SKURIO CYBER THREAT INTELLIGENCE SERVICES GUIDE 2023

SKURIO

Guide to Cyber Threat Intelligence Services for MSPs

What is Cyber Threat Intelligence (CTI)?

CTI provides awareness of an organisation's threat environment so appropriate mitigation actions can be taken. Intelligence needs to perform three key functions:

1. Information relating to security threats needs to be obtained
2. This information must be processed (collated, evaluated, analysed, integrated, and interpreted) to form intelligence
3. Intelligence needs to be disseminated to those who need it

Organisations can use this information to prepare for, identify, prevent, and recover from cyber-attacks. Read our blog for more detailed information.

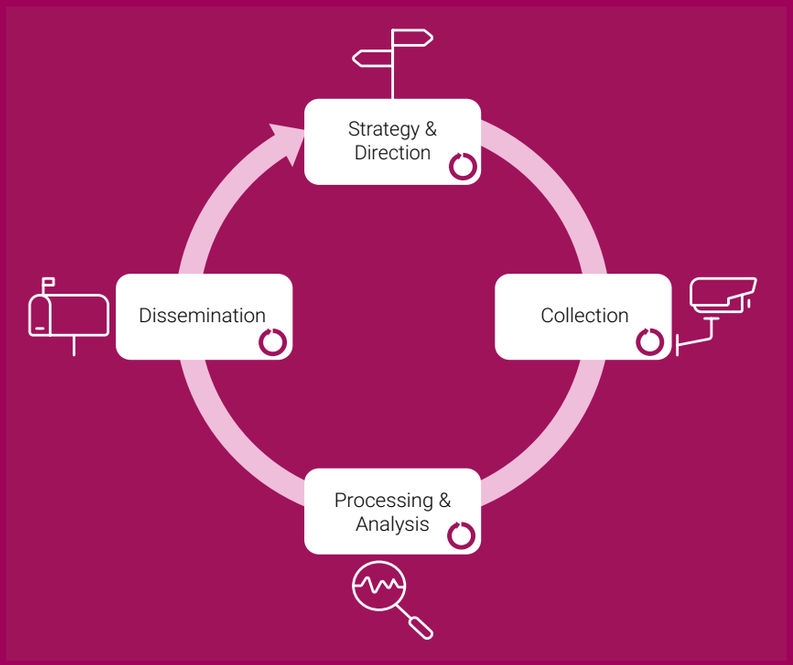
Who needs CTI

No matter how big or small, every organisation that uses a computer system (everyone!) can benefit from cyber threat intelligence – even if it's something simple like monitoring the Dark Web for compromised credentials or detecting typosquatting domains impersonating your brand. From top to bottom of the IT chain, the positive impact of cyber threat intelligence can be felt at every level.

The CTI Cycle

CTI systems automate the collection and processing of information to save analyst time. They can then spend most of their time analysing, reporting, and generating recommendations.

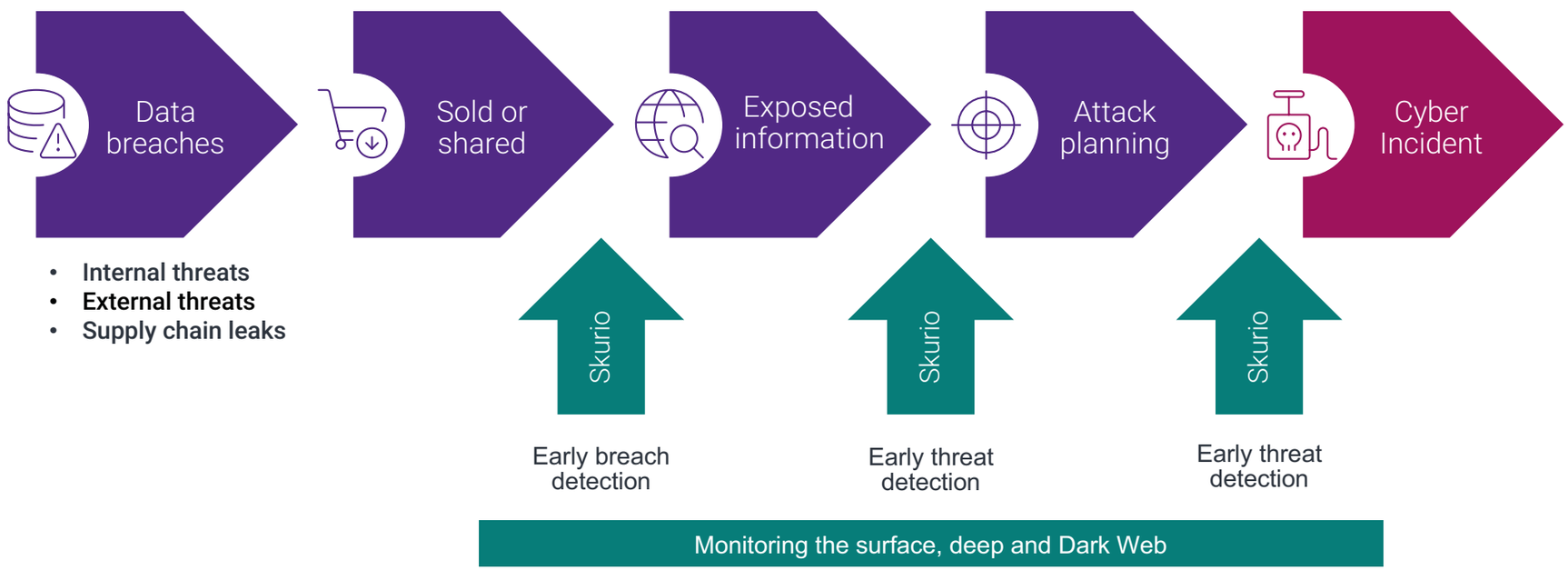
With the correct approach, CTI gathering should be a continuous cycle, with feedback loops at each stage to hone and inform your customers' CTI strategies.



Staying ahead of hackers

The problem CTI solves: early detection of cyber-attacks

Threat actors look for breached data and vulnerabilities to target your customer's business. No matter how comprehensive their current defences are, human error or a breach in one of their supply chain partners could put their company at risk. Skurio can monitor for this information on the surface, deep and Dark Web. By detecting exposed data and threats, you can act on behalf of your customers to prevent attacks.



Why should CTI be tailored?

Many IT and security leaders want to improve their security posture by implementing a CTI solution. However, the cost and the impact on resources often prove too much of a challenge. Every department and team requires something different from cyber threat intelligence.

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

Architects, admins and 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.

Traditional CTI platforms can meet all these demands but come at a hefty price and are generally used by large enterprises with deep pockets and copious resources. These solutions provide blanket coverage of vulnerabilities, potential threats, zero-days, and threat actors - all of which can leave your team swamped with interesting but irrelevant alerts. With Tailored CTI platforms like Skurio, your analysts only focus on information specific to your customers, so they don't waste time looking at irrelevant information.

CTI Use Cases

Threats can be detected using an automated CTI solution, which you can develop services to protect your customers.

Supply chain threats

If a supply chain partner doesn't take cybersecurity seriously, they could provide a back door into your customer's network or enable a successful phishing campaign. Adding a digital risk scan to their selection process is an easy way to stop a vulnerable supplier from being added and prevent their supply chain from becoming a threat or weak link.

Staff credentials exposure

The sooner you know about exposed credentials, the sooner your customer can notify their employees and prevent follow-on attacks, including account takeover. Providing a credential breach feed offers the benefit of early detection without leaving the footprint of manual searches. You can also reduce false positives and rule out duplicates.

Threats to infrastructure

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

Threats to customers

When a cyber-attack starts, it will often culminate in targeting your customer's customers. Cyber-criminals use phishing and pharming to deceive their customers. This captured data has a market value and can also be used to scam customers out of their money. If you know a customer has had a data breach, you can monitor large volumes of data that match theirs.

Threats to VIPs

Compromising any aspect of a customer's senior executive's digital footprint can have serious consequences. Their accounts can be used to coerce staff to commit fraudulent acts or put company finances at risk – this is whale phishing. VIPs can also be targeted through threats to their family or property. Monitoring multiple data sources minimises risk.

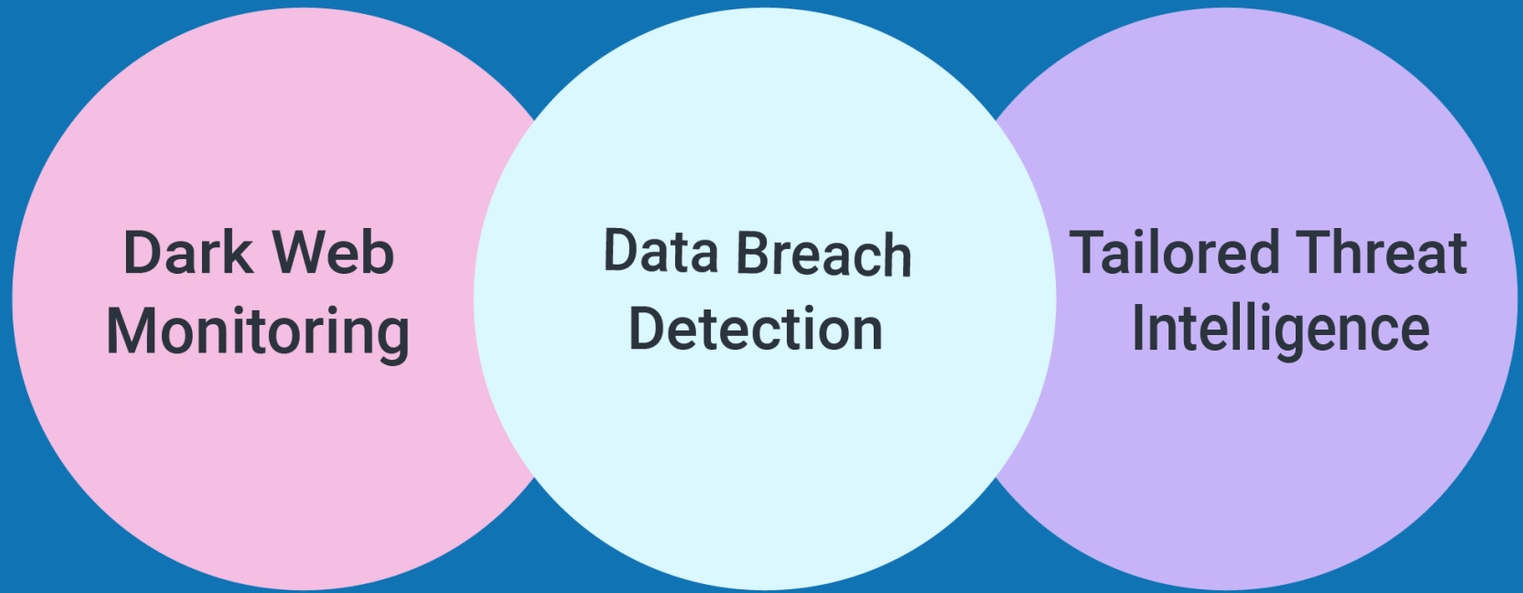
Typosquatting

Fraudsters use multiple methods to generate typosquatting variations of a domain. Basic techniques include removing, adding, or substituting a character. Any of these approaches can produce a convincing URL that could deceive your customer's staff or their customers. You can monitor newly registered 'spoof' domains to minimise the risk of phishing and fraud or even request a takedown.

What is Skurio Digital Risk Protection?

Cyber Threat Intelligence is just one of three solutions the Skurio Digital Risk Protection platform offers, along with Data Breach Detection and Dark Web Monitoring. You can use it to launch and deliver many services that include searching for information or threats found on the Dark Web. And our platform goes even further than that as we monitor many different sources on the surface and deep, as well as Dark Web, to protect organisations from cyber threats. When breaches and threats are detected sooner, remediation is faster, reducing the risk of further data breaches and cyberattacks.

The Skurio DRP platform combines Dark Web Monitoring, Data Breach Detection and Tailored Threat Intelligence



Advanced Managed DRP Service

The Advanced Managed DRP Service allows you to offer your customers the very highest levels of service features for your cyber threat intelligence service. However, you can, of course, tailor the service according to your customers' needs.

Service features include:

- Detect new credential leaks
- Prevent account takeover
- Detect and monitor newly registered 'spoof' domains
- Monitor your customer's infrastructure
- Discover attempts to use your customer's brand fraudulently
- Allow for early detection of threats to their VIPs
- Uncover breaches of critical data through supply chain leaks
- Find fingerprints of senstive corporate data

Advanced Managed DRP Service

Time to onboard
2-5 days

Management per month
8-16 hours

Managed services elements:
Monitoring for:

- Initial alert configuration
- Historical results reports
- Ongoing monitoring
- Monthly/quarterly reporting
- Incident responses & investigation
- Remediation and recommendations

Monitoring for:

- Corporate email domains
- Web & applications domains
- Typosquatting
- Public IPs

Brand and VIP

- Company
- Threat intel
- Partner logins
- High-risk account

Business critical information

- Sensitive data
- Fake/grey market
- Fraud

Data breach detection

- Databases
- Customer emails

Why partner with Skurio?

Skurio has been at the forefront of threat intelligence for 12 years, providing specialist tools for automated data monitoring across the surface, deep and Dark Web. The Skurio DRP platform helps MSPs to implement new services quickly and offers many advantages. You can:

- Respond to growing customer demand for CTI services
- Expand your services portfolio to enhance customer satisfaction and build trusted advisor status
- Deliver highly tailored CTI services to large enterprises and the public sector
- Create highly profitable new revenue streams from one-off project work or ongoing monthly monitoring services

The Skurio platform is easy to use and highly automated. It's operationally very efficient, and you don't need specialist resources to set it up.

Skurio MSSP packages are commercially attractive whether you have one customer or hundreds. You can start small, and you can pay-as-you-grow.

SKURIO

About Skurio

Skurio, the innovative cybersecurity SaaS company, helps MSPs to protect their customers from digital risks. Our Digital Risk Protection platform combines automated, round-the-clock surface, deep and Dark Web monitoring with powerful analytics capabilities for cyber threat intelligence. MSPs can use it to launch Managed DRP Services with various use cases.

Founded in 2011, Skurio is headquartered in the UK with an international partner network. Our partner and distribution network serves hundreds of customers in 33 countries.

Test drive the Skurio platform. See for yourself how easy it is to set up and use.

Click here to request your 2-week free trial

SKURIO LTD | ARTHUR HOUSE | 41 ARTHUR STREET | BELFAST | BT4 1GB +44 28 9082 6226

www.skurio.com partner@skurio.com