World Academy of Science, Engineering and Technology
International Journal of Environmental and Ecological Engineering
Vol:18, No:2, 2024

Partnering with Stakeholders to Secure Digitization of Water

Sindhu Govardhan, Kenneth G. Crowther

***Abstract*—**Modernisation of the water sector is leading to increased connectivity and integration of emerging technologies with traditional ones, leading to new security risks. The convergence of Information Technology (IT) with Operation Technology (OT) results in solutions that are spread across larger geographic areas, increasingly consist of interconnected Industrial Internet of Things (IIOT) devices and software, rely on the integration of legacy with modern technologies, use of complex supply chain components leading to complex architectures and communication paths. The result is that multiple parties collectively own and operate these emergent technologies, threat actors find new paths to exploit, and traditional cybersecurity controls are inadequate. Our approach is to explicitly identify and draw data flows that cross trust boundaries between owners and operators of various aspects of these emerging and interconnected technologies. On these data flows, we layer potential attack vectors to create a frame of reference for evaluating possible risks against connected technologies. Finally, we identify where existing controls, mitigations, and other remediations exist across industry partners (e.g., suppliers, product vendors, integrators, water utilities, and regulators). From these, we are able to understand potential gaps in security, the roles in the supply chain that are most likely to effectively remediate those security gaps, and test cases to evaluate and strengthen security across these partners. This informs a "shared responsibility" solution that recognises that security is multi-layered and requires collaboration to be successful. This shared responsibility security framework improves visibility, understanding, and control across the entire supply chain, and particularly for those water utilities that are accountable for safe and continuous operations.

***Keywords*—**Cyber security, shared responsibility, IIOT, threat modelling.

I. Introduction

WATER utilities face growing threats in the digital age. For example, Dragos [1] is a security company tracking threat activities against utilities and their industrial control systems and they are regularly publishing increasing amount of information about threat activity groups and their tactics, techniques, and procedures to target utilities. This growth in digital threats necessitates a proactive approach to security. This proactive approach is to first define the purpose and functions of our system, define how threat actors might disrupt those functions, and develop remediation strategies before there is evidence of being targeted by adversaries.

Problematically, modern systems are complex and interconnected. It is expensive to gain full visibility, understanding, and control over these systems due to the interconnected nature of remote and cloud services. Typical systems require defence in depth, which is an approach in which we integrate a community of controls to protect systems (e.g., patch management, configuration control, network monitoring, incident response). Modern systems with their added complexity might extend this community of controls to also include responsibility for vendors and integrators to improve the overall efficiency and effectiveness of the defence in depth architecture. We call this movement from traditional community of controls that are within the purview of the owner/ operator towards a defense in depth that expects secure by design and security by default components a *shared responsibility model* [2], [3]. This paper explores the imperative need for implementing shared responsibility in securing water utilities by delving into the evaluation of data flows, attack surfaces and the incorporation of security measures into product development, focusing on how these processes can be adapted to bridge data silos and enhance cybersecurity capabilities.

II. Discussion Architecture

For discussion purposes, we consider a typical architecture of an IIOT system in the water or wastewater industry for the purpose of discussion in this paper. Fig. 1 provides a high-level view of an IIOT system architecture [4], one will notice similarities to the Purdue model [5] although it did not adhere directly to its traditional form to illustrate the interconnections and shared data flows.

1. Levels 0-2 (Measurement, Transmission, Control, Communication): This level consists of sensors and actuators which include legacy and modern industrial devices like robotic camera systems, water-level detectors, flow detectors, temperature sensors etc. Controllers interact with sensors and actuators to manage and control these devices on the network. It collects data from sensors for real time analysis. The data acquisition systems and gateways sit close to sensors and actuators and connect to the sensor/actuators, aggregate outputs, and convert analogue readings from these devices to digital format for transmission and enables communication over Wi-Fi, Ethernet, wired LANs, Bluetooth, cellular or the Internet to Stage 3 systems for further processing. The gateways are capable of analytics, security and data management.
2. Level 3 (Analytics, Management, Archive): This consists of physical data centres or cloud where further processing, analytics, and storage. There are multiple opportunities for processing, including on the edge, in the cloud, through

Sindhu Govardhan, Product Security Leader is with Emerging Markets, Xylem Inc., India (e-mail: sindhu.g@xylem.com).

Dr. Kenneth G. Crowther, Product Security Leader is with Americas, Xylem Inc

shared services, in data centres, and on end-user machines.

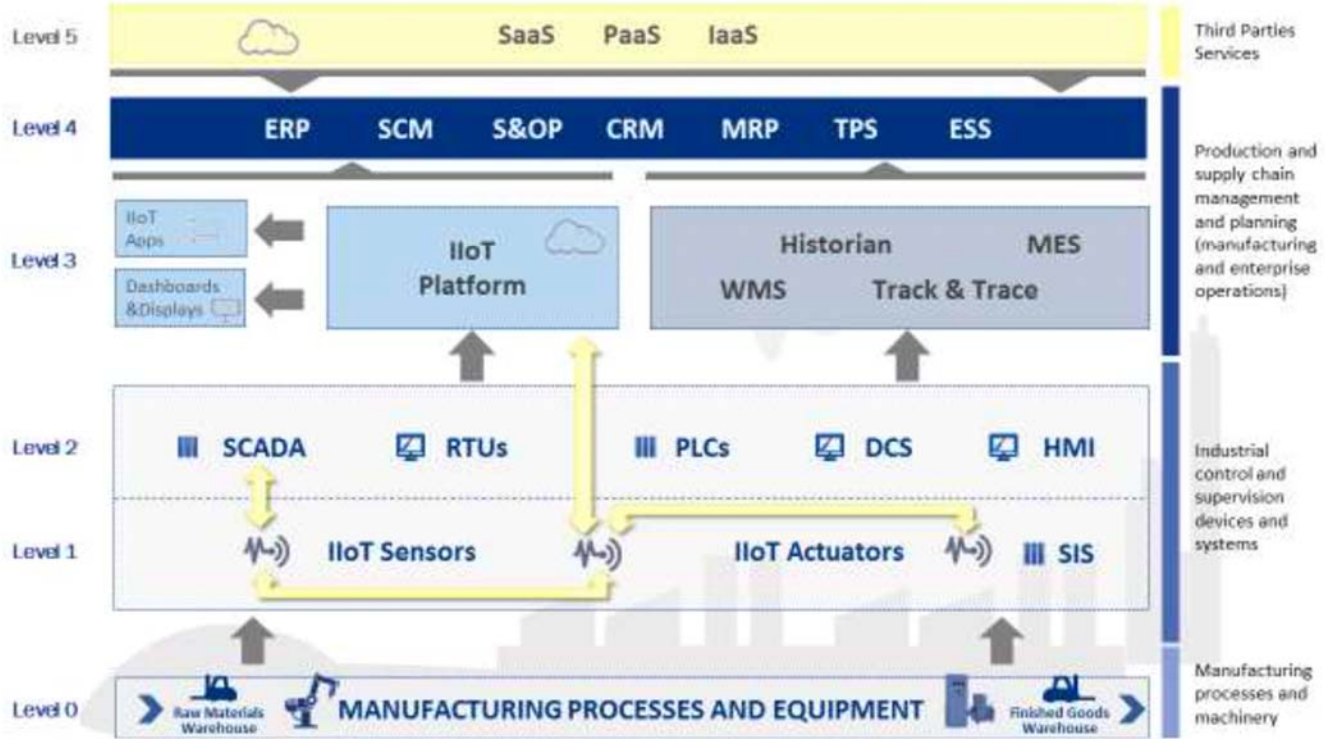

Fig. 1 High level reference model from [4]

3. Levels 4-5 (User Experience and Interpretation): At the top of the web of interconnected devices and services are the decision makers that are providing control decisions, interpretation of analyses, translations to logistics or overall process strategy, and so forth.

There are a couple of important points to draw from Fig. 1. The first is that with increased interconnectivity typical comes increased value. For example, feeding operational data to a digital twin that is optimised for wastewater processes will be able to identify under-utilised and aging assets that could save millions of Euros per year. Second, with increased interconnectivity, there is an increasingly strong business case for multiple ownership of systems and infrastructure. For example, data centre economies of scale and the increasingly common architecture of services are making it such that there is rarely a business case for owning and operating your own hardware and system software, much less your own real estate to house these systems. Shared services are increasing the multiple ownership of modern IIOT systems in the water sector. While these things are increasing the value of system, they are also increasing the exposure across those systems.

III. Threat Modelling for Security Decisions

The rest of the paper provides details on a proactive approach to secure system in Fig. 1 by showing the value of small expansion on existing concepts of threat modelling for secure design decisions. This proactive approach is to define the purpose and functions of our system, define how threat actors might disrupt those functions, and develop remediation strategies before there is evidence of being targeted by adversaries [6], [7].

1. Capture Purpose, Function, and Data Flows of the System

The first step is to thoroughly understand movement of data. To document the movement of data one must include system assets (e.g., sensors, authentication stores, certificate stores), system processes (e.g., protocol conversion, authentication, encryption/decryption), data flows (e.g., movement of data from process to process over specified ports and protocols), and trust boundaries (e.g., when data leave the control of one organization for another), also, document plant's operations and how digital technology contributes to them.

By visualizing all data flows, one can gain deeper insight into the system's dependencies and reveals vulnerable points where data can be spoofed, tampered, disclosed, denied, and abused. As a result, you can develop targeted security measures that address the specific vulnerabilities at each stage of the data journey. The pre-requisites help set the stage are:

- *System identification and scope definition*- Prior to data flow modelling identify the system and define its scope including system functions and use cases.
- *Identify the security or trust boundaries* - Define trust relationships between components and subsystems. This is particularly important for IIOT that sends data through OEMs and 4th party services.
- *Identify stakeholders* - List stakeholders involved in the lifecycle of the infrastructure. This also can be derived from market security requirements and becomes important

to defining share responsibility models to remediate threats of concern across the system.

- *Identifying critical systems and sensitive data*- Identify the critical assets and sensitive data in the system based on business reasons and justification for the need for protection. This would differ in each case considering different interest from the stakeholders in different systems.

Every component in the system may not be critical for the operation or may not be of stakeholders' interest. While some assets are stakeholders' interest, some components/assets like encryption keys in the system are might be of attackers' interest as they help attackers in compromising the system.

Data flow modelling involves the representation of how data moves through a system, illustrating the paths it takes, the processes that manipulate it, and the entities that store or consume it.

Key Components

1. *Processes:* show operations or transformations applied to the data, frequently represented by rectangles or circles.
2. *Data Flows:* show the movement of data between processes, storage, or external entities, frequently represented by one-way arrows with labels to indicate protocol and ports.
3. *Data Stores:* denote where data, such as setpoints, sensor reading, credentials, or keys, are stored within the system, frequently represented by cylinders or parallel lines.
4. *External Entities:* depict sources or destinations of data outside the system. In traditional systems we would not consider these in detail, but the IIOT system these external entities become increasingly important to understand and compensate for weaknesses. These are frequently represented by rectangles connect to the system across a trust boundary.
5. *Trust Boundaries:* are where the level of trust remains same within the boundary, but once the data cross the boundary, it is controlled and manipulated according to a different system of controls and trust. This certainly happens when data cross organizational boundaries, but also happens when data flow from one device to another. Trust boundaries are frequently represented by dashed lines or rounded rectangles.

Fig. 2 shows an example case of water treatment plant where there are smart sensors are interfaced to controllers for monitoring the parameters like level, pressure and flow. This interface uses protocols like RS-232, RS-485, and SDI-12, I2C, SPI, UART, Ethernet, Wi-Fi, Bluetooth etc. The HMI is used to monitor, configure, and do some processing on information by acting as an interface to the operator. Controller collects the data from sensors, converts the reading to digital format. These data are sent to the cloud through edge device or a gateway which is connected internet to send the data to the cloud. The data analytics, real-time monitoring, receive real time alerts, remote control capability and storage are performed in the cloud. In this typical architecture, we also see the complexity of usage of cloud from different vendors.

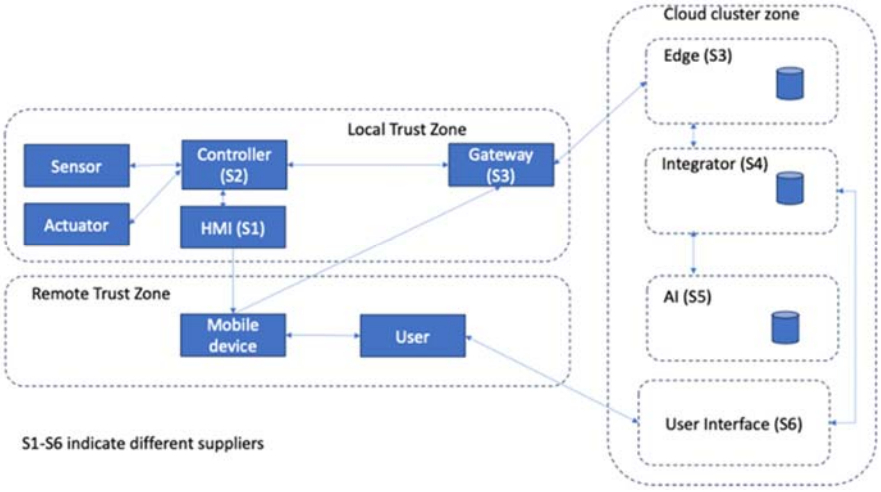

Fig. 2 Example data flow diagram for a representative IIOT product

2. Identify How Threat Actors Might Disrupt Those Functions

Once we have data flows, we need to establish a frame of reference, or some sort of basis for communicating what we consider when making security decisions. This comes from a set of representative attack vectors and risk scenarios. Here are some tips for identify threat susceptibilities of data flows and risk scenarios from those threats.

- *Identify attack surfaces.* An attack surface is the accumulation of the different points (the "attack vectors" or "threat susceptibilities") where an unauthorized user or process can interact with the system that would allow an attacker to compromise the system. Examples of attack surfaces include input and output ports, Admin interfaces, APIs etc.
- *Create an adversary model.* The adversarial model is created considering the motivation for an exploitation, required skills, resources and capabilities for the attack and

successful compromise of assets in the system. We can consider misuse cases from known cyber-attacks, attack surfaces in the system, their attack vectors and common attack goals. MITRE ATT&CK [8] provides a taxonomy of tactics, techniques, and procedures that threat activity groups have used against IT and OT systems. MITRE CAPEC [9] enumerates common attack patterns to exploit weaknesses in systems or devices. Both provide ways to understanding and represent targeting capabilities against utilities.

- *Identify all potential threats.* The Microsoft STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege) model can be used to identify the attack surfaces and attack vectors to compromise an asset. The adversarial models play important role in this analysis [10] and provide a set of prompts that aid users to developing potential threats that are specific to their data flows.
- *Risk assessment of identified threats.* To evaluate risk, we consider combinations of potential threats, the likelihood of those attacks being attempted and successful, and the consequences of such attacks. These measures are combined to obtain the overall risk of the attack.

One of the values of using ATT&CK or STRIDE methodologies is that the threat concepts directly map to security controls and mitigations. For example, Table I describes the model relationship. When you can imagine a threat from the left column of the STRIDE model, then you must strengthen the trust concept in the right column through the development of specific controls and mitigations.

TABLE I
THE CATEGORIES OF THREAT IN STRIDE CORRESPOND TO CATEGORIES OF REMEDIATION IN A TRUST MODEL.

Threat Model	Security Controls (Trust Model) To Mitigate the Threat
Spoofing	Authentication
Tampering	Integrity
Repudiation	Non-repudiation
Information Disclosure	Confidentiality
Denial of Service	Availability
Elevation of Privilege	Authorization

The accumulation of threats forms a frame of reference for your security assurance case. In other words, the list of threats constitutes the threats against which you make decisions to ensure that your product is secure by design and secure by default.

Table II simplifies the data flow diagram into three groups: Utility, OEM, and 4th Party Services. In Table II, the utility column describes illustrative threats that might happen to devices and systems in the utility's domain of visibility, understanding, and control. The OEM and 4th Party Services columns similarly capture illustrative threats that could happen in their spaces and within services that are outside of the visibility or control of the utility.

TABLE II
SEVERAL ILLUSTRATIVE EXAMPLES OF THREATS ACROSS STRIDE CATEGORIES FOR VARIOUS TRUST GROUPS IN THE IIOT EXAMPLE SYSTEM

STRIDE	Utility	OEM	4th Party Services
Spoof	Malicious firmware uploaded to device through physical access	Mimic identity of legitimate devices (e.g., change MAC address) to connect to backend	Forge API tokens/keys to gain unauthorized access
Tamper	Change sensor readings to mask leaks, overflows, or contamination events	Modify settings or control parameters to disable security features or introduce new vulnerabilities	Inject false data to manipulate system behaviour or analytic outcomes
Repudiate	Deny issuing disruptive commands	Modify sensor or system logs and claim inaccuracy	Deny responsibility for bugs in improper services functionalities
Information Disclosure	Disgruntled employees take sensitive information when they leave the utility's employ	Compromised services enable hacker to map product topology, customer & service connections	Intercept customer and ransom customer data through insecure interactions with 3rd party services
Denial of Service	Send malformed packets to IIOT devices	Flood the IIOT system with massive data requests or communication packets	Target specific vulnerabilities to crash critical services
Elevation of Privilege	Use default passwords to change device configurations	Authorized users see and manipulate other utilities' data	Intercept active sessions to get control over critical functions

The collection of these threats forms a frame of reference that can be used as a basis to communicate decisions to make a system secure by design and secure by default. While some threat may seem obvious, taking time to consider these threats provides a basis to evaluate and to communicate security measures. For example, sometimes water pressure or flow rates might seem innocuous, but they could be used by an attacker to identity a vulnerability in the water system or even to predict water shortages, cause panic, manipulate markets. Sending those data to OEM services adds value to operations precisely because the data provide insights into operations that can have large impacts on the efficiency of the water system. Another example might be the multitude of ways that services can be denied at the device, OEM, and 4th party services level. This promotes the needs to improved concepts of resilient operations when using IIOT capabilities.

3. Develop Remediation Strategies Before There Is Evidence of Being Targeted by Adversaries

The final stage is to take these threats and identify existing and needed controls. The risk methodology will help prioritize which threats are most important based on their potential impact, the criticality of the data process that they address, and the potential impact. This threat frame of reference also helps to prioritize the role of shared responsibility in your overall framework. Those threats to your data flows and processes that originate outside of your process require specific attention.

Decisions about remediation in a shared responsibility model, by necessity, must consider more than just the technical control. These decisions must consider the people and processes in addition to the technical control. For example, for the threat

of spoofing a remote server that provides updates, the technical control is to ensure adequate device and server authentication, but this is a shared responsibility. During acquisition phase, the utility needs to ensure that the device is updatable and understand the update process. When this update process requires a remote connection, they should ensure that the device and the update server have mutual authentication and protect the channels. If the update process is manual, then they should define a process to obtain and verify patches and the update procedure. Either way, the update process is a collaboration between the vendor of the device and the utility. Successful device and server authentication is the result of communicating and documenting the processes.

Another example for this paper could be the threat that a sensor is sending tampered data. The general control is measurement authenticity requirements. That is, it may be required to include a proof of authenticity of measurements at the application level (i.e., a proof that is not linked to communications and can be archived with the content). Again, this should consider not just the technical control, but the people and processes associated with its implementation. In this case many processes have skilled operators that can recognize when sensors might be misreading. We need to train those users to not just suspect malfunction, but to know when it is necessary to report to cyber incident response for investigation. Establishing strong incident investigation procedures can triage and evaluate these findings to minimize damage, prevent future attacks, comply with regulations, and maintain trust with stakeholders. It is an ongoing process that contributes to a robust and proactive security culture within your organization.

Frequently, a single remediation provides protection against a variety of threats. For example, for threats that spoof identities and overwhelm system to cripple communication, remediations include those in the category of identity and access management (IAM). IAM ensures the right people and systems (identities) access the right resources at the right time. However, IAM is not completely within the control of the utility. A utility can establish clear policies and procedures for identification of people and assets, requirements for their access, harden internal infrastructure by implementing strong password requirements and auditing, but continuously monitoring user access and dataflow for proper use, etc. The OEM and cloud services must develop solutions that allow for unique access privileges, that use strong encryption to protect accounts, that provide least-privilege access to their own support. There is a need for shared security. For example, OEMs can offer products with strong identity management, logging and patching capabilities. However, these security features can still result in escalation of privilege through improper updates, if the utilities do not properly install updates from correct source and monitoring logs for proper change control. To establish IAM effectively, the utility will need to communicate about these needs as part of the product evaluation and supplier onboarding processes and ensure that those evaluations are specific to the protecting data flows of operations by the IIOT solution and not generic to the supplier's IT systems. These conversations will need to be ongoing and collaborative toward the common goal of shared security through transparency.

IV. Discussion and Conclusions

In general, shared responsibility model benefits systems that need low-cost security implementation, need to scale functionality without exponential increases in costs, generally share security objectives and expectations with IIOT vendors, and need to be able to protect against emerging threats.

The implementation of threat modelling in securing water utilities is useful for safeguarding critical infrastructure. The planning and sharing of responsibility among stakeholders play a pivotal role in establishing a robust security framework. Recognizing that security is a shared responsibility between individuals, organizations, contractors, vendors, and other relevant parties is valuable for creating a comprehensive defence against potential threats.

A major aspect of this approach is to plan the threat model as early as the solution architecting phase. From policymakers and utility operators to cybersecurity experts and local communities, a collective effort is required to formulate and execute effective threat modelling strategies. Establishing clear lines of responsibility and communication channels among these stakeholders is paramount to creating a resilient defence against evolving threats.

The next stage is to consciously divide the threat modelling procedure into more manageable, smaller parts. By doing so, organizations can gradually implement security measures across different facets of their operations, fostering a more adaptive and responsive security posture. This incremental approach not only allows for a more efficient implementation but also facilitates continuous improvement and adaptation to evolving threats, which is a valuable mindset for cybersecurity of systems that are ever changing and evolving.

Regulators are just starting to examine the area of cybersecurity within critical infrastructure, and different states will approach this differently and with differing benefits and societal costs. This threat modelling approach is intended to promote the concept of proactive shared responsibility, even before regulator step in to define rules and accountability. In some states there will eventually be strict rules that mandate specific practices of both utilities and OEM. These strict rules will force a shared responsibility model that has been dictated centrally and will define a common set of accountabilities. However, it is difficult to know if it will ever be enough and the threat modelling approach will still provide value. In other states, regulators will have a lighter touch, focusing on security outcomes or transparency, rather than specific requirements. This transparency could drive markets to compete on verifiable security measures. Again, neither full transparency nor specific security requirements will solve all problems. Moreover, standards are always a couple of years behind and will always lag security for novel solutions that create value.

Measuring the effectiveness of threat reduction and compliance is needed for evaluating the success of security initiatives. Regular assessments and audits should be conducted to ensure that security measures are effective and in compliance

with established standards and regulations. This iterative process enables organizations to identify areas for improvement and refine their security strategies over time.

It is valuable to emphasize that threat modelling must be tailored to specific needs and capabilities. Each water utility, with its unique blend of technology, personnel, contractors, and vendors, requires a tailored approach to threat modelling. Customizing threat modelling methodologies to the specific needs and characteristics of each utility ensures that security measures align with the organization's specific risk landscape. This tailoring should consider the intricacies of the technology stack, the skill set of personnel, and the intricacies of partnerships with external entities.

Securing water utilities demands a holistic and adaptable approach. By embracing threat modelling, sharing responsibility, and tailoring strategies to the unique context of each utility, the water industry can fortify its defences against an evolving threat landscape, safeguarding the vital resource that is water. This collaborative and adaptive approach is essential for the sustainable and resilient protection of critical infrastructure in the face of emerging cybersecurity challenges.

REFERENCES

[1] Dragos, 2023. *Summary of Threat Activity Groups.* Available online: https://www.dragos.com/threat-groups/
[2] AWS, 2023. *Amazon Web Services (AWS) Shared Responsibility Model.* Available online: https://aws.amazon.com/compliance/shared-responsibility-model/
[3] Lostri, E, JA Lewis, G Wood, 2022. *A Shared Responsibility: Public-Private Cooperation for Cybersecurity*. Center for Strategic International Studies. Published March 1, 2022. Available online: https://www.jstor.org/stable/resrep40145
[4] ENISA, 2018. *Good Practices for Security of Internet of Things in the context of Smart Manufacturing.* Available online: https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot
[5] Mission Secure, 2023. Is the Purdue Model Relevant in a World of Industrial Internet of Things (IIoT) and Cloud Services? Available online: https://www.missionsecure.com/blog/purdue-model-relevance-in-industrial-internet-of-things-iiot-cloud
[6] Shostack, A, 2014. *Threat Modeling: Designing for Security*. Wiley.
[7] Microsoft, 2023. *Threat Modeling.* Available online: https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling
[8] MITRE, 2015. ATT&CK Knowledge Base. https://attack.mitre.org/
[9] MITRE, 2007. CAPEC Enumeration. https://capec.mitre.org/
[10] Hernan, S, S Lambert, T Ostwald, A Shostack, 2006. Threat Modeling: Uncover Security Design Flaws Using the STRIDE Approach. *MSDN Magazine*. 2006 (November). Available online: https://learn.microsoft.com/en-us/archive/msdn-magazine/2006/november/uncover-security-design-flaws-using-the-stride-approach