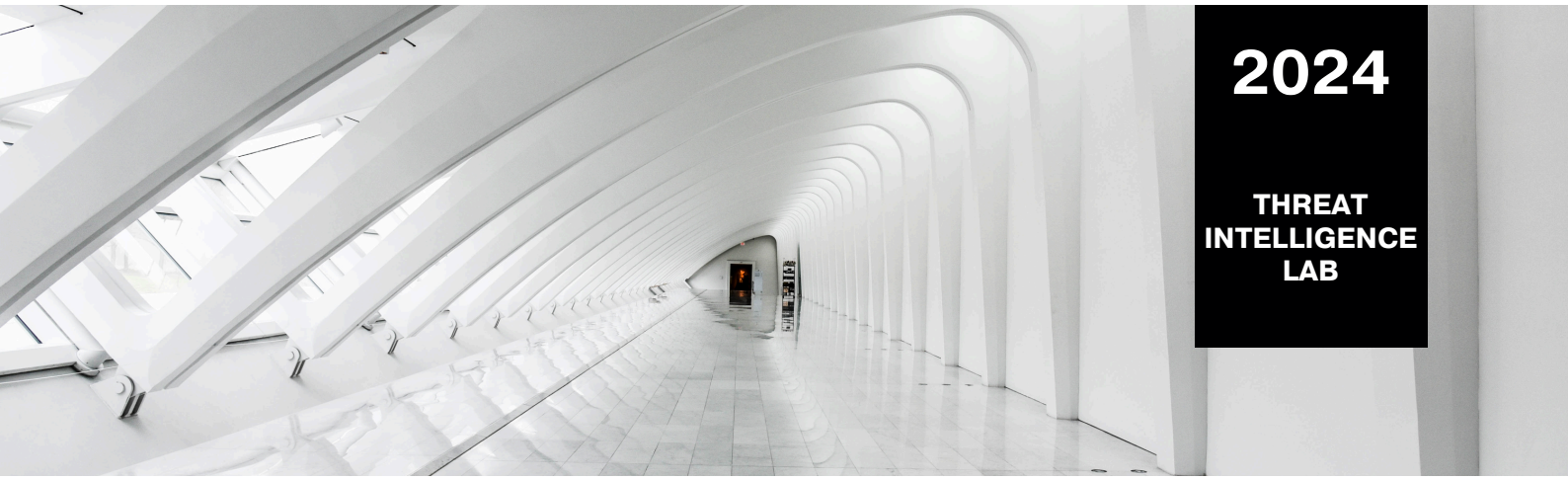


2024

THREAT INTELLIGENCE LAB

BRIEFING

Who works with Cyber Threat Intelligence (CTI) ?

Author
Reza Rafati

Classification
PUBLIC

ABOUT

THREAT INTELLIGENCE LAB

Threat Intelligence Lab focuses on empowering companies to enhance their Cyber Threat Intelligence (CTI) capabilities.

Our team, with over 100 years of combined experience, has developed detection systems, created and maintained cyber threat intelligence feeds, and conducted extensive automated (static and dynamic) malware analysis at scale.

Our expertise extends to incident response, domain takedowns, and reverse engineering.

We offer a service that provides critical knowledge, enabling companies to make informed decisions without selling products.

Our wide range of partners, allows us to offer tailored assistance. We are always open to discussions to explore how we can be of service.

Founded in 2024 by Reza Rafati, our company aims to bridge the gap between technical experts and decision-makers, ensuring effective collaboration and informed decision-making. We are supported by the Threat Intelligence Lab advisory board, ensuring we stay at the forefront of the industry.

.

What is Cyber Threat Intelligence?

Cyber Threat Intelligence (CTI) is the practice of collecting, analyzing, and leveraging information about current and potential cyber threats targeting an organization's digital infrastructure. This intelligence provides actionable insights that help organizations understand threat actors, their tactics, techniques, and procedures (TTPs), and the vulnerabilities they exploit. It helps organisations to prepare and defend against cyber-attacks, reducing risks and enhancing their overall cybersecurity posture.

Who Works with Cyber Threat Intelligence?

Cyber Threat Intelligence (CTI) involves various professionals with specialized roles. They work together to protect organizations from cyber threats. Let’s dive into who these professionals are, who they enable, and the skills they need.

- **How to Conduct an Effective Cyber Threat Intelligence Stand-Up Meeting**
- **The Most Common Cybersecurity Interview Questions and Answers**
- **CTI Job Interview Questions – Part 3**
- **CTI Job Interview Questions – Part 2**
- **Becoming a Cyber Threat Intelligence Analyst (2024)**

Cyber Threat Analysts

Cyber threat analysts are at the forefront of CTI. They gather, analyze, and interpret threat data. Their primary job is to identify potential threats and provide actionable intelligence. They play a crucial role in keeping the organization safe by staying ahead of cybercriminals. Cyber thrat analysts enable several key teams within an organization. Incident response teams rely on them for crucial information that helps in responding to incidents swiftly. The Security Operations Center (SOC) benefits from the insights provided by analysts to monitor and defend against threats. IT security teams also depend on the analysts to stay informed about emerging threats and vulnerabilities.

To excel in this role, cyber threat analysts need a mix of technical and non-technical skills. Technically, they must be adept at data analysis, interpreting large volumes of data to identify patterns and anomalies. Understanding attackers' tactics, techniques, and procedures (TTPs) is crucial. They must also be proficient in using Security Information and Event Management (SIEM) tools. Beyond technical skills, critical thinking is essential for making informed decisions based on data. Excellent written and verbal communication skills are needed to convey findings clearly. Lastly, a keen eye for detail helps spot subtle indicators of compromise.

Incident Responders

Incident responders act on the intelligence provided by threat analysts. When an attack happens, they handle and mitigate security incidents, aiming to minimize damage and recover systems quickly. They play a vital role in the organization's defense strategy. Incident responders enable several groups within the organization. They keep executive management informed by providing detailed reports and updates during incidents. Legal teams benefit from their documentation of incidents for compliance and potential litigation purposes. Public relations teams rely on incident responders to manage communication during and after incidents to protect the organization's reputation.

To be effective, incident responders need a combination of technical and non-technical skills. They should have expertise in digital forensics to investigate breaches thoroughly. A strong understanding of network security principles is also necessary. Additionally, the ability to analyze and understand malware behavior is crucial. Non-technical skills are equally important. Incident responders must have quick and effective problem-solving abilities. They need to manage stress well, staying calm and focused under pressure. Strong collaboration skills are essential to work effectively with various teams.

Security Engineers

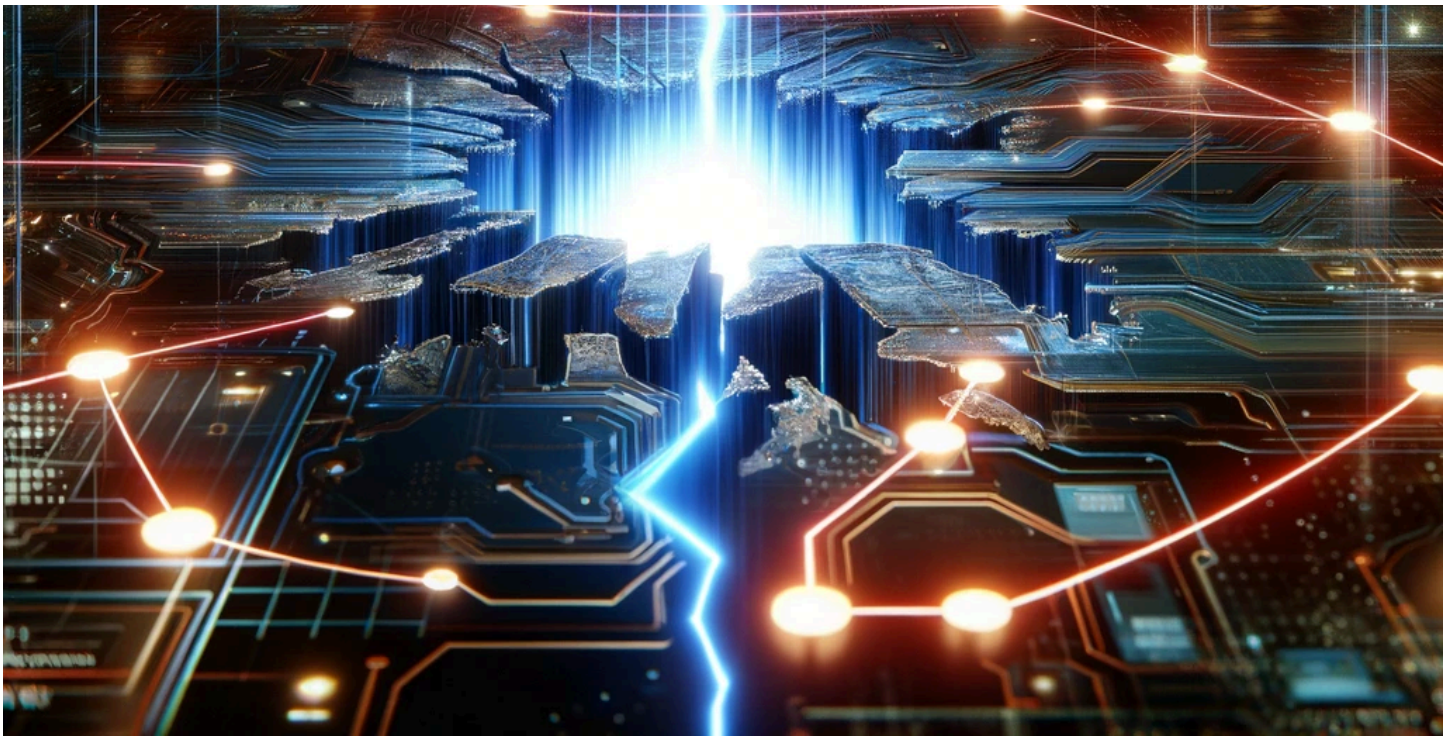
Security engineers design and implement security solutions based on threat intelligence. They ensure that the organization's infrastructure is resilient against cyber threats. Their work is foundational to maintaining a secure environment. Security engineers enable several critical functions within the organization. They support development teams by integrating security into the software development lifecycle. Compliance teams rely on them to ensure security measures meet regulatory requirements. Network administrators benefit from the guidelines and tools provided by security engineers to secure network infrastructure.

To succeed, security engineers require a diverse skill set. Technically, they must know how to harden operating systems and applications. Proficiency in configuring and managing firewalls, intrusion detection, and prevention systems is essential. Understanding encryption technologies and best practices is also crucial. Non-technical skills are vital too. Project management skills help security engineers manage security projects from inception to completion. Analytical thinking is necessary to continuously analyze and improve security measures. Creating detailed documentation and security policies is also a critical part of their role.

Cyber Threat Intelligence Managers

CTI managers oversee the entire threat intelligence program. They coordinate between different teams and ensure the effective use of threat intelligence. Their leadership is crucial for a cohesive and effective security strategy. CTI managers enable several groups within and outside the organization. Executive leadership depends on them for strategic insights and intelligence reports. All security teams benefit from the flow of intelligence and coordination managed by CTI managers. Partners and clients also gain from relevant threat information shared to protect the broader ecosystem.

CTI managers need a blend of technical and non-technical skills. A deep understanding of the global threat landscape is essential. They must be able to develop and execute threat intelligence strategies effectively. Knowledge of integrating threat intelligence into various security tools is also crucial. Leadership skills are paramount for guiding and motivating teams. Effective decision-making abilities are necessary in high-stakes situations. Collaboration skills are vital to work across different departments and with external partners.



The Essential Characteristics of Cyber Threat Intelligence Professionals

At Threat Intelligence Lab (TIL), we believe that anyone working in cyber threat intelligence (CTI) must embody certain key characteristics to excel in their roles. Based on our extensive experience in the field, we've identified five critical traits that define successful CTI professionals.

Restless in the Hunt

A relentless drive to hunt down threats is essential. In the world of CTI, complacency is not an option. Threat analysts and security professionals must constantly search for new vulnerabilities, track emerging threats, and anticipate attackers' next moves. This restless energy ensures that we stay ahead of cybercriminals and protect our organizations from potential breaches.

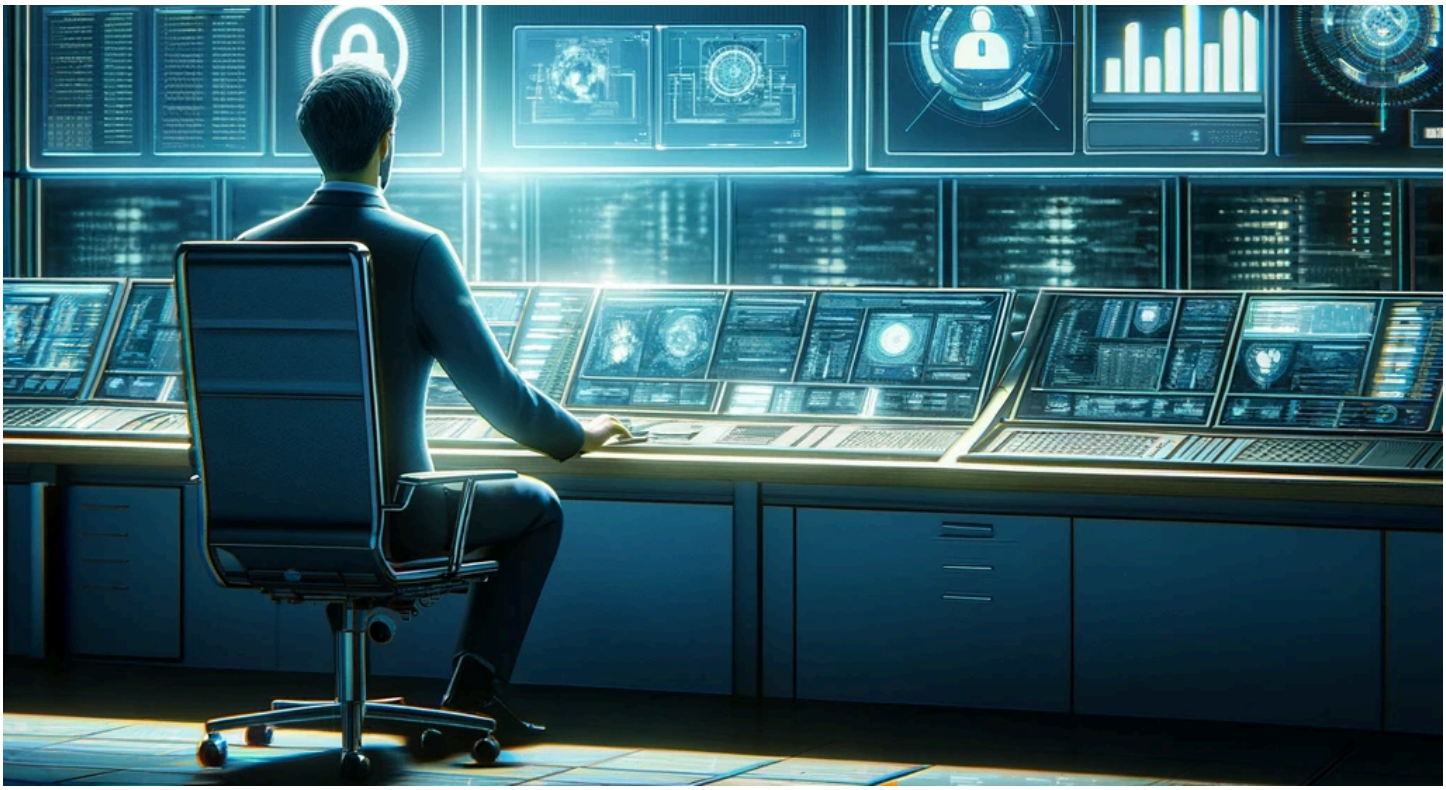
Striving for Error-Free Work

Precision is paramount in CTI. We strive to be error-free because mistakes can have dire consequences. A single oversight can lead to a significant breach, resulting in financial loss and potentially endangering lives. Our commitment to meticulousness helps us maintain the highest standards of security. We understand that attention to detail can make the difference between a thwarted attack and a successful breach.

Recognizing High Stakes

We recognize that the stakes in CTI are incredibly high. Financial repercussions from a cyberattack can be devastating. Additionally, in sectors like healthcare or critical infrastructure, the cost of a

mistake could be measured in human lives. This awareness drives us to perform our work with the utmost diligence and care. Our understanding of the potential consequences motivates us to go above and beyond in our efforts to protect our organizations and their stakeholders.

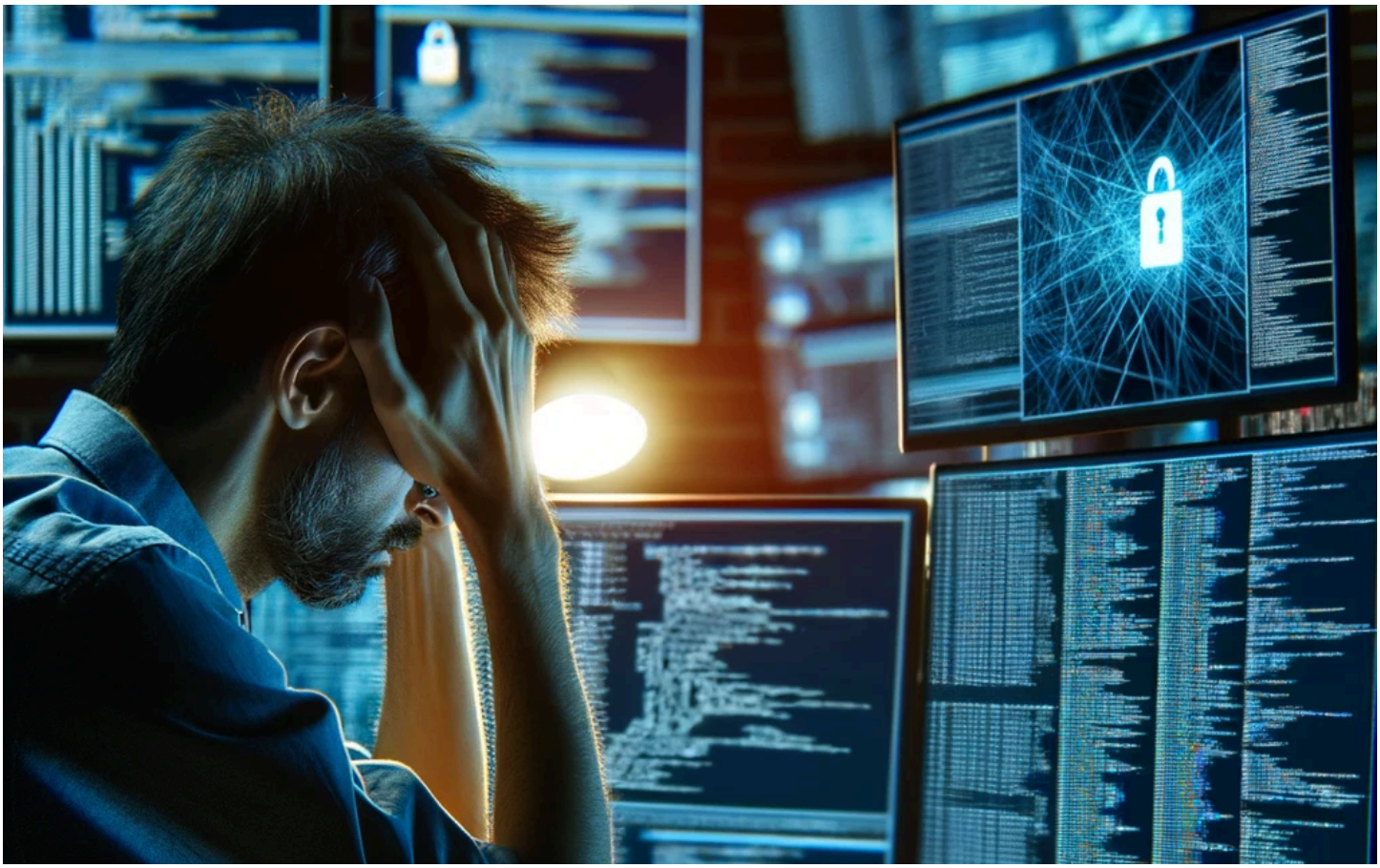


Mastering the Cat and Mouse Game

Cybersecurity is a perpetual cat and mouse game. Threat actors are always evolving their tactics, and we must adapt accordingly. Successful CTI professionals understand this dynamic and thrive in this environment. They stay informed about the latest threats and continuously develop new strategies to counteract them. This adaptability is crucial for staying one step ahead of cybercriminals and maintaining robust security defenses.

Strong Communication Skills

Effective communication is a cornerstone of CTI. Strong communication skills are necessary for conveying complex threat information clearly and concisely. Whether it's writing detailed reports for executive management, briefing incident response teams, or sharing insights with partners, CTI professionals must be able to articulate their findings effectively. Good communication ensures that everyone involved understands the threats and can take appropriate actions to mitigate them.



Balancing Kindness with Strong Boundaries

Lastly, we believe that CTI professionals need to be kind yet strong in setting boundaries. The field requires collaboration and teamwork, often under high-pressure situations. Being kind fosters a positive work environment and builds trust among team members. However, setting strong boundaries is equally important to maintain focus and efficiency. Balancing kindness with firmness ensures that tasks are completed effectively without compromising on the well-being of the team.

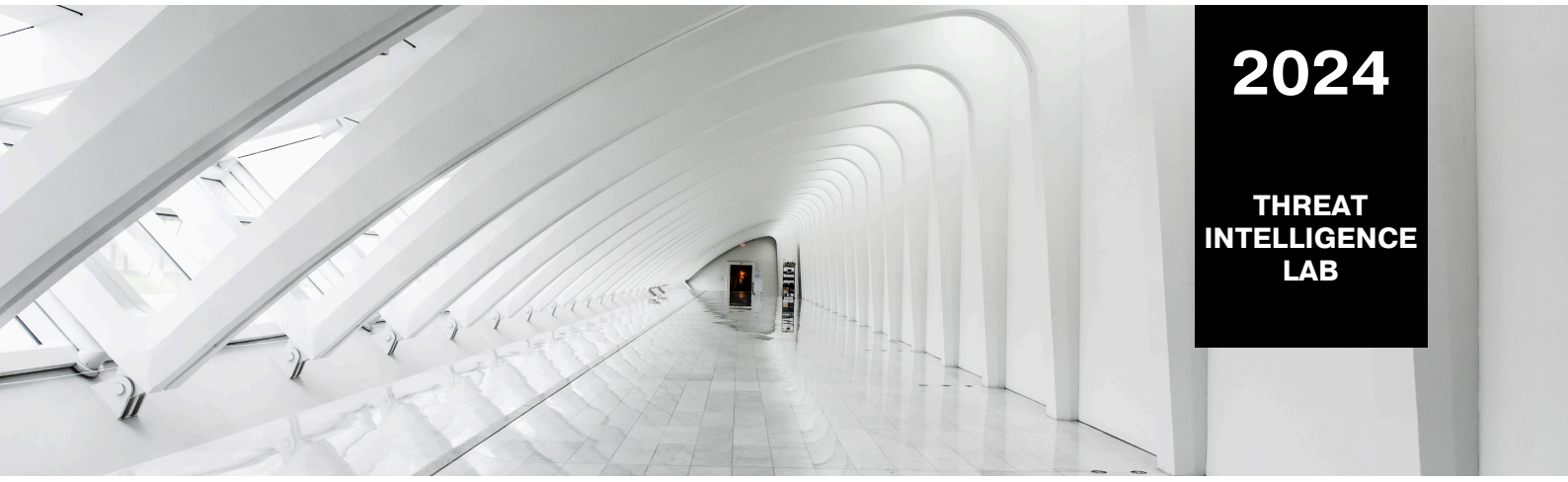
Closing Word

At TIL, we believe that these five characteristics are fundamental for anyone working in cyber threat intelligence. Restlessness in the hunt, striving for error-free work, recognizing the high stakes, mastering the cat and mouse game, and possessing strong communication skills are all essential traits.

Additionally, the ability to balance kindness with setting strong boundaries is crucial for maintaining a healthy and productive work environment. By embodying these characteristics, CTI professionals can effectively protect their organizations from the ever-evolving landscape of cyber threats.

CTI involves a diverse group of professionals. Cyber threat analysts, incident responders, security engineers, and CTI managers play vital roles in safeguarding organizations. They enable various teams within an organization to enhance security. The skills required are a mix of technical and non-technical abilities. Critical thinking, communication, problem-solving, and leadership are just as

important as technical expertise. Investing in the right people with the right skills is crucial for an effective CTI program.



For inquiries, contact us.

www.threatintelligencelab.com

support@threatintelligencelab.com

Find us at LinkedIn: https://www.linkedin.com/company/threat-intelligence-lab/