STAXX: Free STIX / TAXII Solution: Open-Source Threat Intel Platform Technical Review Report

Abstract - (by Keerthi)

STAXX is a free cyber threat intelligence (CTI) client application designed for SMEs and organizations in developing economies. It allows users to collect and manage CTI feeds, which contain information about the latest threats, indicators of compromise (IOCs), and malicious actors. STAXX boasts a simple interface and setup process, making it ideal for organizations with limited IT resources. It also offers powerful search and investigation functionalities, data sharing capabilities, and even offline functionality.

This document provides an overview of STAXX, including its tool description, system requirements, installation process, configuration needs, functional capabilities, performance metrics, usability and accessibility considerations, integration, compatibility, and scalability aspects. It also details the community support and sustainability features offered by Anomali, the developer of STAXX. Finally, the document identifies potential gaps in threat intelligence tools designed for SMEs and developing economies and proposes areas for improvement. [2]

Tool Name :	STAXX: Free STIX / TAXII Solution
Evaluated Version:	
Evaluation period:	
Evaluator(s):	
Purpose of Review:	Assess capabilities for SMEs/developing economies and identify gaps and features for a new threat intel platform.

Tool Overview (by Keerthi)

- ## Tool Description:

STAXX is a free client application developed by Anomali that allows you to collect and manage cyber threat intelligence (CTI) feeds. These feeds contain information about the latest threats, indicators of compromise (IOCs), and malicious actors. By using STAXX, SMEs and organizations in developing economies can improve their threat detection and prevention capabilities without a high-cost barrier. [7]

- ## Key Features:

Free Threat Intelligence: STAXX connects to any STIX/TAXII compatible feed, including free public feeds from government agencies and security communities. This allows you to access valuable threat data without needing to purchase expensive subscriptions.
Easy to Use: STAXX boasts a simple interface and setup process. This makes it ideal for SMEs and organizations with limited IT resources.
Powerful Search and Investigation: STAXX allows you to quickly search through your collected threat intelligence data. You can also investigate specific indicators to understand the broader threat context.
Data Sharing: STAXX allows you to share threat intelligence with trusted partners, further enhancing your organization's threat protection.
Offline Functionality: Even without a constant internet connection, STAXX can store and analyze collected threat intelligence.

Installation and Setup (by Keerthi)

- ## System Requirements:

Before proceeding, ensure your system meets the minimum requirements:

- **Operating System:**
  - Windows 10 (64-bit)
  - macOS 10.12 or later
- **Disk Space:** 100 MB
- **Memory:** 4 GB RAM

Recommended Requirements:

For optimal performance, consider:

- **Operating System:** Latest version of Windows 10 (64-bit) or macOS
- **Disk Space:** 500 MB
- **Memory:** 8 GB RAM

Download STAXX

Visit the official Anomali website: https://www.anomali.com/resources/staxx
Locate the download section for STAXX.
Download the installer file compatible with your operating system (Windows or macOS).

- ## Installation Process:

Locate the Downloaded File: Navigate to your Downloads folder (or wherever you saved the installer file).
Run the Installer: Double-click the downloaded installer file (e.g., "STAX_Installer_vX.X.exe" for Windows or "STAX_Installer_vX.X.dmg" for macOS).

Windows Installation:

User Account Control (UAC) Prompt: You might encounter a UAC prompt asking for permission to run the installer. Click "Yes" to proceed.
Welcome Screen: The STAXX installer window will appear. Click "Next" to continue.
License Agreement: Carefully read the license agreement. If you agree to the terms, select the "I accept the license agreement" checkbox and click "Next."
Installation Location: Choose the location on your hard drive where you want to install STAXX. By default, the installer suggests the program files directory. You can keep the default location or click "Browse" to select a different folder. Click "Next" to continue.
Shortcut Creation: Select whether you want to create shortcuts for STAXX on your desktop and/or Start menu. Click "Next" to proceed.
Ready to Install: Review the installation summary. If everything looks correct, click "Install" to begin the installation process.

Installation Progress: A progress bar will indicate the installation status. Wait until the installation is complete.
Installation Complete: Once finished, a completion message will appear. You can choose to launch STAXX immediately by checking the "Launch STAXX" box. Click "Finish" to exit the installer.

macOS Installation:

Drag and Drop: After downloading the installer (.dmg file), drag and drop the STAXX icon to the Applications folder.
Verification: You may see a message "Are you sure you want to open this application?" Click "Open" to proceed.
Run STAXX (Optional): Double-click the STAXX icon in the Applications folder to launch the application.

Once the installation process is complete, you're now ready to launch STAXX and begin collecting valuable threat intelligence. Here's what to do next:

Launch STAXX: Navigate to the location where STAXX was installed and double-click the application icon to launch it. On Windows, you can typically find it in the Start menu or on the desktop if you opted to create shortcuts during installation. On macOS, locate STAXX in the Applications folder.
Configure CTI Feeds: Upon launching STAXX, you'll need to configure your cyber threat intelligence (CTI) feeds. Refer to the STAXX Configuration Guide for detailed instructions on setting up and managing your feeds. This guide will help you select and connect to the most relevant STIX/TAXII compatible feeds for your organization's needs.
Customize Settings: Explore STAXX's settings and customization options to tailor the tool to your specific requirements. This may include adjusting notification preferences, setting up automated data sharing with trusted partners, and configuring data storage and retention policies.
Start Collecting Threat Intelligence: Once configured, STAXX will begin collecting threat intelligence from your chosen feeds. Monitor the dashboard regularly to stay informed about the latest threats, indicators of compromise (IOCs), and malicious actors relevant to your organization.
Refer to the STAXX Configuration Guide: For further instructions on optimizing STAXX's functionality and getting the most out of the tool, refer to the comprehensive STAXX Configuration Guide. This guide provides step-by-step instructions, best practices, and troubleshooting tips to ensure smooth operation.
https://assets-global.website-files.com/6453db2ad32b573c40a15c49/649e4a854d05799152972ddd_Anomali_STAXX_Installation__Administration_Guide_2023.pdf

Additional Notes

- **Firewall Configuration:** In rare cases, your firewall might block STAXX from communicating properly. The Configuration Guide will provide instructions on adjusting firewall settings if necessary.
- **Administrator Privileges:** Running the installer might require administrator privileges. Ensure you have the necessary permissions on your system.

Troubleshooting

If you encounter any issues during installation, refer to the STAXX support resources available on the Anomali website or contact Anomali support for further assistance.

- ## Configuration Needs:

STAXX is designed for immediate use with minimal configuration. Here's why:

Pre-Configured for Common Feeds: STAXX comes pre-configured to work with many popular STIX/TAXII threat intelligence feeds. This eliminates the need for extensive manual configuration.

Simple Feed Addition: Adding new feeds is a straightforward process. You'll typically just need to provide the feed URL and credentials (if required).

Intuitive Interface: The user interface is clean and uncluttered, allowing you to easily navigate and understand the available settings.

However, the STAXX Configuration Guide https://assets-global.website-files.com/6453db2ad32b573c40a15c49/649e4a854d05799152972ddd_Anomali_STAXX_Installation__Administration_Guide_2023.pdf will offer general guidance on:

- Adding and managing CTI feeds
- Customizing threat intelligence views
- User account management

Functional Capabilities (by Keerthi)

- ## Core Functionalities:

Core Functionalities:

Threat Intelligence Collection: STAXX allows users to collect cyber threat intelligence (CTI) feeds from various sources, including free public feeds from government agencies and security communities. This functionality provides SMEs in developing economies with access to valuable threat data without the need for expensive subscriptions. [6]

Simplicity in Setup and Navigation: STAXX boasts a simple interface and setup process, making it ideal for SMEs with limited technical capabilities. This functionality ensures that even organizations with minimal technical expertise can easily deploy and navigate the tool to derive intelligence. [8]

Search and Investigation: STAXX enables users to quickly search through collected threat intelligence data and investigate specific indicators of compromise (IOCs). This functionality helps SMEs in developing economies to identify and understand potential threats, even with minimal technical resources. [1]

Data Sharing: The tool allows users to share threat intelligence with trusted partners, enhancing overall threat protection capabilities. This functionality is valuable for SMEs in developing economies, as it enables collaboration and information sharing within the cybersecurity community, even with limited financial capabilities. [4]

Offline Functionality: STAXX can store and analyze collected threat intelligence data even without a constant internet connection. This functionality ensures continuous threat monitoring and analysis for SMEs in developing economies, even in regions with unreliable or limited internet access.

- ## Performance Metrics:

  Due to unforeseen system issues, we were unable to conduct a comprehensive performance evaluation of STAXX as originally planned. The following metrics were intended for measurement: [6,1.8]

Resource Utilization

- **CPU Usage:** Monitor CPU usage during various tasks like initial launch, data collection, and threat intelligence searches.
- **Memory Usage:** Track memory consumption under different workloads to identify potential bottlenecks.
- **Startup Time:** Measure the time it takes for STAXX to launch and become fully functional.
- **Data Collection Speed:** Evaluate the speed at which STAXX collects data from CTI feeds. This can be influenced by factors like feed size and internet connection speed.

Performance

- **Search and Retrieval Performance:** Measure the time it takes to search for specific indicators or threat actors within the collected intelligence.
- **Scalability:** Test how STAXX handles increasing data volumes and user demands. Ideally, performance shouldn't degrade significantly as the amount of threat intelligence grows.

Usability in Resource-Constrained Environments

- **Offline Functionality:** Verify that STAXX can function effectively without a constant internet connection. This is crucial for environments with unreliable internet access.
- **Error Handling and Stability:** Monitor for errors or crashes during operation. A stable application with proper error handling is essential for resource-constrained environments.
- **User Interface Responsiveness:** Evaluate the responsiveness of the user interface on a computer with limited resources. A slow or unresponsive interface can hinder productivity.

- ## Accuracy and Reliability:

Data Collection:

STAXX offers a variety of CTI feeds relevant to common SME threats such as malware, ransomware, and phishing attacks. These feeds are sourced from reputable sources including government agencies and security communities, providing SMEs with diverse threat intelligence.

Adding, removing, and managing CTI feeds is straightforward within STAXX. The tool comes pre-configured with popular STIX/TAXII compatible feeds, and users can easily customize their feed selection based on specific needs.

Data Processing:

STAXX provides clear information on how collected CTI data is filtered, aggregated, and transformed for presentation. The tool employs advanced algorithms to normalize data from different sources, ensuring consistency and accuracy in threat intelligence analysis.

While STAXX does not offer explicit options to prioritize or categorize threats within the tool, users can leverage customizable views and filtering options to focus on relevant threat data for their organization.

Data Presentation:

The user interface of STAXX is designed to be intuitive and easy to navigate, catering to users with limited technical expertise commonly found in SMEs. Clear visualizations and

straightforward navigation enhance user experience and facilitate effective threat intelligence management.

STAXX offers some customization options for dashboards and views, allowing users to tailor their display preferences to highlight the most critical threat intelligence for their business. However, the extent of customization may be limited compared to more advanced threat intelligence platforms.

Export functionality within STAXX enables SMEs to share threat intelligence data with internal teams or external stakeholders for further analysis or collaboration, supporting information sharing and collaboration efforts.

Control and Visibility:

STAXX provides users with control over CTI feeds, allowing them to manage which feeds are used and how they are updated. Users can configure feed settings and update schedules based on their organization's requirements.

Configuration options for alerts and notifications enable SMEs to set up automated alerts for specific threat indicators relevant to their environment. Users can customize alert thresholds and notification preferences to ensure timely response to potential security risks.

Users have control over data filtering and views within STAXX, enabling them to create custom views tailored to their organization's needs. While the level of customization may not be as extensive as in more advanced platforms, SMEs still have the flexibility to focus on high-priority threats. The evaluation provided above is based on the existing data available.

Usability and Accessibility (by Keerthi)

- **Ease of Use:**

Considering the skill level available in SMEs and developing economies, STAXX strives to be user-friendly. However, there may still be challenges for users with limited technical expertise. The tool's simplicity in setup and navigation helps mitigate these challenges, but further improvements could enhance usability, particularly in guiding users through more complex tasks like configuring CTI feeds or interpreting threat data. [5]

- **Interface Design:**

STAXX aims to cater to both technical and non-technical users with its intuitive interface. While it provides essential functionalities for threat intelligence collection and management, the interface may still present some barriers for non-technical users. Simplifying terminology and providing clear visual cues can enhance accessibility for users with varying levels of technical expertise. [1]

- **Documentation and Support:**

STAXX may have some room for improvement in terms of clarity and comprehensiveness, as there is no clear documentation on the webpage, however there is a clear support video to assist in the installation process and a clear way in which users can contact STAXX support.

Installation video - https://youtu.be/gowDFVc_5qU?si=DZ7A0OF3p_vAjfQW

A clear support video is crucial for users with limited technical expertise as it provides visual guidance on how to navigate the tool or resolve issues. The video effectively communicates instructions in a step-by-step manner, with understandable language and visuals, it enhances clarity and facilitates comprehension for less technical users.

Making it easy to contact STAXX support is beneficial for users who may encounter difficulties during installation or usage. Users with limited technical expertise may feel reassured knowing that help is readily available and accessible. A straightforward process for contacting support, through a dedicated portal, this enhances the user experience by providing assistance when needed.

Integration, Compatibility, and Scalability (by Mitchell)

- **Interoperability with Existing Tools:**

  - Integration with SIEM (Security Information and Event Management), EDR (Endpoint Detection and Response), and TIPs (Threat Intelligence Platforms): STAXX can enrich these systems with contextual threat intelligence data, enhancing detection and response capabilities by providing additional context about threats and indicators.

  - Collaboration with Threat Feeds and Sharing Platforms: STAXX interoperates with external threat feeds and sharing platforms, such as ISACs (Information Sharing and Analysis Centers) or industry-specific sharing communities, facilitating the exchange of intelligence data for collective defense efforts.

- ## APIs and Customization:

  - STAXX offers APIs (Application Programming Interfaces) that allow users to integrate it with other tools and systems. These APIs enable communication between STAXX and other security solutions, facilitating data exchange and automation of workflows. For example, organizations can use STAXX APIs to pull threat intelligence data into their existing security infrastructure or push indicators of compromise (IOCs) from their systems to STAXX for analysis.
  - STAXX also provides customization options to tailor the platform to specific organizational requirements. This includes customizable dashboards, alerting rules, reporting templates, and user roles. Customization allows organizations to configure STAXX according to their unique security needs, workflows, and preferences, enhancing its effectiveness and usability in their environment.

  - Additionally, STAXX supports the development of add-ons or extensions by third-party developers. These add-ons can extend the functionality of STAXX beyond its core features, addressing niche requirements or integrating with specialized security tools. This ecosystem of add-ons enhances the flexibility and extensibility of STAXX, allowing organizations to further customize and enhance their security operations.

- ## Scalability:

- STAXX is designed to scale both horizontally and vertically to accommodate growing volumes of data and users. Horizontal scalability allows organizations to add more servers or instances to distribute the workload and handle increased data processing demands. Vertical scalability enables organizations to scale up resources within a single server or instance, such as increasing CPU, memory, or storage capacity, to handle larger datasets and user loads.

- STAXX employs a distributed architecture that allows it to scale across multiple nodes or servers in a network. This distributed approach enables load balancing, fault tolerance, and high availability, ensuring that STAXX can handle increased traffic and data volumes without sacrificing performance or reliability.

- STAXX can offer integration with cloud computing platforms, allowing organizations to leverage scalable cloud infrastructure for deploying and managing the platform. Cloud integration enables organizations to allocate resources based on demand, scale infrastructure up or down as needed, and take advantage of cloud-native services for enhanced scalability, resilience, and cost-efficiency.

- **Flexibility:**
  STAXX features a modular architecture that allows organizations to customize and extend its functionality according to their specific requirements. This modular approach enables organizations to selectively deploy and integrate different modules or components based on their needs, preferences, and existing infrastructure. For example, organizations can choose to deploy specific modules for threat intelligence analysis, data enrichment, or reporting, depending on their priorities and use cases.

Community Support and Sustainability (by Mitchell)

- **Developer Community:**
  STAXX provides dedicated support channels such as email, phone, or ticketing systems for users to seek assistance with technical issues, questions, or concerns. Having accessible support channels ensures that SMEs can easily reach out for help when needed, regardless of their technical expertise.

- **Updates and Maintenance:**
  STAXX provides regular software updates and patches to address security vulnerabilities, introduce new features, and improve overall performance. Ensuring that SMEs have access to timely updates is essential for maintaining the security and reliability of the platform, especially for organizations without dedicated IT staff to manage software maintenance.

- **Local and Global Support Networks:**

The support networks STAXX provides are very accessible at the top of the company's website, the channels available include:

- Call Support: A dedicated phone line (1-844-4THREATS) is available for users to reach out to support representatives directly, enabling real-time communication and immediate assistance.
- Email Support: Users can also contact support via email (support@anomali.com) to report issues, ask questions, or request assistance. Email support offers asynchronous communication and provides a documented record of interactions.
- Support Portal: The support portal is mentioned, but without a direct link, it's unclear whether this provides additional resources or serves as a platform for submitting support tickets or accessing documentation.

STAXX also provides Customer Success Organization (CSO):

- CSO offers a variety of services to help clients successfully deploy and develop their threat intelligence programs, indicating a commitment to customer success and ongoing support.
- CSO provides 24-hour support and additional services, including management of intelligence information, support/management of STAXX software solutions, assistance with integration solutions, and training of staff involved in threat intelligence operations. This comprehensive support covers various aspects of using STAXX, ensuring that users receive assistance with deployment, management, integration, and training.

Assessment of Gaps (by Keerthi)

- ## Identified Gaps:

While STAXX addresses many challenges faced by SMEs and developing economies, there's still room for improvement in threat intelligence tools for these specific users. Here's an assessment of identified gaps and potential areas for development: [7,8]

Identified Gaps:

Limited Threat Analysis: Many free tools, including STAXX, primarily focus on collecting and displaying CTI feeds. Advanced threat analysis capabilities, such as threat actor attribution or malware analysis, might be limited or absent.
Lack of Contextualization: The raw data from CTI feeds might not be readily understandable for non-security experts. Tools might not provide enough context to interpret the threats and their relevance to the specific organization.
Language Barriers: Many threat intelligence feeds are in English. This can be a barrier for organizations in non-English speaking countries.
Limited Automation: Manual configuration and analysis can be time-consuming for resource-constrained SMEs.
Integration Challenges: Integrating threat intelligence tools with existing security solutions can be complex, requiring additional expertise.

- ## Potential for Improvement:

Enhanced Threat Analysis: Develop AI-powered features that can automatically analyze CTI feeds, identify potential threats, and prioritize them based on relevance to the organization.

Contextual Threat Intelligence: Provide easy-to-understand explanations of threats and their potential impact on the organization. This could include summaries, visualizations, and recommendations for mitigation actions.
Multilingual Support: Offer the tool interface and threat intelligence feeds in multiple languages to cater to a wider audience.
Automated Threat Response: Develop functionalities that can automatically trigger security measures based on incoming threat intelligence, such as blocking malicious IPs or quarantining infected files.
Simplified Integrations: Design tools with pre-built connectors to popular security platforms, allowing for seamless integration with minimal configuration.

Additional Considerations:

Cost-Effectiveness is Key: While STAXX is free, some advanced features in other tools might come with subscription fees. Developing cost-effective solutions with tiered pricing models could make these tools more accessible to budget-conscious SMEs.
Training and Support for All: Comprehensive training materials and readily available support resources are crucial. By empowering SMEs to understand and leverage threat intelligence effectively, we can significantly improve their overall cybersecurity posture.

Use Cases and Practical Applications (by Mitchell)

- **Relevant Scenarios for SMEs/developing economies:**
    - SMEs and developing economies often face resource constraints and may lack dedicated cybersecurity expertise. STAXX provides access to advanced threat intelligence capabilities without requiring significant additional investment in security infrastructure or specialized staff. Through its intuitive interface, comprehensive documentation, and support services, STAXX empowers SMEs to effectively detect, analyze, and respond to cyber threats with minimal technical expertise [7].

    - SMEs and developing economies are increasingly targeted by cyber-attacks due to perceived vulnerabilities and limited cybersecurity measures. STAXX enhances SMEs' cyber resilience by providing real-time threat intelligence data, actionable insights, and automated workflows to detect and mitigate cyber threats proactively. By leveraging STAXX's threat intelligence capabilities, SMEs can

stay ahead of emerging threats and better protect their sensitive data and systems [7].

- **Examples of Successful Use:**

    - Although direct examples of STAXX usage are unavailable, instances of STIX and TAXII implementation demonstrate their efficacy in addressing cybersecurity challenges. Notably, in a recent review, STIX and TAXII were instrumental in combating phishing attacks, showcasing their relevance and effectiveness in threat mitigation.
    - When a phishing attack occurs, a cyber threat analyst would scrutinize the suspicious email, assess attached files and links for potential threats, investigate if the email was distributed to others, analyze the common targets of the attack, ascertain if any malicious attachments were accessed or links followed, and document all analysis conducted [8].
    - In the event of a phishing attack, a cyber threat analyst extracts pertinent details (such as sender information, subject, embedded URLs, attachment types) from the email analysis. They identify the attack's tactics, techniques, and procedures (TTPs), correlate them with the kill chain model, assign confidence levels to indicators, devise handling protocols, create automated detection rules (e.g., Snort, YARA, OVAL), suggest response actions, and compile a comprehensive report for sharing and future use [8].

    - Upon confirming a phishing attack and identifying specific indicators, cyber decision-makers collaborate with operations personnel to comprehend the attack's impact, including any malware installations or executions. They evaluate the cost-effectiveness of response strategies and implement suitable preventive or detective measures to mitigate further risks [8].

Conclusion and Recommendations for Development (by mitchell)

- **Overall Suitability:**
    - STAXX, a free client application by Anomali, facilitates the collection and management of cyber threat intelligence (CTI) feeds, offering SMEs and organizations in developing economies an avenue to enhance their threat detection and prevention

capabilities without significant financial investment. The tool provides several key features, including access to free threat intelligence feeds, easy setup and navigation, powerful search and investigation functionalities, data sharing capabilities, and offline functionality.

- Regarding its suitability for SMEs in developing economies, STAXX offers numerous advantages. It connects to STIX/TAXII compatible feeds, providing access to valuable threat data without costly subscriptions. Its user-friendly interface and simple setup make it ideal for organizations with limited IT resources. Additionally, its offline functionality ensures continuous threat monitoring, even in areas with unreliable internet access.

- However, while STAXX addresses many challenges faced by SMEs and organizations in developing economies, some areas for improvement exist. These include limited threat analysis capabilities, lack of contextualization in threat data interpretation, potential language barriers, and integration challenges with existing security solutions.

- To determine whether STAXX is suitable for SMEs in developing economies, it's essential to consider its benefits in enhancing threat detection and prevention capabilities, its ease of use and accessibility, as well as its potential limitations and areas for improvement outlined in the assessment.

Recommendations for New Platform:

- To address the gaps and needs identified in the evaluation of STAXX and the requirements for Deakin Threat Mirror, several features and capabilities can be suggested:
- Develop AI-powered features to automatically analyze CTI feeds, identify potential threats, and prioritize them based on relevance to the organization. This would enable SMEs to gain actionable insights into emerging threats without requiring extensive manual analysis.
- Provide explanations that are easier to understand of threats and their potential impact on the organization. This could include summaries, visualizations, and recommendations for mitigation actions tailored to the organization's specific context and risk profile.
- Offer the platform interface and threat intelligence feeds in multiple languages to cater to a wider audience, including organizations in non-English speaking countries. This would help overcome language barriers and ensure accessibility for diverse user groups.
- Develop functionalities that can automatically trigger security measures based on incoming threat intelligence, such as blocking malicious IPs or quarantining infected files. This would enable proactive threat mitigation and reduce the manual effort required to respond to security incidents.

- Design the platform with pre-built connectors to popular security platforms, allowing for seamless integration with minimal configuration. This would streamline the deployment and operation of the platform within existing security infrastructures, reducing complexity and enhancing interoperability.
- Implement features that facilitate secure sharing of threat intelligence data among trusted partners and communities. This could include standardized data formats, secure communication protocols, and access controls to ensure confidentiality and integrity of shared information.
- Provide tools for organizations to define and automate threat intelligence workflows, including data collection, analysis, and response activities. This would allow organizations to tailor the platform to their specific requirements and operational processes, improving efficiency and effectiveness in managing cyber threats.
- Offer more in-depth training materials, documentation, and support resources to help users effectively leverage the platform's features and capabilities. This would empower organizations to maximize the value of the platform and enhance their cyber threat management capabilities over time.

Reference

[1] Hadi, H.J., Riaz, M.A., Abbas, Z. and Nisa, K.U. (2023). "Cyber Threat Intelligence Model: An Evaluation of Taxonomies and Sharing Platforms." In *Big Data Analytics and Intelligent Systems for Cyber Threat Intelligence*, pp. 3-33. River Publishers.
[2] Ramsdale, A., Shiaeles, S. and Kolokotronis, N. (2020). "A comparative analysis of cyber-threat intelligence sources, formats and languages." *Electronics*, 9(5), p.824.
[3] "STIX & TAXII," YouTube, Sep. 16, 2022. [Online]. Available: https://youtu.be/4ESCy5P5t3M. [Accessed: May 5, 2024].
[4] "IR 380: STIX Threat Intelligence (35 pts extra)," *SamsClass.info*, [Online]. Available: https://samsclass.info/152/proj/IR380.htm.[Accessed: May 5, 2024].
[5] "Anomali STAXX STIX TAXII Installation Tutorial," *YouTube*, Aug. 11, 2017. [Online]. Available: https://youtu.be/gowDFVc_5qU?si=DZ7A0OF3p_vAjfQW. [Accessed: May 5, 2024].
[6] "Structured Threat Information eXpression (STIX™)," [Online]. Available: https://makingsecuritymeasurable.mitre.org/docs/stix-intro-handout.pdf. [Accessed: May 5, 2024].
[7] Collins J (2023, October 17) *Opinion piece: Small business critical to cyber security strategy* [Website]. Available: https://ministers.treasury.gov.au/ministers/julie-collins-2022/articles/opinion-piece-small-business-critical-cyber-security-strategy#:~:text=In%20fact%2C%20the%20average%20cost,their%20vulnerability%20to%20cyber%20attacks.
[8] SOCRadar (2021, February 15) *What You Need to Know About STIX and TAXII?* [Website]. Available: https://socradar.io/what-you-need-to-know-about-stix-and-taxii/