

Product Requirements Document (PRD)

Product Name: SaPy

Coordination and Support: TuxAcademy (<https://tuxacademy.org>)

Ideazation and Product Delivery: Linux Mantra IT Services Pvt Ltd(<https://linuxmantra.com>)

SaPy is an advanced cybersecurity validation platform that empowers organisations to proactively identify and remediate vulnerabilities in their security infrastructure. By continuously simulating sophisticated, real-world cyber attacks, SaPy provides actionable insights into how security controls perform under pressure. Its automated adversarial testing and detailed traffic simulation help organisations uncover detection gaps, measure incident response effectiveness, and maintain a strong security posture against both known and emerging threats.

1. Product Overview

- SaPy harnesses state-of-the-art technology to deliver a robust cybersecurity platform centered on continuous adversarial testing. Through advanced traffic simulation, it emulates a wide range of attack techniques—including malware, phishing, lateral movement, and zero-day exploits—to comprehensively evaluate the resilience and responsiveness of security tools like IDS, IPS, WAF, and XDR. This enables organizations to identify weaknesses, optimize detection capabilities, and improve overall threat defense.
- Continuously evaluates an organization's security posture by subjecting systems to ongoing, real-world attack simulations. This approach ensures that vulnerabilities are promptly identified and addressed as new threats emerge.
- Thoroughly tests the effectiveness of various security technologies, including Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), Web Application Firewalls (WAF), and Extended Detection and Response (XDR) platforms, by exposing them to a variety of simulated attacks.
- Simulates a comprehensive range of attack patterns, replicating actual threat scenarios such as malware infections, phishing campaigns, privilege escalation, lateral movement, and advanced persistent threats (APTs) to assess organizational readiness.

2. Objectives

- Deploys an automated engine capable of generating and executing complex attack scenarios, reducing manual testing efforts and enabling scalable, repeatable security validation.
- Provides ongoing security validation by persistently challenging defenses and adapting to newly discovered vulnerabilities and evolving attack techniques.
- Offers deep visibility into detection gaps by highlighting points where current security controls fail to identify threats, enabling targeted improvements to threat detection capabilities.
- Utilizes artificial intelligence to generate novel attack methods and identify anomalous behaviors that standard rule-based systems may overlook, enhancing detection of sophisticated threats.
- Delivers comprehensive, customizable reports tailored for enterprise needs, including detailed analytics on simulation outcomes, detection rates, areas for improvement, and actionable recommendations.

3. Target Users

- Security teams within large organizations responsible for monitoring, defending, and improving their cybersecurity posture.
- Red teams and penetration testers tasked with emulating adversary tactics to uncover weaknesses and validate the effectiveness of existing defenses.
- Cloud operations and DevOps teams focused on securing cloud-native applications and infrastructure throughout the development and deployment lifecycle.

- Managed Security Service Providers (MSSPs) offering outsourced monitoring, threat detection, and incident response services to multiple clients.

4. Problem Statement

- Traditional security tools only respond to threats after they have occurred, leaving organizations exposed during the critical window between an attack and its detection. This reactive approach often allows attackers to exploit systems before defenses can be activated.
- Many organizations lack ongoing, automated security testing of their environments. Without continuous validation, new vulnerabilities or misconfigurations can go undetected, increasing the risk of successful cyberattacks.
- Existing solutions often provide only basic or narrowly-focused attack simulations, failing to cover the full spectrum of modern threats such as APTs, insider attacks, and multi-stage exploits. This limitation hinders comprehensive security assessment.
- Many current platforms offer basic or insufficient fuzz testing, which limits their ability to uncover unknown vulnerabilities in complex systems, protocols, and applications. This gap leaves organizations at risk from emerging, previously unidentified threats.

5. Solution

- SaPy continuously generates realistic, malicious network traffic to simulate a wide variety of cyberattacks. This persistent traffic flow exposes security controls to real-world attack conditions, ensuring ongoing validation of defense mechanisms.
- The platform orchestrates complex, multi-layer attack scenarios that mimic the tactics, techniques, and procedures (TTPs) of modern adversaries. These simulations span across different network layers and attack vectors, providing a holistic assessment of organizational defenses.
- SaPy leverages artificial intelligence and advanced fuzzing techniques to discover vulnerabilities that are not detectable by traditional methods. This combination enables the identification of novel attack paths and zero-day exploits, strengthening security posture against unknown threats.
- SaPy delivers immediate feedback on the effectiveness of security defenses by validating their performance in real time as simulated attacks take place. This allows for rapid remediation and continuous improvement of security measures.

6. Key Features

- The Traffic Generation Engine creates high-fidelity, customizable network traffic that mimics both benign and malicious behaviors. It supports diverse protocols and traffic patterns to stress-test security controls and uncover detection gaps in real-world conditions.
- The Attack Simulation Library contains a rich collection of pre-built, customizable attack scenarios covering a wide spectrum of threats, including malware, ransomware, phishing, insider attacks, and zero-day exploits. These simulations replicate adversary tactics to evaluate organisational resilience.
- The Fuzzing Engine systematically generates unexpected or malformed data to probe software, network protocols, and applications for vulnerabilities. Its advanced fuzzing capabilities help identify security flaws that conventional testing methods may miss.
- Scenario Orchestration enables the creation and management of complex, multi-stage attack campaigns. It allows users to combine different attack vectors, sequence actions, and automate adversarial testing workflows for comprehensive security validation.
- The AI Engine leverages machine learning and artificial intelligence to generate adaptive attack techniques, detect anomalous behaviours, and identify novel vulnerabilities. It enhances the platform's ability to challenge defences with unpredictable and sophisticated threats.
- Monitoring & Reporting
- API & Automation

7. Architecture

- **Scapy Engine:** This core component generates custom network packets and simulates both typical and malicious network traffic. It provides the foundation for realistic attack and traffic scenarios across a wide range of protocols.
- **Attack Modules:** Modular components designed to emulate diverse cyberattack techniques, such as malware delivery, phishing, privilege escalation, and lateral movement. These modules can be updated or extended to reflect new and emerging threats.
- **Fuzzing Engine:** An advanced system that systematically injects unexpected or malformed data into applications, services, and network protocols to uncover hidden security vulnerabilities that traditional testing methods may miss.
- **Orchestrator:** The control layer that manages and coordinates multi-stage attack scenarios, sequencing different simulation steps and ensuring the smooth execution of complex adversarial campaigns.
- **AI Engine:** Utilises machine learning and artificial intelligence to create adaptive attack strategies, detect anomalies during simulations, and identify vulnerabilities that require dynamic testing approaches.
- **Dashboard:** An interactive interface providing real-time monitoring, visualisation of simulation activities, performance metrics, and actionable insights for users to assess and improve their security posture.
- **API Gateway:** Facilitates seamless integration with external tools and workflows, enabling programmatic control, automated testing, and interoperability with enterprise security ecosystems.

8. User Flow

- **Define Simulation Parameters:** The user begins by selecting the target environment, specifying the systems, networks, or applications to be tested, and choosing the types of attacks or scenarios to simulate.
- **Configure and Launch Simulation:** Users customise the attack settings, such as attack vectors, intensity, and timing, then initiate the simulation to launch realistic adversarial activities against the specified targets.
- **Monitor Live Simulation:** During execution, users can monitor system behaviour and security control responses in real time via the dashboard, observing alerts, logs, and performance metrics as simulated attacks unfold.
- **Analyse Detailed Results:** After the simulation completes, the platform provides in-depth analytics, highlighting vulnerabilities discovered, detection gaps, and the effectiveness of security controls during each stage of the attack.
- **Generate Comprehensive Reports:** Users can generate and export detailed, actionable reports that summarise findings, outline remediation steps, and provide recommendations for improving the organisation's security posture.

9. KPIs

- **Detection Rate:** Measures the percentage of simulated attacks or threats that are successfully identified and flagged by the security controls during testing. A higher detection rate indicates stronger defensive capability.
- **Mean Time to Detect (MTTD):** Calculates the average time it takes for the platform to detect a security incident from the moment it begins. Lower MTTD signifies faster threat recognition and response.
- **False Negatives:** Tracks the number of attacks or threats that were missed or not detected by security systems during simulations. Fewer false negatives demonstrate more effective detection mechanisms.
- **Coverage:** Assesses the range and completeness of security validation by measuring the proportion of attack techniques, vectors, and scenarios tested against the organisation's environment.
- **Performance:** Evaluates the efficiency and resource utilisation of security controls and the SaPy platform during simulations, ensuring minimal impact on production systems while maintaining robust testing.

10. Uses for Compliance

- Authorised usage only
- ISO 27001

- SOC2
- DPDPA

11. Future Enhancements

- Autonomous red teaming
- Zero-day AI simulation
- Cloud attack modules

12. Timeline

100 Days

13. Skill Required

- Basics for Data Structures and Databases
- Python/Node/Java/Angular/ReactJS Programming
- Problem-solving approach