TITLE: The importance of early detection of vulnerabilities and attacks for a healthy supply chain

Authors: Joao Costa, Jan Antič, Aleš Černivec, Lucija Korbar

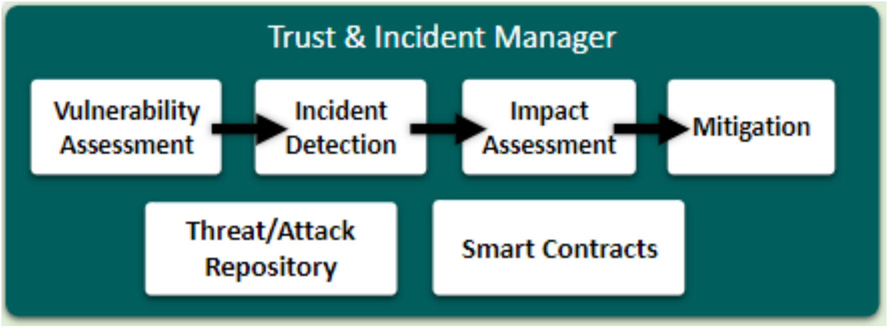
When addressing the resilience of supply chains in their complexity, a platform that provides vulnerability forecast, risk estimation and mitigation must consider the heterogeneous nature of supply chain infrastructures as an important driver of architectural design and exposing it as one of the Key Exploitable Results of the project. Its planned functionality includes monitoring and gathering metrics from supply chain infrastructure, performing analysis, raising alerts, and proposing mitigation actions. This innovative technology is addressing the problem of vulnerability assessment spread across several components and domains of different technologies, owned by different parties and with different objectives. This cannot be done in an individual way, but must cover all the different aspects and constraints together. Its architecture is being designed for supply chains, instead of a single network. It considers a combination of multiple different tools (vulnerability detection, IDS – intrusion detection system, SIEM – security information and event management, ...) to provide as wide of a coverage of cybersecurity as possible. It is integrating with the most popular infrastructure providers, such as cloud providers and container services, but also allows monitoring and management of bare-metal systems and IoT devices.

The Trust & Incident Manager (TIM) is a FISHY component that performs the analysis of metrics collected by the monitoring components of the FISHY platform. TIM is responsible for determining the vulnerabilities, detecting attacks and/or incidents and generating mitigating actions for the purpose of hardening the cybersecurity level of a monitored infrastructure. TIM is composed of several modules that facilitate its functionality, listed and briefly described below:

- **Vulnerability Assessment,** automated vulnerability and risk analysis, estimation and detection;
- **Incident detection,** detection of anomalous events from data gathered by monitoring, supported by ML methods;

- **Impact Assessment**, inferring the scope of possible damage (data loss/theft, service downtime…) posed by the vulnerabilities and incidents detected by the previous components;
- **Mitigation,** providing actions and recommendations for cybersecurity hardening and minimizing the scope of incidents;
- **Threat/Attack Repository,** storage for both incoming monitoring metrics and results of TIM analysis tools. By using a pub/sub layer over storage, the Threat/Attack Repository allows responsible components to have immediate access to new data for analysis and also serves as the integration point between TIM and other architectural blocks within FISHY;
- **Smart Contract,** manages service-level agreements and notifies stakeholders in case of violations and ensures the temporal succession of stored events.

The Vulnerability Assessment toolset contributed by XLAB is addressing the problem of the continuous detection of vulnerabilities in production infrastructures and during software development phases, appearing in the infrastructure when new services or features are added, or simply when new vulnerabilities are discovered in existing (outdated) services. It is solving this problem by continuously (according to a defined schedule) running vulnerability scans towards the monitored infrastructure, VAT (vulnerability assessment tool) can detect vulnerabilities and alert the administrators when they are discovered. It enables users to set up custom scans based on any user-provided script or by using the integrated vulnerability scanners to run the scanning tasks on-demand immediately or set up automatic repeated schedules, being alerted to new vulnerabilities discovered. It is highly customizable: new scanning tools can be easily integrated, user-provided scripts can be run using various interpreters, notification and alerting modules can be added. It can integrate into CI/CD flows or connect to existing tools (e.g. SIEM) with little effort.



On the other hand, XLAB is also contributing with detection and protection components, addressing problems related to the detection and protection components are detection of malicious activities on the network level within specific organisations using the detection and protection components that trigger specific actions. Our components will integrate with existing monitoring infrastructure provided by FISHY platform and will contribute security events that are not expected (as baseline) by the system defined or described within FISHY. Systems can be deployed on different target (also edge, light-weight) environments. Currently, the components can be installed independently and are running as self-contained systems, providing basic honeypot functionalities (SSH and Telnet honeypot logging brute force attacks and the shell interaction performed by an attacker).

In particular, the Wazuh[1] extensions that we are developing at FISHY are based on use cases' requirements and other functional requirements from technical partners. Wazuh will be further developed with additional/extended interfaces. The Intrusion and Detection Services, on the other hand, are a collection of containerized tools, such as honeypots (based on Cowrie), IDS (based on

[1] https://wazuh.com/

Suricata) and SIEM (based on Wazuh) that are used in the processes on threat detection, mitigation and certification assessment. Both of these will represent important contributions to the Open Source community under GPL2 licensing.

Besides the above-mentioned custom-built tools, XLAB is engaged in developing advanced anomaly detection solutions for log streams integrations, based on the enhanced monitoring and anomaly detection of log streams powered by AI. Applications such as security incident detection and prediction, failure detection, failure prediction and root cause analysis can benefit the efficiency of operations and reduced response times, optimizing the usage of resources. They provide a dynamic perspective to the vulnerability assessment using machine learning for anomaly detection on generated logs and building new security rules out of the gained knowledge in an automatic way. In that context, we are building a threat attack repository gathering this data in a standard way to build models and detect anomalies based on those models, providing integration with AI-based technology to gather the data appropriately.