Chapter 7
Cyber Threat Intelligence for Industrial Automation:
AI-Powered Strategies

Abuh Ibrahim Sani
https://orcid.org/0009-0004-4296-0701
Eybrids, UK

ABSTRACT

The increased reliance of industrial automation on interconnected systems has made it vulnerable to cyber threats. Conventional security techniques frequently inadequately handle the dynamic and developing threat landscape. This chapter examines the essential function of Cyber Threat Intelligence (CTI) in improving the security framework of IACS environments. It specifically emphasizes utilizing artificial intelligence (AI) to automate and enhance cyber threat intelligence (CTI) processes, facilitating proactive threat detection, analysis, and response. This chapter will explore the problems associated with safeguarding IACS, the advantages of establishing a comprehensive CTI program, and the utilization of AI methodologies, including machine learning, deep learning, and natural language processing, for the gathering, analysis, and dissemination of threat data. Practical examples and case studies will demonstrate the implementation of AI-driven CTI techniques in reducing cyber risks and enhancing the resilience of essential industrial infrastructure.

1. INTRODUCTION

The increased reliance of industrial automation on interconnected systems has made it vulnerable to cyber threats. Industrial automation has tremendously transformed manufacturing, energy, and critical infrastructure, improving efficiency, precision, and scalability (Chatziamanetoglou & Rantos, 2024). This development has widened the attack surface for cyber threats targeting industrial control system (ICS) and Supervisory Control and Data Acquisition (SCADA) networks, cyber attackers, state-sponsored actors, and internal threats exploit vulnerabilities to either cause physical or operational damage (Knapp, 2024). In an industrial setting, concrete cybersecurity solutions are sorely needed as Advanced Persistent Threats (APTs) find their way there and ransomware and supply chain attacks find their place. Companies

DOI: 10.4018/979-8-3373-3241-3.ch007

have shifted from reactive cybersecurity policies to more proactive and predictive strategies given the dynamic character of these dangers (Aminu et al., 2024).

The backbone of modern industrial processes, linked with many equipment, sensors, and software solutions, cybersecurity is also important in Industrial Automation and Control Systems (IACS). Although digital development has improved operations significantly, it has also brought several; cybersecurity challenges. Unlike legacy systems, IACS space prioritizes availability and operational continuity, making cybersecurity implementation difficult to handle. Cyber incidents in industrial environments can result in reputational damages, financial losses, safety hazards, regulatory negligence, and even national security threats (Arikan et al., 2024). Therefore, a strategic approach to secure IACS is very critical to ensuring resilient industrial operations.

Cyber threat intelligence (CTI) plays a huge role in defending industrial automation systems against growing threats. Cyber threat intelligence involves collecting, analyzing, and distributing actionable intelligence about cyber threats to enhance defensive capabilities. In industrial settings, CTI helps identify weaknesses, detect anomalous activities, and mitigate risks before they escalate into full-scale attacks (Chatziamanetoglou & Rantos, 2024). CTI exerts a predominantly favorable influence, chiefly by providing early warnings that facilitate more proactive and efficient defense actions. Furthermore, strategic-level insights guide investment decisions and enhance risk evaluations. However, in both instances, some individuals find it challenging to validate this impact and to ascribe particular security enhancements or decisions exclusively to CTI (Goksør, 2024). Using artificial intelligence (AI) driven methods, companies can automatically detect threats, forecast attack trends, and react to cyber events in real time. Situational awareness guaranteed by AI-driven CTI helps industrial companies keep ahead of rivals and improve their cybersecurity architecture using which they can keep ahead of enemies.

As cyber-attacks grow in complexity and frequency, artificial intelligence-driven threat intelligence has become indispensable for enhancing cybersecurity systems throughout companies. From adaptive defenses to predictive detection, artificial intelligence offers abilities that not only increase security but also foresee and actively remove any dangers. These technologies are transforming cybersecurity by automating tedious tasks, identifying trends in large datasets, and allowing faster incident reaction times. Particularly for companies in sectors such as finance and healthcare information systems, these characteristics are rather crucial (Islam et al., 2024).

2. WHAT IS CYBER THREAT INTELLIGENCE?

Cyber threat intelligence is simply put as the process of gathering, evaluating, and interpreting data and information concerning current or potential cyber threats to determine their type, extent, and possible impact is known as cyber threat intelligence or CTI. Cyber threat intelligence encompasses far more than mere feeds of technical indicators about ongoing cyber-attacks. This field is separate from forensic cyber analysis or malware analysis; it aims not merely to provide raw data on attacks but to enhance that information for deeper comprehension (Lee, 2023).

Threat intelligence is evidence-based knowledge, such as context, mechanisms, indicators, implications, and actionable guidance regarding current or potential risks to the assets, according to Gartner Research and Mcmillan, 2003. The threat has grown in significance as a component of business cybersecurity phases because it enables them to be more proactive and identify the attacks that pose the greatest risk to their operations. Cyber threat intelligence plays an important in an organization because it helps de-