Int. J. Inf. Cybersec.-2022

Security and Resilience in Sustainable Smart Cities through Cyber Threat Intelligence

Kannan Nova
Grand Canyon University

Abstract

As sustainable smart cities continue to evolve, the importance of Cyber Threat Intelligence (TI) becomes evident in ensuring the security and seamless operation of these urban environments. This research presents three objectives that highlight the vital role of TI in sustainable smart cities, its types, along with the phases of the TI lifecycle. Objective focuses on the practical applications of TI in sustainable smart cities. These include integration with security products, enriching security alerts, proactive security measures, incident response, tuning security controls, incident investigation, assessing root causes and scope, gathering evidence and analysis, and assessing threat levels and developing security roadmaps. The second objective delves into the different levels at which TI addresses cyber threats in sustainable smart cities. Tactical intelligence focuses on identifying indicators of compromise (IOCs) to rapidly mitigate risks. Operational intelligence centers around understanding threat actors' tactics, techniques, and procedures (TTPs), enhancing incident response, and proactive threat hunting. Strategic intelligence involves comprehending the motivations and identities of threat actors, enabling cities to develop robust strategies to mitigate risks and defend against Advanced Persistent Threats (APTs). The last objective outlines the phases of the Cyber Threat Intelligence Lifecycle in sustainable smart cities. Starting with requirements, the lifecycle progresses through collection, processing, analysis, dissemination, and feedback. This systematic approach ensures the collection of relevant and reliable data, its transformation into actionable insights, and the effective communication of

findings to stakeholders. Feedback from stakeholders allows for continuous improvement and adaptation of TI operations to meet changing needs. This research emphasizes the significance of integrating TI into the security fabric of sustainable smart cities. With TI's capabilities, cities can proactively defend against cyber threats, respond swiftly to incidents, and develop resilient systems aligned with sustainability goals.

Keywords: *Threat Intelligence, Sustainable and Smart Cities, Use Cases, Cyber Threats, Incident Response, Intelligence Analysis, Security Roadmap*

Introduction

A sustainable smart city is a paradigm shift in urban development that leverages the power of information and communication technologies (ICTs) to create a more efficient, livable, and environmentally friendly urban environment. By integrating various technological advancements, such as IoT devices, data analytics, and renewable energy solutions, smart sustainable cities aim to enhance the quality of life for residents while minimizing the negative impact on the environment.

One of the key goals of a smart sustainable city is to improve the efficiency of urban operations and services. Through the use of ICTs, cities can optimize energy consumption, transportation systems, waste management, and resource allocation. For example, smart grids can monitor and regulate electricity usage, ensuring a more stable and reliable power supply while reducing energy waste. Intelligent transportation systems can optimize traffic flow, reducing congestion and travel times, and improving air quality. Additionally, advanced data analytics can enable predictive maintenance of infrastructure, preventing costly breakdowns and minimizing disruptions to city services [1].

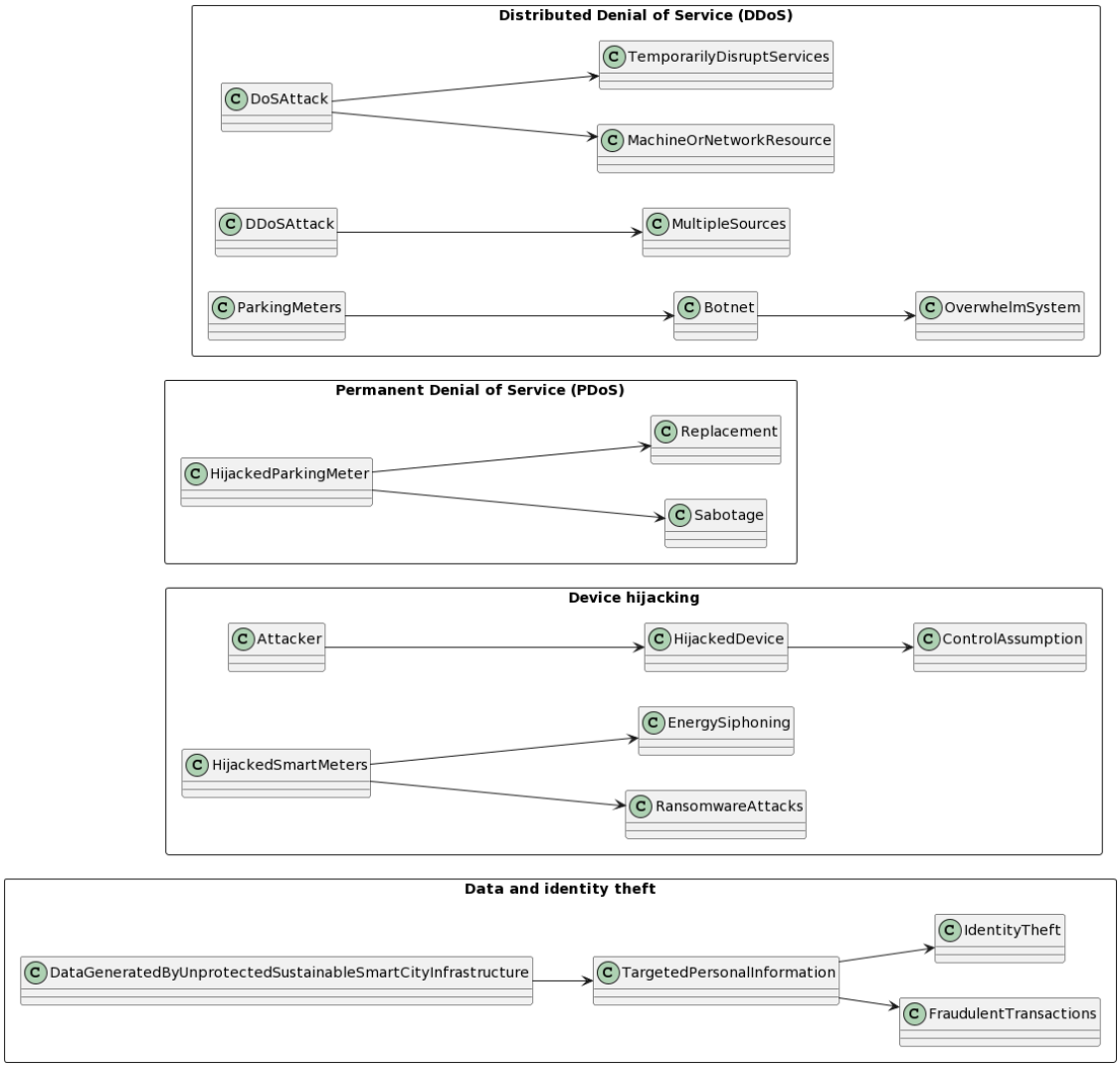
Furthermore, a smart sustainable city focuses on meeting the needs of present and future generations by considering economic, social, environmental, and cultural aspects. Economic sustainability involves fostering innovation and entrepreneurship, attracting investment, and creating job opportunities. Social sustainability entails providing equal access to basic services, promoting social inclusion, and enhancing citizen participation in decision-making processes. Environmental sustainability focuses on reducing carbon emissions, preserving natural resources, and promoting clean and renewable energy sources. Lastly, cultural sustainability emphasizes the preservation of cultural heritage, promoting arts and culture, and fostering a sense of community identity [2].

Many of connected 'things' deployed in smart sustainable cities worldwide represent a significant expansion of the Internet of Things (IoT) ecosystem [3]. This proliferation of interconnected devices and systems brings about numerous benefits, such as improved efficiency, enhanced services, and data-driven decision-making. However, the rapid growth of the IoT also introduces a wide range of vulnerabilities

that can be exploited by cyber criminals and other malicious actors. Neglecting cyber security measures in smart sustainable cities can lead to severe risks for both residents and authorities.
The interconnected nature of smart sustainable cities creates a complex network of devices and data exchange, increasing the potential attack surface for cyber threats. These threats can target various components of the city's infrastructure, including sensors, smart grids, transportation systems, and critical service providers. For example, a cyber attack on the transportation system could disrupt traffic management, leading to chaotic situations or even accidents. Similarly, compromising the smart grid infrastructure can result in power outages and disruptions to essential services.

Sustainable smart cities are susceptible to a wide range of potential vulnerabilities and attack methodologies, some of which are commonly observed in the cybersecurity landscape. One prevalent attack vector is data and identity theft, where cyber attackers exploit unprotected infrastructure within the smart city ecosystem, such as parking garages, EV charging stations, and surveillance feeds. These attackers can gain access to a significant amount of targeted personal information, which can be exploited for fraudulent transactions and identity theft. The consequences of such attacks can be severe, as they compromise the privacy and security of individuals residing in the smart city.
Another concerning attack technique is device hijacking, where an attacker assumes control of a device without altering its basic functionality. In the context of a sustainable smart city, this type of attack can have detrimental consequences. For instance, a cyber-criminal could exploit hijacked smart meters to launch ransomware attacks on Energy Management Systems (EMS). Additionally, they could clandestinely siphon energy from the municipality, leading to financial losses and disruption of critical services. Device hijacking attacks are often challenging to detect, making them particularly insidious as they undermine the integrity and reliability of the smart city infrastructure.
Furthermore, sustainable smart cities face the risk of Permanent Denial of Service (PDoS) attacks, also known as phlashing. In a PDoS attack, the attacker causes irreversible damage to a device, rendering it inoperable and necessitating hardware replacement or reinstallation. This attack scenario is especially worrisome in the context of a hijacked parking meter within a smart city. A malicious actor could sabotage the meter, causing it to malfunction or become permanently damaged.

Figure 1. Some common cybersecurity risks in a sustainable smart city



Consequently, the city would incur costs to replace the compromised device, leading to financial burdens and potential disruptions to essential services.

Distributed Denial of Service (DDoS) attacks pose another significant threat to sustainable smart cities. In a DDoS attack, the attacker overwhelms a target system

by flooding it with an excessive number of requests, making the system inaccessible to legitimate users. Unlike a traditional denial-of-service attack, DDoS attacks involve multiple sources, making it challenging to mitigate the offensive by blocking a single point of origin. In a smart city environment, various devices, such as parking meters, can be breached and coerced into joining a botnet, a network of compromised devices [4]. This botnet can then launch a coordinated DDoS attack, saturating the city's network infrastructure and impeding the normal functioning of critical services.

Cyber Threat Intelligence TI can ensure the security and resilience of smart sustainable cities. As these cities become more connected and reliant on digital infrastructure, the risk of cyber attacks and vulnerabilities can increase. TI can provide valuable insights into potential threats, emerging attack patterns, and adversary tactics, enabling city authorities and stakeholders to proactively identify and mitigate cyber risks [5].

In the context of smart sustainable cities, TI can help in several key areas. Firstly, it can assist in proactive threat detection and prevention. By monitoring and analyzing various data sources, including threat feeds, security logs, and open-source intelligence, TI can help identify indicators of compromise (IOCs) and detect potential malicious activities. This can enable security teams to respond swiftly and effectively, minimizing the impact of cyber attacks on critical city systems and infrastructure [6].

Secondly, TI can aid in incident response and recovery. In the event of a cyber attack, having access to up-to-date threat intelligence can enable city authorities to understand the nature of the attack, the motivations behind it, and the tactics employed by the attackers. This information can be crucial for formulating an effective incident response plan, containing the attack, and recovering the affected systems. TI can also provide valuable insights for conducting post-incident analysis, facilitating the identification of vulnerabilities and weaknesses in the city's security posture. Lastly, TI can enable proactive security enhancements and risk management. By continuously monitoring the threat landscape, city authorities can stay informed about emerging cyber threats and trends. This information can empower them to make informed decisions regarding security investments, infrastructure upgrades, and policy improvements. TI can also facilitate the sharing of threat intelligence within the smart city ecosystem, allowing collaboration among various stakeholders to collectively defend against common threats and vulnerabilities [7].

Cyber Threat Intelligence Use Cases in sustainable smart cities

Threat Intelligence (TI) is a vital component in the realm of sustainable and smart cities, as it helps ensure the security and smooth functioning of these urban environments. There are various use cases for TI within this domain, each serving a specific function. One significant application is the role of the Sustainable and Smart City Analyst. These analysts can integrate TI feeds with other security products and systems utilized in these cities. This integration allows for comprehensive protection of the city's infrastructure, including IoT devices, sensors, and data networks, against known threats [8]. By blocking malicious IPs, URLs, domains, files, and other indicators provided by TI feeds, analysts can safeguard critical systems and maintain the overall security of the city's operations [9].

Another crucial use case for TI lies within the City Operations Center (COC). When the COC receives alerts regarding security incidents or anomalies within the city's infrastructure, TI can play a pivotal role in enriching these alerts. Analysts can utilize TI to gather valuable information about Indicators of Compromise (IOCs) mentioned in the alerts, such as suspicious network traffic, compromised devices, or potential cyber-physical threats. This enriched information equips the COC with a better understanding of the severity of the alert and empowers them to take appropriate and timely action [10].

Furthermore, TI can be instrumental in enhancing the city's incident response capabilities. When a security incident occurs, TI can provide critical insights into the tactics, techniques, and procedures (TTPs) employed by threat actors. By understanding these TTPs, city officials and security teams can proactively implement countermeasures to mitigate the impact of the incident and prevent similar attacks in the future. TI feeds enable the COC to stay up-to-date with emerging threats and the evolving tactics used by malicious actors, enabling them to strengthen the city's defenses.

Moreover, TI can contribute to the development of proactive security measures for sustainable and smart cities. By analyzing historical threat data and identifying patterns and trends, analysts can gain valuable insights into potential future threats. This information can then be utilized to devise preventive strategies, design resilient systems, and implement effective security measures. By leveraging TI, sustainable and smart cities can stay one step ahead of threats, ensuring the safety and security of their citizens and infrastructure [11].

Another valuable application of Threat Intelligence (TI) in sustainable and smart cities is the ability to link alerts together into incidents. TI helps identify connections

between various alerts received by the City Operations Center (COC), allowing analysts to piece together a bigger picture of ongoing incidents within the city [12]. By correlating data from multiple sources, the COC can uncover patterns, trends, or even coordinated attacks targeting the city's smart infrastructure. This comprehensive view enables the COC to respond effectively, mitigate threats, and minimize the impact on city operations.

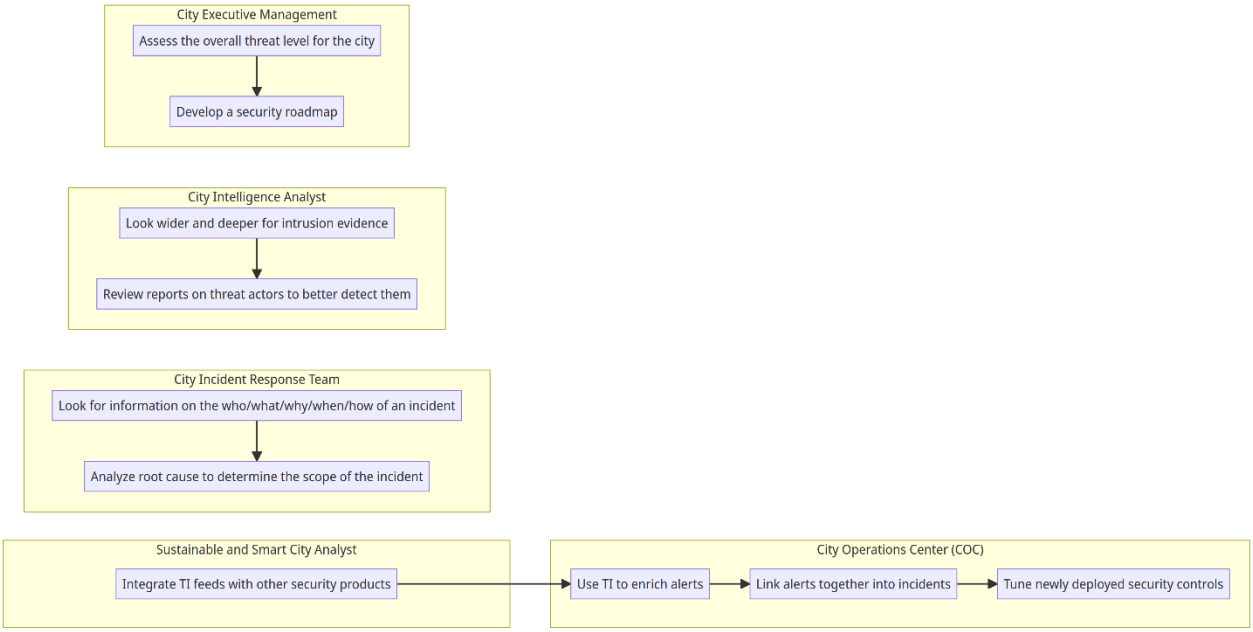
Additionally, TI plays a crucial role in tuning newly deployed security controls. As sustainable and smart cities continually adopt new technologies and implement security measures, TI insights can assist analysts in fine-tuning the configurations of these controls. By leveraging TI, analysts can optimize the settings and policies of security controls to ensure they effectively detect and respond to emerging threats. This proactive approach enhances the city's resilience and the overall efficiency of its security measures, enabling it to stay ahead of potential threats.

Furthermore, during incident response activities, the City Incident Response Team heavily relies on TI to gather relevant information about the incidents at hand. TI provides valuable insights into the "who," "what," "why," "when," and "how" of an incident. Analysts can utilize TI to identify the source of the incident, understand the attack vectors or methods employed, determine the motivations or objectives behind the incident, and establish a timeline of events. This comprehensive information empowers the response team to assess the scope and impact of the incident accurately, enabling them to formulate effective strategies for containment, eradication, and recovery.

One of its key applications is analyzing the root cause of incidents to determine their scope. TI provides valuable insights into the tactics, techniques, and procedures (TTPs) employed by threat actors targeting these cities. By comparing observed TTPs with known threat actor profiles or attack patterns available in TI sources, the Incident Response Team can assess whether an incident is isolated or part of a broader campaign. This analysis enables the team to respond appropriately and implement measures to prevent future incidents.

In the role of a City Intelligence Analyst, professionals play a vital role in gathering and analyzing TI to uncover evidence of intrusions, cyber-attacks, or vulnerabilities within sustainable and smart cities. Through comprehensive investigations and leveraging TI sources such as threat reports, open-source intelligence, and dark web monitoring, analysts provide insights into potential threats, vulnerabilities, and emerging risks. This intelligence supports strategic decision-making and the development of proactive measures to protect the city's infrastructure [13].

Figure 2. Cyber Threat Intelligence Use Cases in sustainable smart cities



TI helps intelligence analysts review reports on threat actors to better detect them. TI sources often include detailed reports and analysis on known threat actors, their techniques, motives, and infrastructure. By staying updated on the latest threat actor profiles and behaviors, analysts can align security systems and strategies with the latest TI. This alignment enhances cities' detection capabilities and strengthens their defenses against evolving threats [14].

City executives, on the other hand, rely on TI to assess the overall threat level for the city. Having a holistic understanding of the threat landscape impacting sustainable and smart cities is crucial for decision-making. TI provides insights into emerging threats, vulnerabilities in critical infrastructure, and factors such as geopolitical risks that may affect the city's security. Armed with this information, executives can assess the overall threat level and make informed decisions regarding security investments, resource allocations, and the prioritization of smart city initiatives. TI assists city executives in developing a comprehensive security roadmap for sustainable and smart cities. Leveraging TI insights, executives can identify key areas of vulnerability, anticipate emerging threats, and determine the necessary countermeasures. This roadmap guides the allocation of resources, the

implementation of resilient security measures, and the establishment of long-term security strategies aligned with the city's sustainability goals and smart initiatives.

Tactical, Operational, and Strategic intelligence in sustainable smart cities

Tactical intelligence

In the context of sustainable smart cities, Cyber Threat Intelligence (CTI) operates at the strategic level by providing crucial insights into the "who" and "why" behind potential threats. CTI aims to identify the individuals or groups responsible for specific threats or a family of threats, while also addressing ongoing trends. By understanding the "who," city authorities and stakeholders can better prepare and respond to cyber threats, ensuring the sustainable development and operation of smart city infrastructure.

At the strategic level, CTI goes beyond identifying the perpetrators and delves into the "why" of targeting organizations within a smart city ecosystem. By comprehending the motivations behind these attacks, city authorities can proactively develop strategies to mitigate risks and safeguard critical systems and services. For instance, understanding why a specific malicious cyber actor or group of actors is interested in a particular industry vertical like healthcare can help stakeholders implement targeted security measures to protect sensitive medical data and ensure the uninterrupted delivery of healthcare services within a sustainable smart city framework [15].

It is important to note that strategic level CTI often intersects with Advanced Persistent Threats (APT) activities, although not exclusively. APTs are sophisticated and prolonged cyber attacks carried out by well-resourced threat actors. Sustainable smart cities, with their interconnected infrastructure and abundance of valuable data, can become prime targets for APTs. By leveraging strategic CTI, city authorities can proactively identify and track APT activities, enabling them to adopt proactive defense measures and develop resilient systems that can withstand such persistent threats. This approach strengthens the overall security posture of a smart city, ensuring its sustainability and long-term resilience in the face of evolving cyber threats [16].

Operational intelligence

In the context of sustainable smart cities, Operational Cyber Threat Intelligence (CTI) plays a crucial role in addressing the "how" and "where" of potential threats. At the operational level, CTI focuses on understanding the observed Tactics,

Techniques, and Procedures (TTP) of threat actors. By analyzing these TTPs, city authorities and stakeholders can gain insights into how cyber attacks are conducted, allowing them to better understand the extent of a breach and prepare defense measures in advance.

The "how" aspect of operational CTI goes beyond simply receiving alerts or series of alerts. It involves a comprehensive analysis of the attack techniques employed by threat actors, such as social engineering, malware propagation, or network exploitation. By understanding the specific TTPs used, organizations within a smart city ecosystem can enhance their incident response capabilities, identify potential vulnerabilities, and strengthen their defenses against similar attack vectors. This knowledge allows them to proactively mitigate risks and minimize the impact of potential breaches on the sustainability of smart city services and infrastructure [17].

Additionally, the "where" of CTI plays a vital role in the operational level. It involves conducting proactive threat hunts, both before a compromise occurs and during the recovery phase after an incident. Threat hunting involves actively searching for signs of malicious activity within a smart city's network or system, aiming to identify any indicators of compromise or ongoing cyber threats. By knowing where to look and what to look for, city authorities can detect and respond to threats more effectively, preventing potential disruptions to essential services and preserving the sustainability of the smart city environment.

Strategic intelligence

In the context of sustainable smart cities, Tactical Cyber Threat Intelligence (CTI) plays a critical role in addressing the "what" of potential threats. At the tactical level, CTI focuses on the identification and analysis of Indicators of Compromise (IOCs). These IOCs encompass various elements such as file names, file hashes, domain names, IP addresses, and more, which provide valuable insights into the specific characteristics of cyber threats.

The "what" aspect of tactical CTI involves leveraging IOCs to triage and validate alerts within the smart city's Security Operations Centers (SOC). IOCs serve as key data points that help SOC analysts determine the nature and severity of a potential threat. By comparing observed IOCs against known threat intelligence feeds and internal databases, organizations can rapidly identify malicious activities and take appropriate actions to mitigate risks. Tactical CTI is instrumental in supporting the creation of rules for firewalls, intrusion detection/prevention systems, endpoint detection & response systems, and other similar security capabilities deployed within a smart city environment.

Internally generated data within the SOC, along with trusted external feeds, forms the foundation of tactical CTI. Organizations strive to maintain a comprehensive and up-to-date repository of IOCs specific to their smart city's environment. These trusted feeds provide real-time information about emerging threats, enabling proactive defense measures and ensuring the sustainability of smart city services. By continuously analyzing and leveraging the "what" of CTI, stakeholders can enhance their incident response capabilities, promptly identify and neutralize threats, and protect the critical infrastructure and systems that underpin the sustainable operation of a smart city [18].

Cyber Threat Intelligence Lifecycle in sustainable smart cities

Phase 1

In the context of sustainable smart cities, the requirements stage plays a crucial role in the threat intelligence lifecycle. This initial planning phase serves as a roadmap for a specific threat intelligence operation, aligning the goals and methodology of the intelligence program with the needs of the stakeholders involved. By carefully defining the requirements, the team can effectively address security challenges and enhance the overall sustainability of the smart city ecosystem.

One of the primary objectives during the requirements stage is to identify the attackers and understand their motivations. By gaining insight into potential threat actors, such as hackers or cybercriminals, city administrators can better anticipate and counter their actions. Understanding the motivations behind these attacks enables proactive measures to be taken, focusing on the specific risks that the smart city infrastructure may face.

Another essential aspect that the requirements stage explores is the attack surface. This term refers to the various entry points or vulnerabilities that attackers may exploit to compromise the smart city's systems [19]. Identifying and mapping the attack surface is crucial for developing effective defense strategies. It helps the team understand the potential weak points within the smart city infrastructure, which can then be addressed to enhance security and protect against future attacks.

Furthermore, the requirements stage involves determining the specific actions that should be taken to strengthen the defenses against future attacks. This may include implementing robust security measures, developing incident response plans, conducting regular security assessments, and enhancing cybersecurity awareness among stakeholders. By setting clear objectives and defining actionable steps, the

smart city can mitigate potential risks and ensure the long-term sustainability of its infrastructure.

In the context of sustainable smart cities, the requirements stage is vital because it facilitates a proactive approach to threat intelligence. By understanding the attackers, their motivations, the attack surface, and the necessary defensive actions, smart city administrators can build resilient systems that can withstand potential threats. A sustainable smart city should prioritize security and leverage threat intelligence to continuously adapt and improve its defenses, ensuring the safety and well-being of its residents and supporting the long-term development of the city in a sustainable manner [20], [21].

Table 1. Cyber Threat Intelligence Lifecycle in sustainable smart cities

Phase	**Details**
Phase 1 - Requirements	- Identifying threat actors and understanding their motivations - Mapping the attack surface and vulnerabilities - Defining defensive actions and objectives
Phase 2 - Collection	- Gathering data from traffic logs and publicly available sources - Monitoring forums and social media platforms - Engaging with industry experts for specialized knowledge
Phase 3 - Processing	- Organizing data into standardized formats - Decrypting encrypted data if necessary - Translating foreign-sourced data - Evaluating data relevance and reliability
Phase 4 - Analysis	- Using statistical analysis, data mining, and machine learning algorithms - Identifying patterns, trends, and anomalies - Translating analysis into actionable recommendations
Phase 5 - Dissemination	- Presenting findings and recommendations to stakeholders - Using concise and accessible formats -

	Adapting communication style to the audience - Encouraging collaboration and open dialogue
Phase 6 - Feedback	- Seeking stakeholder feedback on the provided report - Evaluating the effectiveness of operations - Adjusting priorities and objectives - Modifying reporting frequency and format - Incorporating suggestions for improved communication

Phase 2.

Once the requirements are defined during the threat intelligence lifecycle in sustainable smart cities, the next step is to collect the necessary information to meet those objectives. The team embarks on a comprehensive data collection process, leveraging various sources to gather valuable insights. The specific sources and methods employed may vary depending on the goals outlined in the requirements stage. The team often seeks out traffic logs, which provide valuable information about network activities and potential security incidents. Analyzing traffic logs helps identify patterns, anomalies, and suspicious behavior that could indicate a cyber threat. By monitoring and analyzing network traffic, the team can detect potential vulnerabilities or signs of unauthorized access, enabling them to take prompt action to mitigate risks.

In addition to traffic logs, publicly available data sources play a significant role in the information-gathering process. These sources may include open-source intelligence (OSINT), which involves collecting data from publicly accessible platforms such as news articles, public forums, and government websites. By monitoring and analyzing OSINT, the team can gather relevant information about potential threats, emerging attack techniques, or vulnerabilities affecting the smart city ecosystem [22].

Relevant forums and social media platforms also serve as valuable sources of information for threat intelligence teams. These platforms allow for discussions and knowledge sharing among security professionals, researchers, and even potential threat actors. Monitoring and participating in these forums can provide insights into the latest trends, techniques, and potential indicators of compromise, enabling the team to stay ahead of evolving threats and bolster their defenses.

Additionally, engaging with industry or subject matter experts is crucial in gathering specialized knowledge and insights. These experts possess deep understanding and expertise in specific domains related to smart city infrastructure and cybersecurity. Collaborating with them helps the team gain valuable insights, identify potential vulnerabilities, and devise effective countermeasures to enhance the security posture of the smart city.

Phase 3

Once the raw data has been collected during the threat intelligence lifecycle in sustainable smart cities, the next step is to process it into a format suitable for analysis. This data processing stage involves several tasks to ensure the data is organized, decrypted (if necessary), translated (if from foreign sources), and evaluated for relevance and reliability.

Organizing the collected data points into spreadsheets or databases is a common practice in data processing. This allows for easier manipulation, sorting, and filtering of the information, facilitating subsequent analysis. By structuring the data in a standardized format, the team can efficiently extract insights and identify patterns or correlations that may be crucial in understanding potential threats to the smart city infrastructure.

In some cases, the collected data may be encrypted, requiring decryption before analysis [23]. Decrypting files or data ensures that the team can access and utilize the information effectively. Decrypting the data is often done using encryption keys or algorithms specific to the encryption method employed, ensuring the integrity of the data during the decryption process.

If the collected data includes information from foreign sources, translation may be necessary. This involves converting the data into a language understood by the threat intelligence team. Translating the data enables the team to extract valuable insights from international sources, expanding their knowledge and understanding of potential threats and vulnerabilities that may impact the smart city ecosystem.

Once the data is organized, decrypted, and translated, it is crucial to evaluate its relevance and reliability. This evaluation process involves assessing the quality and accuracy of the data. The team examines the sources, considering factors such as credibility, reputation, and potential biases [24]. Evaluating the relevance and reliability of the data ensures that the subsequent analysis is based on trustworthy and actionable information.

Phase 4

Once the dataset has been processed during the threat intelligence lifecycle in sustainable smart cities, the next crucial step is to conduct a thorough analysis. The analysis phase is where the team dives deep into the data to find answers to the questions posed in the requirements phase. Additionally, the team works on deciphering the dataset to extract actionable insights and valuable recommendations for the stakeholders involved.

During the analysis phase, various techniques and tools are employed to extract meaningful information from the processed dataset. This may include statistical analysis, data mining, machine learning algorithms, and visualization techniques. By applying these methods, the team can uncover patterns, trends, correlations, and anomalies within the data that may indicate potential threats or vulnerabilities in the smart city ecosystem.

The analysis phase not only focuses on finding answers to the questions raised in the requirements phase but also aims to translate the analyzed data into actionable items. The team identifies key findings and translates them into practical recommendations and measures that can be implemented to strengthen the security and sustainability of the smart city infrastructure. These recommendations may include specific steps to mitigate identified risks, enhance monitoring and detection capabilities, improve incident response protocols, or invest in necessary technological upgrades [25].

Moreover, the analysis phase considers the context of the stakeholders involved in the smart city ecosystem. The team tailors the findings and recommendations to align with the specific requirements, constraints, and priorities of the stakeholders. This ensures that the analysis results are relevant, practical, and actionable for the decision-makers, allowing them to make informed choices to enhance the security and sustainability of the smart city [26].

Phase 5

In the threat intelligence lifecycle for sustainable smart cities, the dissemination phase plays a vital role in effectively communicating the results of the analysis to the stakeholders. During this phase, the threat intelligence team focuses on translating their analysis into a digestible format and presenting the findings and

recommendations to the intended audience. The presentation of the analysis depends on the stakeholders and their specific needs, often emphasizing concise and jargon-free communication.

To ensure clarity and accessibility, the recommendations derived from the analysis are typically presented in a concise manner, avoiding confusing technical jargon. The goal is to convey the key insights and actions to be taken without overwhelming the stakeholders with complex technical details. This may involve condensing the findings into a one-page report or a short slide deck that provides a high-level overview of the analysis and its implications.

The format and structure of the dissemination materials may vary depending on the preferences and requirements of the stakeholders. Some stakeholders may prefer visual representations, such as charts, graphs, or infographics, to convey the analysis effectively. Others may require a more narrative-based approach, using plain language to explain the findings and recommendations in a step-by-step manner.

In addition to presenting the analysis itself, the dissemination phase may also involve interactive sessions or workshops where the threat intelligence team engages with the stakeholders. These sessions allow for further discussion, clarification, and the opportunity for stakeholders to ask questions and provide input. By fostering collaboration and open dialogue, the dissemination phase ensures that the stakeholders have a clear understanding of the analysis and can actively participate in the decision-making process [27].

Phase 6

In the threat intelligence lifecycle for sustainable smart cities, the final stage involves seeking feedback from the stakeholders regarding the provided report. This feedback is crucial for evaluating the effectiveness of the threat intelligence operations and making any necessary adjustments for future endeavors. Stakeholders may have valuable insights and perspectives on their priorities, preferences for the frequency and format of intelligence reports, and suggestions on how data should be disseminated or presented.

Engaging in a feedback process allows the threat intelligence team to understand the evolving needs and expectations of the stakeholders. It provides an opportunity to assess whether the current approach aligns with the stakeholders' requirements and identify areas for improvement. Stakeholders may offer suggestions for modifying

the priorities or objectives of the threat intelligence program based on changes in the threat landscape or the smart city ecosystem [28].

Feedback on the cadence at which intelligence reports are provided is particularly important. Stakeholders may have varying needs, ranging from regular updates to periodic briefings or on-demand reports. Adjusting the frequency of reporting ensures that the stakeholders receive information in a timely and efficient manner, enabling them to make informed decisions regarding the security and sustainability of the smart city infrastructure [29].

Moreover, city stakeholders may provide input on how data should be disseminated or presented to maximize its impact and usability. This could involve suggestions for enhancing the clarity, relevance, and accessibility of the reports. Stakeholders' preferences regarding the format of reports, visual representations, or interactive elements can inform the threat intelligence team's approach to effectively communicate the analysis and recommendations. By actively seeking feedback and incorporating it into future operations, the threat intelligence team can improve the value and relevance of their work. This feedback loop promotes a collaborative relationship between the team and the stakeholders, fostering an environment of continuous improvement and adaptability.

Conclusion

A sustainable smart city is a new approach to urban development that utilizes information and communication technologies (ICTs) to create a more efficient and environmentally friendly urban environment. These cities integrate technologies like IoT devices, data analytics, and renewable energy solutions to enhance residents' quality of life while minimizing negative environmental impact [30], [31]. They aim to optimize energy consumption, transportation systems, waste management, and resource allocation through ICTs. Furthermore, they prioritize economic, social, environmental, and cultural sustainability, fostering innovation, providing equal access to services, reducing carbon emissions, and preserving cultural heritage.

However, the rapid growth of interconnected devices in smart sustainable cities also introduces cybersecurity risks. Neglecting cybersecurity measures can lead to severe risks for both residents and authorities. The interconnected nature of these cities expands the attack surface for cyber threats, which can target infrastructure components such as sensors, smart grids, and transportation systems. Cyberattacks on transportation systems can disrupt traffic management and compromise public

safety, while attacks on the smart grid can result in power outages and disruptions to essential services.

Sustainable smart cities face various cybersecurity vulnerabilities and attack methodologies. Data and identity theft is a prevalent attack vector, compromising personal information and threatening individuals' privacy and security. Device hijacking allows attackers to assume control of devices within the smart city ecosystem, potentially leading to ransomware attacks and energy theft. Permanent Denial of Service (PDoS) attacks can cause irreversible damage to devices, requiring costly replacements and impacting essential services. Distributed Denial of Service (DDoS) attacks overwhelm target systems by flooding them with requests, hindering the normal functioning of critical services. These cybersecurity risks must be addressed to ensure the resilience and security of smart sustainable cities.

Threat Intelligence (TI) plays a crucial role in ensuring the security and smooth functioning of sustainable and smart cities. It has various applications within this domain, such as integrating TI feeds with security products and systems to protect the city's infrastructure against known threats. TI also enriches alerts received by the City Operations Center (COC), providing valuable information about potential security incidents and aiding in timely and appropriate responses. Additionally, TI enhances incident response capabilities by providing insights into threat actors' tactics, enabling proactive countermeasures. By analyzing historical threat data, TI helps develop preventive strategies and resilient systems, staying ahead of emerging threats.

Another important application of TI in sustainable and smart cities is its ability to link alerts into incidents. By correlating data from multiple sources, the City Operations Center can identify patterns and coordinated attacks targeting the city's infrastructure. This comprehensive view allows for effective response and mitigation. TI also assists in tuning newly deployed security controls, optimizing their configurations to detect and respond to emerging threats. During incident response activities, TI provides valuable information about the scope, impact, and root causes of incidents, enabling effective containment, eradication, and recovery strategies.

In the role of a City Intelligence Analyst, professionals gather and analyze TI to uncover evidence of intrusions, cyber-attacks, or vulnerabilities within sustainable and smart cities. They investigate and leverage TI sources to provide insights into potential threats and emerging risks, supporting strategic decision-making and proactive measures. TI helps analysts review reports on threat actors, enhancing

detection capabilities and strengthening defenses. City executives rely on TI to assess the overall threat level, understand emerging threats, vulnerabilities, and geopolitical risks. This information guides security investments, resource allocations, and the development of comprehensive security roadmaps aligned with sustainability goals and smart initiatives.

In the context of sustainable smart cities, Cyber Threat Intelligence (CTI) plays a vital role at different levels: tactical, operational, and strategic. At the strategic level, CTI provides insights into the "who" and "why" behind potential threats, helping city authorities and stakeholders understand the motivations of attackers and develop strategies to mitigate risks. It also intersects with Advanced Persistent Threats (APTs), aiding in proactive defense measures against sophisticated and prolonged attacks.

Operational CTI focuses on the "how" and "where" of potential threats, analyzing the Tactics, Techniques, and Procedures (TTPs) employed by threat actors. This knowledge allows organizations to enhance their incident response capabilities, identify vulnerabilities, and strengthen defenses. Proactive threat hunting helps detect indicators of compromise and ongoing threats, ensuring early detection and response. Tactical CTI addresses the "what" of threats, focusing on Indicators of Compromise (IOCs). By analyzing IOCs, organizations can triage and validate alerts within Security Operations Centers (SOC) and rapidly identify malicious activities. Tactical CTI supports the creation of rules for security systems, enabling proactive defense measures and the sustainability of smart city services.

The requirements stage is crucial for establishing an effective threat intelligence program in sustainable smart cities. By understanding the goals and methodology of the program and aligning them with stakeholder needs, cities can anticipate and counter potential threats more effectively. Mapping the attack surface helps identify vulnerabilities, enabling the implementation of robust defense strategies. Determining necessary actions involves implementing security measures, developing incident response plans, conducting assessments, and enhancing cybersecurity awareness. In the collection stage, information is gathered from various sources to meet the defined requirements. Traffic logs and open-source intelligence provide insights into network activities, emerging threats, and vulnerabilities. Monitoring forums and social media platforms helps identify trends and indicators of compromise, while engaging with industry experts enhances knowledge of potential threats in the smart city environment.

The data processing stage involves organizing, decrypting, translating, and evaluating the collected data. Standardizing the data format facilitates subsequent analysis, decrypting files provides access to critical information, and translation broadens the scope of insights. Evaluating relevance and reliability ensures that subsequent analysis is based on trustworthy information. During the analysis phase, meaningful insights are extracted from the processed dataset using statistical analysis, data mining, machine learning, and visualization techniques. The analysis provides actionable recommendations tailored to stakeholder needs, considering the contextual factors of the smart city ecosystem. In the dissemination phase, analysis findings and recommendations are effectively communicated to stakeholders using digestible formats such as reports, slide decks, and visual representations. Interactive sessions and workshops foster collaboration and input, promoting a deeper understanding of the intelligence provided. The feedback stage involves seeking input from stakeholders to evaluate the effectiveness of threat intelligence operations. By understanding evolving needs and suggestions for improvement, adjustments can be made to ensure timely and efficient delivery of intelligence reports. This continuous feedback loop ensures that the threat intelligence lifecycle remains adaptable and responsive to the evolving challenges faced by sustainable smart cities.

References

[1] M. Shafiq, Z. Tian, A. K. Bashir, A. Jolfaei, and X. Yu, "Data mining and machine learning methods for sustainable smart cities traffic classification: A survey," *Sustainable Cities and Society*, vol. 60, p. 102177, Sep. 2020.

[2] A. H. Sodhro, S. Pirbhulal, Z. Luo, and V. H. C. de Albuquerque, "Towards an optimal resource management for IoT based Green and sustainable smart cities," *J. Clean. Prod.*, vol. 220, pp. 1167–1179, May 2019.

[3] A. Aurigi and N. Odendaal, "From 'Smart in the Box' to 'Smart in the City': Rethinking the Socially Sustainable Smart City in Context," *Journal of Urban Technology*, vol. 28, no. 1–2, pp. 55–70, Apr. 2021.

[4] A. Bodepudi and M. Reddy, "Cloud-Based Gait Biometric Identification in Smart Home Ecosystem," *International Journal of Intelligent Automation and Computing*, vol. 4, no. 1, pp. 49–59, 2021.

[5] P. Gao, F. Shao, X. Liu, X. Xiao, Z. Qin, and F. Xu, "Enabling efficient cyber threat hunting with cyber threat intelligence," *2021 IEEE 37th*, 2021.

[6] R. Trifonov, O. Nakov, and V. Mladenov, "Artificial Intelligence in Cyber Threats Intelligence," in *2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC)*, Plaine Magnien, 2018, pp. 1–4.

[7] A. Ramsdale, S. Shiaeles, and N. Kolokotronis, "A Comparative Analysis of Cyber-Threat Intelligence Sources, Formats and Languages," *Electronics*, vol. 9, no. 5, p. 824, May 2020.
[8] K. Thiagarajan, C. K. Dixit, M. Panneerselvam, C. A. Madhuvappan, S. Gadde, and J. N. Shrote, "Analysis on the Growth of Artificial Intelligence for Application Security in Internet of Things," in *2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS)*, 2022, pp. 6–12.
[9] D. Preuveneers and W. Joosen, "Sharing Machine Learning Models as Indicators of Compromise for Cyber Threat Intelligence," *Journal of Cybersecurity and Privacy*, vol. 1, no. 1, pp. 140–163, Feb. 2021.
[10] S. E. Jasper, "US cyber threat intelligence sharing frameworks," *Int. J. Intell. CounterIntelligence*, 2017.
[11] I. Sarhan and M. Spruit, "Open-CyKG: An Open Cyber Threat Intelligence Knowledge Graph," *Knowledge-Based Systems*, vol. 233, p. 107524, Dec. 2021.
[12] S. Samtani, R. Chinn, and H. Chen, "Exploring emerging hacker assets and key hackers for proactive cyber threat intelligence," *J. Manage.*, 2017.
[13] R. Brown and R. M. Lee, "The evolution of cyber threat intelligence (cti): 2019 sans cti survey," *SANS Institute. Available online: https://www. sans. org/white-papers/38790/(accessed on 12 July 2021)*, 2019.
[14] T. Schaberreiter, V. Kupfersberger, and K. Rantos, "A quantitative evaluation of trust in the quality of cyber threat intelligence sources," *Proceedings of the 14th*, 2019.
[15] S. Qamar, Z. Anwar, M. A. Rahman, E. Al-Shaer, and B.-T. Chu, "Data-driven analytics for cyber-threat intelligence and information sharing," *Comput. Secur.*, vol. 67, pp. 35–58, Jun. 2017.
[16] A. Bodepudi and M. Reddy, "Spoofing Attacks and Mitigation Strategies in Biometrics-as-a-Service Systems," *ERST*, vol. 4, no. 1, pp. 1–14, Feb. 2020.
[17] J. Zhao, Q. Yan, J. Li, M. Shao, Z. He, and B. Li, "TIMiner: Automatically extracting and analyzing categorized cyber threat intelligence from social data," *Comput. Secur.*, vol. 95, p. 101867, Aug. 2020.
[18] A. de Melo e Silva, J. J. Costa Gondim, R. de Oliveira Albuquerque, and L. J. García Villalba, "A Methodology to Evaluate Standards and Platforms within Cyber Threat Intelligence," *Future Internet*, vol. 12, no. 6, p. 108, Jun. 2020.
[19] E. Nunes *et al.*, "Darknet and Deepnet Mining for Proactive Cybersecurity Threat Intelligence," *arXiv [cs.CR]*, 28-Jul-2016.

[20] H. Griffioen, T. Booij, and C. Doerr, "Quality Evaluation of Cyber Threat Intelligence Feeds," in *Applied Cryptography and Network Security*, 2020, pp. 277–296.
[21] R. Brown and R. M. Lee, "2021 SANS Cyber Threat Intelligence (CTI) Survey," *Tech. Rep*, 2021.
[22] E. W. Burger, M. D. Goodman, P. Kampanakis, and K. A. Zhu, "Taxonomy Model for Cyber Threat Intelligence Information Exchange Technologies," in *Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security*, Scottsdale, Arizona, USA, 2014, pp. 51–60.
[23] A. Bodepudi and M. Reddy, "Cloud-Based Biometric Authentication Techniques for Secure Financial Transactions: A Review," *IJIC*, vol. 4, no. 1, pp. 1–18, Jan. 2020.
[24] X. Liao, K. Yuan, X. F. Wang, Z. Li, and L. Xing, "Acing the ioc game: Toward automatic discovery and analysis of open-source cyber threat intelligence," *Proceedings of the 2016*, 2016.
[25] A. Bodepudi and M. Reddy, "The Rise of Virtual Employee Monitoring in Cloud and Its Impact on Hybrid Work Choice," *Journal of Artificial Intelligence and Machine Learning in Management*, vol. 5, no. 1, pp. 25–50, 2021.
[26] H. Ahvenniemi, A. Huovila, I. Pinto-Seppä, and M. Airaksinen, "What are the differences between sustainable and smart cities?," *Cities*, vol. 60, pp. 234–245, Feb. 2017.
[27] W. Tounsi and H. Rais, "A survey on technical threat intelligence in the age of sophisticated cyber attacks," *Comput. Secur.*, vol. 72, pp. 212–233, Jan. 2018.
[28] S. Samtani, M. Abate, V. Benjamin, and W. Li, "Cybersecurity as an industry: A cyber threat intelligence perspective," *The Palgrave Handbook of*, 2020.
[29] K. Oosthoek and C. Doerr, "Cyber Threat Intelligence: A Product Without a Process?," *Int. J. Intell. CounterIntelligence*, vol. 34, no. 2, pp. 300–315, Apr. 2021.
[30] M. V. Moreno, M. A. Zamora, and A. F. Skarmeta, "User-centric smart buildings for energy sustainable smart cities," *Trans. Emerg. Telecommun. Technol.*, vol. 25, no. 1, pp. 41–55, Jan. 2014.
[31] S. Heitlinger, N. Bryan-Kinns, and R. Comber, "The Right to the Sustainable Smart City," in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, Glasgow, Scotland Uk, 2019, pp. 1–13.