily avoided, for the most part. Start with the basics. Enforce policies to limit access and privileges to those which are necessary. Introduce a password manager if you haven't already. And, use multi-factor authentication (MFA) where you can to make unauthorised access more difficult - should the worst happen.

Monitoring for data breaches on the surface, deep, and Dark Web makes total sense. The sooner you know about exposed credentials, the sooner you can notify users and prevent follow-on attacks. Using a Digital Risk Protection platform to provide a credential breach feed offers the benefit of early detection without leaving the footprint of manual searches.

Staff credentials may still be compromised even if they haven't been publicly exposed. Bad actors sometimes secretly share or sell data before posting a complete data dump. Monitoring for posts that mention the applications you use will also help you spot threats before credentials are exposed.

Tailor your alerts

Restrict your searches to specific terms, including:

- Individual email addresses
- Names of the applications that you use

Select sources are best to monitor

- Dark Web | Chat Forums | Data Dumps | Social sources

Consider adding suitable risk identifiers, to ensure results are relevant:

- fullz/deets/dox
- fresh/dump/breach etc.

Staff credentials exposure

Develop your intelligence

Tailoring threat intelligence isn't simply about filtering out the noise. What makes it valuable is that it is actionable. For example, a new post containing data from a historic breach that you have already processed is a 'false positive'. False positives are a distraction and an unnecessary drain on your resources. Use these steps to determine whether a credential breach is actionable:

- Quickly rule out duplicates - over 60% of credentials offered on market places are copies.
- Check the source of the data breach. Is it credible and reliable?
- Review associated meta-data. For example, how old is the file? How many sets of credentials does it contain?
- Are any of the breached credentials in use? Automating checks against current, valid email accounts can save precious time.
- Which software applications are at risk?
- Has other sensitive data been disclosed?

Take action

- Notify application users of credential breaches
- Enforce password resets
- Review your authorised application list and remind your staff they should only use approved vendors
- Anticipate and monitor for increased phishing activity
- Deploy multi-factor authentication (MFA) to further prevent unauthorised access
- Increase awareness training where necessary

Typosquatting

It may sound surprising, but trademark and copyright protection won't prevent fraudsters from creating websites that impersonate your brand.

Fraudsters use multiple methods to generate typosquatting variations of a domain. Basic techniques include removing, adding or substituting a character. More specialised tactics include registering a site with a different top-level domain (TLD) and replacing letters with lookalikes from international character sets. Any one of these approaches can produce a convincing URL that could deceive your staff or customers.

Criminals can register domains, obtain hosting, set up websites and configure mail services with alarming speed. They can also hide their details using data protection regulations and employ untraceable payment methods to prevent them from being caught. Typosquatting websites can be used to monetise traffic or divert it from your official channels, capture sensitive information from your customers, or distribute malware. Removing them can be complex, so early identification is vital.

SKURIO

Tailor your alerts

Restrict your searches to specific terms, including:

- Brands with existing domains - drmartens
- Product names - airwair

Select sources are best to monitor

- Domain Registration Feeds

Consider adding suitable risk identifiers, to ensure results are relevant:

- Similar words - airway

Typosquatting

Develop your intelligence

Non-malicious typosquatting domains can be quickly and easily ruled out using freely available online services. Suspicious domains typically fall into two categories: those that are already active and those that have been registered in preparation for a future scam. In any case, security teams should avoid visiting sites without investigating it first.

- Quickly rule out non-malicious sites using tools which provide an image of the website to highlight if it's impersonating your brand
- Update your alert monitor – if you've discovered a brand with a similar but non-competitive domain – add it to your list of exclusions
- Check registration details and discover if mail services have been configured for the domain using a reputable look up service

Take action

- Request a site takedown
- Monitor for DNS changes
- Monitor for mail service creation
- Notify customers of potential phishing threats
- Investigate bad actors and monitor their future activity

Step four: Extended use cases

Become a master tailor

Using Tailored Threat Intelligence, you can cover the basics incredibly easily and quickly. But, the size and complexity of your attack surface will depend on factors including your digital supply chain and even the behaviour of your senior executives. This section examines the ways Tailored Threat Intelligence can help you cover these critical risk aspects.

Threats to VIPs

Supply chain threats

Threats to your customers

Threats to VIPs

A rock-star CEO can be a valuable asset for a business, but they can also be a liability, as any Tesla investor will remind you! Even low-profile executives can be targeted if, for example, your business works in an unpopular industry or they can authorise financial transactions. Compromising any aspect of a senior executive's digital footprint can have serious consequences. Their accounts can be used as a vector to coerce staff to commit fraudulent acts or put company finances at risk. Little wonder there is a term specifically created to describe an attack of this kind - whale phishing. And, of course, they also have access to all types of sensitive documents and information.

VIPs can also be targeted through threats to their family or property. Bad actors will use open-source intelligence resources to gain as much background information as possible to improve their chances of success. But, you can keep one step ahead of them if you already know what's out there and have already taken steps to reduce risk.

Tailor your alerts

Restrict your searches to specific terms, including:

- Names / email addresses
- User account names
- Address / telephone details
- Banking information
- Family member names
- Company and brand names

  It's important to note that you can use partial details to recover sensitive breaches. Exposure of every element is rarely made. Combining partial information from multiple data types can often provide good results. For example, a surname, bank name, and last four credit card digits may produce better results than a complete card number.

Select sources are best to monitor

- Dark Web | Chat Forums | Data Dumps | Social sources

Consider adding suitable risk identifiers, to ensure results are relevant:

- Celebrities with similar names
- Trusted sources

Threats to VIPs

Develop your intelligence

Focusing on who is targeting a VIP and why can help you reduce risk, but you will almost certainly need your VIP's cooperation to do this.

- Investigate the source of the results - determine if hacktivists, trollers or known criminal organisations involved
- Consider if a breach or threat has implications across your supply chain
- Has sensitive data been publicly disclosed?

Take action

- Notify the VIP of any potential threats
- Enforce a password reset to prevent application compromise
- Monitor threat actor activity
- Notify stakeholders of potential reputational threats
- Advise third parties, such as banks, if accounts have been compromised
- Request a post takedown
- Notify authorities of illegal activities

Supply chain threats

These days, you can outsource almost every aspect of your operations - and many businesses do just that. One thing you cannot outsource, however, is your risk. Each new supplier could represent a potential risk to the data you have shared with them. If a supply-chain partner doesn't take cybersecurity seriously, they could provide a back door into your network or enable a successful phishing campaign. Your management team make decisions that impact your digital supply chain every day - you can help them by spotting weak links before it's too late. Adding a digital risk scan to your selection process is an easy way to stop a vulnerable supplier from being added and prevent your supply chain from unravelling.

Tailor your alerts

Restrict your searches to specific terms, including:

- Supplier/partner names and domains
- Third-party applications
- Internet of Things (IoT) / Smart devices

Select sources are best to monitor

- Dark Web | Chat Forums | Data Dumps | Social sources

Consider adding suitable risk identifiers, to ensure results are relevant:

- Document identifiers (for intellectual property protection)
- Model numbers
- Indicators of Compromise - CVE / zero-days / data breach

Exclude terms or names which could generate false-positive results:

- Companies or products with similar names
- Trusted sources

Supply chain threats

Develop your intelligence

Ransomware gangs, for example, rely on a steady stream of vulnerabilities and data breaches to provide new attack vectors and victims. Subscribing to a vulnerability news source (CVE data feed) could overwhelm your team with results that prevent them from identifying the severe threats.

- Review your suppliers in advance, and assess which ones are most critical to your operations
- Prioritise potential threats which are most likely to disrupt your business
- Investigate priority cases - consider the supply chain of the supplier that’s been compromised too

Take action

- Notify operations staff of potential threats or attacks in progress
- Lock down applications shared with partners
- Enforce a password reset to prevent application compromise
- Monitor threat actor activity
- Request a post takedown
- Notify authorities of illegal activities

Threats to your customers

However a ‘sophisticated cyber attack’ may start, it will often culminate in targeting your customers. Cyber-criminals use fine-tuned phishing and pharming campaigns to deceive your customers and capture their data.
This data has a market value, but details can also be used to scam customers out of their money.

This is one type of threat hunting where more search terms are better. Many data breaches include duplicates and data from historic breaches, so it isn’t possible to draw a conclusion on whether the data is yours from a single matched customer identity. Detecting and quantifying threats can be done effectively by comparing data sets at a macro level. Alternatively, you could use synthetic identities to seed a database and provide proof that a data dump originated from your business or supply chain.

Tailor your alerts

Restrict your searches to specific terms, including:

- Synthetic identity details
- Encrypted customer data sets

Select sources are best to monitor

- Dark Web | Chat Forums | Data Dumps | Social sources

Consider adding suitable risk identifiers, to ensure results are relevant:

- Database headers
- Company name
- Names of applications used to process data

Exclude terms or names which could generate false-positive results:

- Information from previous breaches that were not considered a threat

Threats to your customers

Develop your intelligence

Getting to the root cause of a customer data leak or threat can take skill and experience. If you don't have such resources in-house, it may be time to call in some help. Post-breach services are widely used and can provide distinct advantages over an internal team investigation. This is because a specialist team is likely to have seen similar attacks in the past, so they can efficiently identify methods and threat actors, and:

- Rule out duplicates
- Check the source of the data breach. Is it credible?
- Review associated meta-data. For example, how old is the file?
- How many sets of credentials does it contain?
- Identify if other sensitive data been disclosed

Take action

- Notify regulatory bodies and customers
- Advise customers to anticipate phishing attacks and update their passwords
- Monitor threat actor activity
- Request a post takedown
- Notify authorities of illegal activities

Step five: Plan for the future

Building a seamless capability

You might think that deploying a threat intelligence solution requires you to build a complete Security Operations Center (SOC). However, whilst a fully functioning SOC may be desirable in the longer term, it isn't necessary to get you started. Using a tailored threat intelligence solution as part of a Digital Risk Protection suite is a practical and affordable option. It will cover the basics, like data breach detection, and provide a valuable tailored threat intelligence feed with useful investigation features.

This combination of elements can provide the protection you need for your business without the need for hiring skilled, experienced cybersecurity staff. Onboarding is quick and straightforward, and in-app access to intelligence analysts gives help when you need it. Choosing a platform with an Application Programming Interface (API) capability will ensure you can smoothly combine other systems; when you're ready.

Skurio Digital Risk Protection - with Tailored Threat Intelligence

Skurio DRP combines surface, deep and Dark Web monitoring with data breach detection and tailored threat intelligence. If you're under pressure from your leadership team to deliver a response to growing threats in your industry, our teams are on standby to help you grow your threat intelligence capability. Contact us to see how we measure up - Skurio could be the perfect fit!

The perfect fit...

Digital Risk Protection combines the power of automated surface, deep and Dark Web monitoring with data breach detection and tailored threat intelligence. Data collection is automated, which means security teams can spend more time on processing and analysis. Collaboration and analytics tools help staff manage investigations efficiently.

Data from Dark Web and data dump sites, Pastebins, news, RSS and surface chat sites is harvested using automated scraping tools. This means security staff are not directly exposed to extreme content, contact with criminals is avoided and no search history is left behind that could identify them. Queried sources, including YouTube, VK, Twitter and Flickr, use secure API queries to bring data into the platform.

Flexible search terms are configured to monitor for any data you want protect, supporting a wide range of use cases.

Staff

Credential breaches
Account takeovers
VIP | Doxxing | PII
Payment cards

Infrastructure

IP address exposure
Attack planning detection
Supply chain compromise
Vulnerabilities

Customers

Customer data breach
Spam lists
Dark Web data sale
Account takeover

Brands

Typosquatting
Customer phishing
Impersonation
Activist targeting

Revenue & Margin

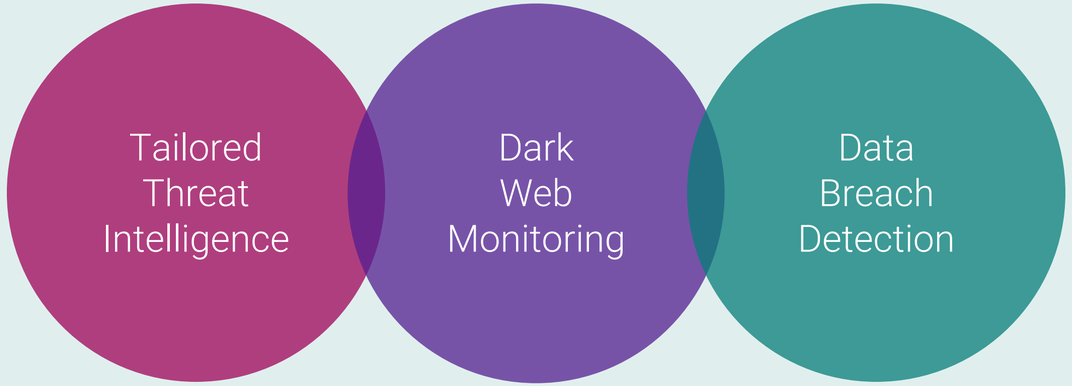
Discount abuse
Contract loopholes
Voucher abuse
Loyalty scheme breach

Products & Services

Critical data breach
Gift card sale
Source code leak
Loyalty scheme breach

SKURIO

Digital Risk Protection



Expand monitoring with queried sources, powerful filtering and analytics.

Automated surface, deep and Dark Web monitoring for compromised credentials, PII, intellectual property customer data breaches, threats and more : 24x7.

Get Instant alerts via text, email, Slack or Teams. Save messages, collaborate on investigations and track progress. Get in-app analyst help.