Greater Manchester | Greater Security | Greater Business

Cyber Foundry

Leveraging Threat Intelligence Services

An Insight into Cyber Security for SMEs

Audience: General **Reading Time: 5 Mins**

In an era dominated by digital transformation, small and medium-sized enterprises (SMEs) are facing an escalating number of cyber threats. Whether it is safeguarding your customers' data or ensuring the integrity of your internal systems, the significance of cyber security cannot be understated.

In the fight against cybercrime Threat Intelligence services are a key tool which SMEs can leverage to their advantage. Threat intelligence in cybersecurity refers to knowledge about potential or existing cybersecurity threats that can harm a system. It involves understanding the tactics, techniques, and procedures (TTPs) of cybercriminals, the security vulnerabilities they exploit, and the ways in which they penetrate systems.

Understanding Threat Intelligence Services

Threat Intelligence Services, at their core, are akin to a sophisticated weather forecast for the cyber realm. Just as meteorologists interpret environmental data to predict future weather conditions, Threat Intelligence Services analyse data from multiple sources to predict, detect, and mitigate cyber threats. This data can include details about threat actors, their methodologies, the tools they use, and their potential targets.

In practical terms, Threat Intelligence Services involve the collection, analysis, and dissemination of information about existing and emerging threat trends. The information collected can be from a range of sources, including open-source intelligence (OSINT), social media intelligence (SOCMINT), human intelligence (HUMINT), and technical intelligence or telemetry data.

The Value of Threat Intelligence Services

In a world where cyber threats evolve continuously, the ability to proactively identify potential risks is invaluable for any organisation, including SMEs. Threat Intelligence Services offer several key

European Union
European Regional Development Fund
The Cyber Foundry project is part funded by the European Regional Development Fund
Lancaster University
MANCHESTER 1824 The University of Manchester
Manchester Metropolitan University
University of Salford MANCHESTER

potential advantages:

Proactive Security: Threat intelligence can predict potential risks, providing an opportunity for an organisation to strengthen their security before an attack occurs. For instance, say a particular type of ransomware is spreading rapidly across the healthcare industry. Threat intelligence could flag this trend and recommend steps to fortify defences, such as patching software vulnerabilities that the ransomware is known to exploit. This enables healthcare SMEs to be prepared and possibly avoid a costly disruption.

Perhaps your business operates an online store. A proactive Threat Intelligence Service might identify that a new type of malware, which specifically targets e-commerce platforms like yours, is spreading. Having this early warning allows you to tighten your security measures, update your software, and warn your IT team about this emerging threat, possibly preventing an attack that could have crippled your operations.

Instead of waiting for an attack to occur and then reacting, Threat Intelligence Services enable businesses to predict and prepare for threats. This proactive approach can help to reduce the impact of a cyber-attack, or even prevent it entirely.

Prioritised Defence Strategy: With the wide array of potential threats, it can be challenging for SMEs to decide where to focus their security resources. Threat intelligence offers a solution by ranking threats based on their likelihood and potential impact. For example, a threat intelligence service might identify that your industry is experiencing a slight increase in spear-phishing attacks targeting C-level executives. With this insight, you can prioritise security awareness training for these high-risk individuals in your organisation.

Another scenario might be that your Threat Intelligence Service alerts you to two potential threats: one is a large-scale botnet attack targeted at businesses in your sector, the other is a less common phishing scheme. By analysing the specifics of these threats, their prevalence, and their potential impact, your Threat Intelligence Service could determine that the botnet attack poses a higher risk to your business. With this insight, you can focus your resources on shoring up your defences against this botnet, ensuring that your most significant vulnerabilities are addressed first.

Threat Intelligence Services not only identify potential threats, but they also rank them based on their severity and potential impact on your business. This allows you to prioritise your defence strategy and allocate resources where they are most needed.

Having this early warning allows you to tighten your security measures, update your software, and warn your IT team about this emerging threat

Enhanced Incident Response: When an incident occurs, time is of the essence. Threat intelligence helps speed up the response by providing detailed information about the threat. For instance, if a banking SME suffers an attack from a known hacking group, threat intelligence could provide information about that group's typical methods and targets. This could range from the malware they use to their preferred modes of data exfiltration. With this knowledge, the incident response team can quickly mitigate the attack, minimising its impact.

When a cyber-attack does occur, having detailed information about the threat can significantly reduce response times. Threat Intelligence Services can provide this

information, enabling your team to respond effectively and limit damage.

Regulatory Compliance: Many sectors, especially those handling sensitive data, are subject to strict regulations that require proactive risk management. For example, General Data Protection Regulation (GDPR) imposes significant penalties for data breaches. Threat intelligence can aid in compliance by identifying the methods most used to breach data in a specific sector. With this information, SMEs can bolster their defences in these areas, helping to prevent breaches and maintain regulatory compliance, saving you from hefty fines, not to mention the reputational damage of a regulatory breach.

Many industries now require businesses to demonstrate that they are taking proactive steps to manage cyber security risks.

Employing Threat Intelligence Services can help your business meet these requirements.

Competitive Advantage: Cybersecurity can be a selling point for potential customers or partners. For example, where an e-commerce SME uses threat intelligence to monitor for threats to its payment systems, it can use this fact in its marketing materials. Customers concerned about data security may be more likely to choose this SME over a competitor that does not publicise its cybersecurity measures. Equally, consider sectors where customer trust is paramount, like healthcare or finance. By using a Threat Intelligence Service, you could keep abreast of the latest threats and maintain a robust defence system, which you could then advertise to potential customers. This could give you an edge over competitors who might not take cyber security as seriously. If a major cyber-attack hits your industry but your business remains unaffected, that is a powerful testament to your security measures that could attract new customers.

A strong security posture can give your business a competitive edge, particularly if you handle sensitive customer data. It can enhance your reputation, build trust with customers, and potentially lead to new business opportunities.

Wrapping it Up

In the complex and ever-evolving landscape of cyber threats, Threat Intelligence Services provide an essential tool for SMEs. By enabling a proactive and informed approach to security and providing actionable insights about potential threats, these services can help businesses to remain one step ahead of cybercriminals, protecting both their own operations and the data of their customers.
Remember, threat intelligence is about staying ahead of potential threats, so regular learning and staying updated with the latest in cybersecurity news is key.

There are many resources where you can learn more about threat intelligence. Here are a few places where you might start your search for more information.

Cybersecurity blogs, cybersecurity journals and news sites, threat intelligence platforms (TIPs), security reports and whitepapers, government and non-profit resources such as the NCSC.