Strategic Threat Intelligence Overview

Contents

The Value of Threat Intelligence

"Threat Intelligence is actionable knowledge and insight on adversaries and their malicious activities; enabling defenders and their organisation to reduce harm through better security decision making"

Organisations of all shapes and sizes are increasingly becoming targets for miscreants and while attacks are generally more sophisticated, even the trivial ones can have a serious impact on the bottom line.

Building an impenetrable perimeter is no longer a viable strategy and instead resilience based on a mature governance and risk strategy is the way forward. Each organisation's strategy will be unique, but one thing that remains constant is the need for threat intelligence to inform it.

Gaining value from threat intelligence

For threat intelligence to have a business value to your organisation it needs to be useable, and this will depend upon the seniority of the audience consuming it, as well as the specificity of the threat intelligence in question.

The lack of a robust governance, risk management or cyber resilience strategy, or ones that do not integrate threat intelligence appropriately will likely result in you being unable to action it effectively. Consuming threat intelligence for the sake of consumption, without being able to contextualise it will result in you gaining little, if anything.

Appropriate use of threat intelligence allows you to make risk-based decisions that inform future budgets and where to focus your security efforts. Over time it is likely that threat intelligence will go beyond being just an enabler, to become something that yields an increasingly competitive advantage.

What we cover

- The value of threat intelligence and the key benefits it's use can bring to your organisation.
- The goals of a Cyber Threat Intelligence (CTI) programme and the characteristics of a successful one.
- NCC Group's Strategic Threat Intelligence service offerings and how they help support the CTI programme you need.

Closing thoughts

Threat intelligence can be an invaluable tool for mature and maturing organisations alike. However, in order to derive this value you must be able to consume, interpret and respond effectively.

NCC Group's Strategic Threat Intelligence Services are at the forefront of the market, we provide services that build confidence in, and support the development of your current capabilities, along with providing information on the threats you face not only today but also tomorrow.

Key benefits

- Assess organisation exposure - gain insights into the threats and associated risks faced by your organisation and the sector within which you operate.
- Threat landscape overview - the tools and techniques being used by malicious actors, as well as information regarding the systems they are actively targeting. Our horizon understanding and thought leadership can be drawn upon to have a greater awareness of future threats and issues your organisation is likely to face, giving you time to prepare well in advance.
- Understand threat actors perspective - what threat actors see when they look at your online presence. In turn, this will allow you to mitigate any immediate risks with regards to exposed services, and information leakage; the types of information that could provide valuable information to malicious parties.
- Identification of past breaches - identify if your corporate account information has appeared in breach datasets, and is therefore potentially usable by malicious actors to log in to your corporate environment.
- Reduce risk of fraud and theft - by uncovering details of stolen information, commoditised access to your environment, or personally identifiable customer and employee information being exposed online.
- Brand protection - by identifying fake websites or insecure social media profiles.

Your Cyber Threat Intelligence Programme

Today, preparing for and predicting potential attacks against your organisation are two of the most important roles that can be played by your security function. Developing and understanding who is likely to target your organisation, what will be targeted, and what the attack will look like, are all vital questions that need to be answered.

An organisation that has an understanding of these things, can have a significant positive impact on its ability to prevent, detect and then respond to any attacks. Only through threat intelligence can you fully understand the risks that cyber adversaries (both accidental and malicious) pose.

What

What are they looking to target?

Who

Who is likely to target the organisation?

How

How is the attack likely to happen?

Why

Why are they attacking you or likely to target you in the future?

When

When is the organization going to be targeted?

Where

Where is the attack likely to come from and where will it impact?

You should ideally build a Cyber Threat Intelligence (CTI) programme that allows them to take a methodical, structured approach to conducting intelligence activities that match the organisation's needs.

This includes the types of intelligence required, and the frequency of these outputs.

Strategic

High-level overviews of a threat's impact and value, measurable security metrics, and annual intelligence summary reports.

Operational

Intelligence reports, alerts and briefings, and technical reports with a course of action.

Tactical

Specific indicators of compromise: hashes, IP addresses, command and control infrastructure, signatures, file names, email addresses.

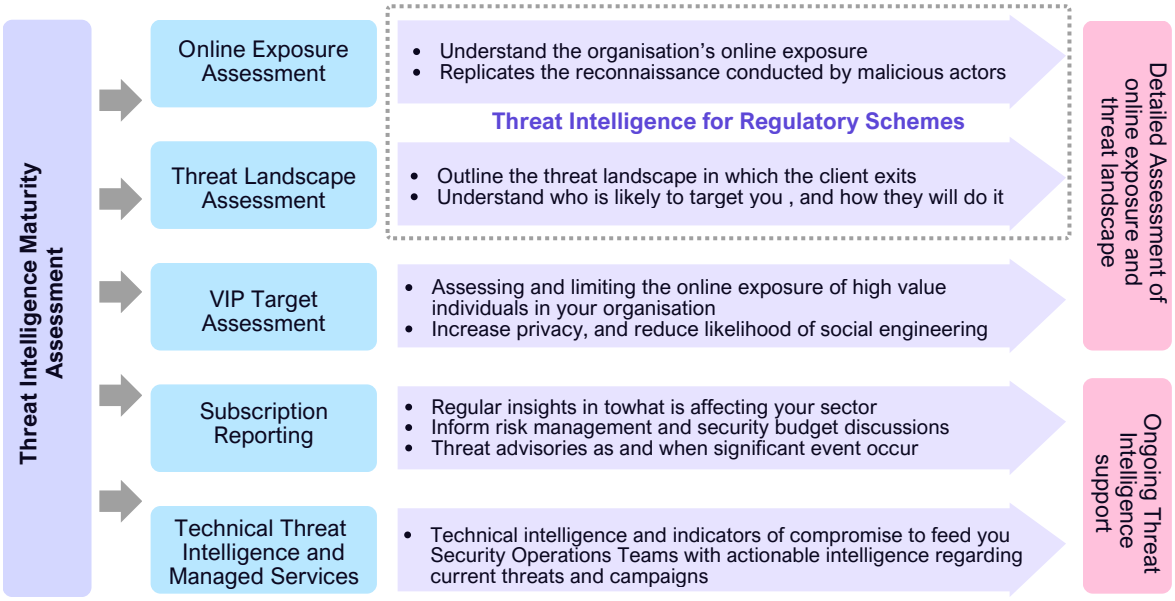
Your CTI programme should be made up of adequately skilled individuals who are guided by well-designed, repeatable processes that make effective use of applicable technologies to undertake continuous and effective analysis. These individuals and processes need to work to ensure that your organisation's threat intelligence is:

- Centralised – Centralised controls allow for efficient allocation of resources and a primary point of contact
- Responsive – Intelligence should be responsive to consumers, with clearly defined reporting lines
- Objective – Analysts should remain impassive with assessments, which should be made independently from the policy process
- Systematic – Source, data and information should be methodically exploited in a coherent and coordinated fashion
- Sharing – Intelligence should be shared according to protective markings, while protecting sources, when required
- Continuous review – Assessments should be continually tested against new information, while feedback should spread throughout the cycle
- Accessible – Intelligence products should be designed and delivered with its intended audience in mind
- Timely – Intelligence is useless if delivered too late. Less than perfect outputs delivered on time are preferable to outdated material

Our Strategic Threat Intelligence service forms part of our wider Threat Intelligence offerings, and focuses on consultant-led activities which allow you to understand the threat landscape in which your organisation operates, review the maturity of your Cyber Threat Intelligence function, and provide threat intelligence for regulatory driven exercises such as CBEST and TIBER.

The work undertaken for you as part of this service can be a single 'snapshot-in-time' to help you inform current risk management decisions, or can be delivered over extended periods to provide you with regular insights in to the threats posed to your organisation.

Threat Intelligence Services



Threat Intelligence Maturity Assessment

Many organisations do not know how effective their CTI programme is in practice. One of the best ways to help determine the effectiveness of your programme is to measure the level of maturity of your programme in terms of:

- Governance
- Programme Planning
- TI Operations
- Function Management

Our cyber threat intelligence maturity assessment will help you develop a robust threat intelligence function to keep you informed of the latest threats, allowing you to prepare for things that are more likely to impact your organisation.

We will assist you in identifying your CTI requirements, and provide a benchmark score to work towards in each of the above areas. We will advise on how to fill any gaps in your capabilities, thus improving your maturity, something you can monitor over time to show where improvements are made.

Online Exposure Assessment

We have a number of threat intelligence solutions including a focused engagement designed to mimic the preparations of a skilled threat actor preparing for a concerted attack.

Using a variety of OSINT sources and research techniques, we produce a synopsis of the most significant, publicly available information which is available about your organisation, which would facilitate an attack by a malicious threat actor.

This includes information about your people, processes and technologies.

OSINT research can also be bespoke to specific intelligence requirements such as; identifying evidence of your organisation's PII being sold on the dark web, specific OSINT on a certain product or software solution, in support of Mergers and Acquisitions, in support of Incident Response work, etc.

Threat Landscape Assessment

These assessments outline the threat landscape in which the client exits. They bring together information about the attackers that are likely to impact you. This includes details regarding their Tactics, Techniques, Procedures (TTP), along with current activities and their capability to deliver an attack.

NCC Group has a global client base that operate across multiple sectors, and it is through engagement with these clients (whether this is security infrastructure development, network monitoring, malware analysis, incident response, or any of the other services NCC Group offers) we have a thorough understanding of what the current threats are, and how they are being manifested.

These assessments can be combined with a Targeted Threat Intelligence report to provide more holistic analysis of the most likely threats, unsurprisingly we create greater value when working in a collaborative manner with yourselves.

Threat Intelligence Services

Threat Intel for Regulatory Assessments (CBEST, GBEST iCAST, TIBER-EU & CORIE):

NCC Group can deliver the entire Full Spectrum Attack Simulation package of services in a manner that meets both UK and international regulatory requirements. These engagements typically involve an extensive preparation phase where we will evaluate your requirements, agree an appropriate scope and a communication plan to ensure you are able to action all the subsequent remediation advice

VIP Target Assessment

Much like targeted threat intelligence, but focussing on an individual rather than an organisation. We identify what information is available that is being exposed by key individuals within your organisation to potential attackers, and how they are likely to use this information to facilitate an attack.

This knowledge forms a significant part of a company's threat profile and will allow the client to invest in the appropriate security controls to reduce or remove the threats.

We will provide a detailed assessment that will provide the following key benefits:

- An understanding of the information which is available to a hostile threat actor seeking to target certain individuals
- An outline of how and why threat actors collect such information, and how it can be subsequently used to facilitate an attack
- Advice on how to maximise online privacy

Subscription Reporting

NCC Group can provide you with sector-specific Strategic Threat Intelligence reports on a quarterly basis. These reports will help your organisation stay informed on the latest evolutions in the threat landscape within the sector your organisation operates, as well as providing strategic insight regarding the activities of various threat groups. These reports will provide high level summaries of recent attacks, exploits and campaigns by threat actors.

As part of this subscription service, you will also receive ad-hoc threat advisories when we become aware of issues that are likely to impact you. These advisories will provide you with an overview of the threat, technical information and Indicators of Compromise (IoC's), and other mitigation advice

Technical Threat Intelligence and Managed Services

NCC Group's Technical Threat Intelligence team conduct regular threat hunts and research in to the latest activities of threat actors, mapping their activities and developing curated threat intelligence feeds that can then be ingested by your monitoring and detection platforms and Security Operations Centres.

These feeds can be provided in their raw format, or with added context and details regarding our research via our InTell platform.

Who should take this course?

NCC Group's Azure security review training is a focused course for security consultants and cloud architects interested in learning how to assess the main elements of a cloud environment based in Azure. We will cover the techniques and tools necessary to perform a thorough security review and provide an understanding of the major risks, along with the best security practices that should be considered when designing a cloud infrastructure.

Requirements

Participants are expected to have some familiarity with the PowerShell command line and basic IP networking knowledge.

Students should bring a laptop with an SSH client installed. The laptop should not have any corporate security software which restricts Internet access or forces use of a corporate proxy server for browsing.

Recommended setups are: PowerShell installed on Linux, MacOS or Windows.

Deliverables

PDF presentation of over 250 slides covering all modules of the training course.

About NCC Group

NCC Group is a full-spectrum cyber security specialist delivering the expertise and solutions to research and mitigate threats and vulnerabilities and secure citizen services from initial design right through to day-to-day operation.

In the UK, the nation's digital infrastructure and public services are now central to how citizens live, work, learn and play. They are also core to the UK's national security and international success. Which is why we've made it our mission to create a safer, more resilient United Kingdom.

NCC Group partners with public sector organisations to help develop resilient digital solutions where security is an enabler, not a barrier.

We'll help you turn your strategy into real-world services that balance high-trust, proven security measures with intuitive ease of use for citizens. We'll support you with world-class experts who will test and refine your security, systems and infrastructure against both existing and emerging threats.

Ultimately, we provide continuous assurance that the systems, services and infrastructure the country relies upon, are resilient in the face of today's sophisticated cyber security threats. Whether it's national security programmes, digital transformation initiatives or the delivery of local services, we help secure the UK's citizens in the digital world.

NCC Group's Unmatched Capabilities in Public Sector Protection

NCC Group has a number of distinct advantages in the public sector market.

We understand public sector objectives and the challenges in accomplishing them — so we can tailor our solutions to help customers make tangible real-world progress towards their most important outcomes.

We have both depth and breadth of technical capability — from managed detection and response to threat intelligence and cloud services, we NCC Group has a number of distinct advantages in the public sector market.

We understand public sector objectives and the challenges in accomplishing them — so we can tailor our solutions to help customers make tangible real-world progress towards their most important outcomes.

We have both depth and breadth of technical capability — from managed detection and response to threat intelligence and cloud services, we

For more information from NCC Group on our G-Cloud 15 service, please contact:

+44 (0)161 209 5200

bidteam@nccgroup.com