Cyber Threat Intelligence

NSB Cyber
No Steps Backward

Actionable cyber threat intelligence that strengthens organisational security. Our services are structured across Strategic, Tactical, and Operational levels, providing insights tailored to your needs - whether you're planning long-term, managing risks, or responding in real time.

Intelligence across every level of your defence

Strategic Intelligence

We help our clients by providing a foundation for understanding and preparing for threats.

Our services include:

- **Tracking the Cyber Threat Landscape**

We continuously observe, assess and report on the global cyber environment, pinpointing emerging threats, vulnerabilities, and exploits - such as advanced persistent threats (APTs), zero-day exploits, and changing techniques - that could impact your operations. This helps update security plans and responses to stay ahead of risks.

- **Monitoring Your External Presence and Attack Surface**

We oversee public-facing assets, including domains, websites, and online services, to detect vulnerabilities, misconfigurations, unauthorised changes, or signs of compromise that could lead to breaches or reputational harm. Using continuous scans and threat data, we prioritise risks, alert you to suspicious activity, and provide steps to address issues, helping you maintain control and reduce exposure as new risks emerge.

- **Supply Chain Risk Management**

We evaluate the security of your third-party vendors and partners, identifying risks from their systems, practices, or breaches that could affect you. This provides visibility into your supply chain's threat landscape and actionable steps to mitigate cascading vulnerabilities.

Operational Intelligence

We help our clients by providing focused insights to link planning with execution.

Our services include:

- **Threat Actor Profiling & Investigations**

We can deliver in-depth analysis of the cybercriminal ecosystem, including threat actors, tools, markets, and emerging trends. By examining tactics, behaviours, and motivations, we create comprehensive profiles to guide targeted investigations, enhance threat hunting, and strengthen defences.

- **Cyber Threat Actor Engagement**

We manage interactions with various threat actors - including ransomware engagement and negotiation, as well as other attacker types - through channels like the dark web and beyond, both during incidents and proactively. This enhances investigations, mitigates risks, and collects intelligence to inform your broader security operations.

Our Cyber Threat Actor (CTA) Engagement services are backed by our deep expertise in Cyber Threat Intelligence and Cyber Incident Response. Download our **NSB CTA Framework** for more information.

Tactical Intelligence

We help our clients by providing real-time tools and resources to support your team's daily security operations.

Our services include:

▸ Supplying Real-Time Threat Data

We deliver current indicators of compromise (IOCs), malware signatures, and live threat intelligence feeds, tailored to your environment. This equips your team to detect, block, and adapt to attacks as they emerge.

▸ Retained CTI Analyst (Virtual Resource)

We provide a virtual cyber threat intelligence (CTI) resource to enhance your team's capabilities. Acting as an instantly available resource, we analyse threats and deliver expert insights, augmenting your in-house operations without adding headcount.

▸ Deep and Dark Web Monitoring

We scan the deep and dark web – either as a one-time assessment or ongoing monitoring - to uncover vulnerabilities, exposures, or compromised data tied to your domains, assets, or accounts. This delivers a prioritised view of risks with guidance to reinforce your defences against exploitation.

CredWatch - Basic Credential Monitoring for Small Businesses

We help our clients by providing a simple, targeted service to protect small businesses from credential-based threats. With **CredWatch**, we monitor the dark web and known breach sources for exposed credentials - usernames, passwords, or account details - linked to your business's domains or employee emails. When a match is detected, we send clear, actionable alerts along with basic instructions to secure your accounts.

▸ How It Works

We use automated scans to check leak databases and dark web forums, tailored to your provided domains or email patterns. Alerts arrive via email - no technical expertise required.

▸ Why It Matters

This helps you catch credential leaks early, reducing the risk of account takeovers or phishing attacks, all at a scale and cost that fits small business needs.

Designed for teams without dedicated security staff, **CredWatch Essentials** keeps your business safe without complexity or overhead. It's a set-it-and-forget-it solution that delivers peace of mind, letting you focus on running your business. You'll stay ahead of threats without needing to hire experts or manage complicated tools.

To stay up-to-date with cyber threats, risks and developments, signup to **NSB Signals** via the **website** or via **LinkedIn**.

To find out about Adversarial Action Advisory and Vulnerability Exposure Advisory alerts, head to our **website**.

For more information, contact us via email on info@nsbcyber.com or visit www.nsbcyber.com

Cyber Threat Actor (CTA) Engagement

NSB Cyber
No Steps Backward

Our Cyber Threat Actor Engagement Framework (CTAEF) allows organisations that have suffered a cyber-attack to engage with the Cyber Threat Actors responsible for the attack, in a structured and planned manner as part of overall incident response activities.

Engaging with a Threat Actor is not a commitment to pay or a concession to their demands.

Engaging with a Threat Actor allows a victim organisation immediate access to potentially new information provided directly from the adversary responsible, that can then be considered as part of the overall incident response and recovery decision making process.

Based on NSB Cyber's experience in CTA Engagement assignments, we are able to uncover information such as how the threat actor claims to have successfully conducted the attack, what their attack process has been, what information they have taken, who they claim to be, what they are demanding and why they are demanding it.

Assessing this information carefully allows a victim organisation to make fully informed decisions when executing their response and recovery strategy. It also allows access to fulsome information to conduct a Cyber Threat Actor Attribution assessment, such that subsequent consideration of any relevant sanctions or negotiation outcomes can be considered.

Our CTAEF phased approach establishes a controlled and informed response strategy, leveraging intelligence and tactical insights to guide decision-making. This includes assessing the credibility and intention of the Threat Actor, evaluating the risks, and the potential impact of various response strategies.

The What

The immediate recognition of the specific characteristics and behaviours of an Advanced Persistent Threat (**APT**) or Ransomware Attack within a network or system.

The How

By integrating an NSB Cyber specialist into the Incident or IT Environment, the goal here is to identify and attribute the Incident as quickly as possible to limit the damage.

BACKGROUND OF THREAT ACTOR

A brief background and specific characteristics of the Threat Actor, including previous attacks, affiliations with known groups, Threat Actor origins, skill level, and possible locations.

INSIGHTS & MOTIVATION

The motivations driving the Threat Actor, which may range from financial gain to ideological reasons or even state-sponsored activities. This can provide insights into their potential actions and willingness to negotiate or escalate the attack.

VICTIMOLOGY

Examine the Threat Actor choice of victims to identify any patterns in their selection process. This could include industry preferences, company sizes, geographic locations that make certain organisations more likely targets.

TACTICS, TECHNIQUES & PROCEDURES (TTPs)

The specific methods the Threat Actor uses to execute attacks. This includes their technical capabilities, such as malware deployment, exploitation of vulnerabilities, and methods of communication with victims. Understanding these can help in predicting and defending against their attacks.

We help our clients with the following services:

Attribution

Threat Actor and Attack Tradecraft Analysis

With the rapidly evolving cyber threat landscape and increased focus on Australia as a viable target for cyber-crime, conducting a high-priority analysis of Threat Actor Attribution and Attack Tradecraft as part of incident response activities is imperative. These insights are critical not only for comprehending the full extent of the attack, but also for crafting a targeted and effective Threat Actor engagement strategy.

The NSB Cyber Response & Recovery team conduct this analysis as part of all CTA Engagement assignments, working alongside in-place incident response and recovery teams with information they have already uncovered through their investigations, or by deploying our own technical DFIR team to assist with the required activities.

The objective of our analysis is to identify with the highest degree of confidence as possible, the threat actor behind the attack, their affiliations, their Techniques, Tactics and Procedures (TTPs) and Indicators of Compromise (IOCs). Our attribution service leverages the NSB Cyber Intelligence Centre and our extensive database of on-incident intelligence.

This analysis is crucial not only for grasping the full scope and impact of the incident, but also for identifying the underlying vulnerabilities and tactics used by attackers. Understanding these elements is key to performing meaningful due diligence on the Threat Actor, including as part of sanctions checks, and also for developing the most effective and nuanced Threat Actor communications strategy, including planning for the most appropriate exit.

Communications

End-to-End Threat Actor Interactions