USE CASE/OPENAEV

Filigran

Intelligence-led Breach and Attack Simulation

With one click, OpenAEV empowers cybersecurity teams to operationalize threat intelligence from OpenCTI, automatically generating relevant simulation scenarios.

Filigran Capabilities

The synergy between OpenCTI and OpenAEV enables a comprehensive assessment of the readiness and effectiveness of all teams and stakeholders in responding to cyber incidents.

ATTACK SCENARIOS BASED ON LATEST AND GREATEST CTI

Threat intelligence on the growing number of cyber attack methods comes from a wide variety of sources such as OSINT feeds, commercial vendors and user generated data. OpenCTI automatically collects all of it and filters it to ensure that you have an up to date and relevant knowledge base to rely on.

OpenAEV can directly benefit from OpenCTI's curated intelligence thanks to a seamless and automated integration between the two platforms. Leveraging this synergy ensures that your security operations teams is building breach and attack simulations that reflect the reality of your organization's threat landscape.

RECURRING PAIN POINTS

UNINFORMED TESTING

Uninformed testing due to lacking relevant threat intelligence

OUTDATED SIMULATIONS

Rapidly evolving attack mechanisms and malware render simulations outdated or irrelevant quickly

TIME LOST

Manual scenario preparation is time-consuming

IRREGULAR TESTS

Unable to assess security posture on a regular basis

FREQUENT AND REPEATABLE SCENARIO EXECUTION

Frequent and highly relevant assessments are crucial for validating and maintaining an organization's security posture. However executing simulations is often considered an expensive activity due to the many hours of preparation required.

This pain and cost can be resolved thanks to the automated integration between OpenCTI and OpenAEV. In a matter of seconds, SecOps teams can transform the latest threat report into a full blown breach and attack scenario that replicates the latest methods used by threat actors and malware.

The injects and their timeline are all configured in a few clicks and their execution can be repeated as many times as necessary to assess your security controls appropriately.

CONFIRM PREVENTION AND DETECTION WITH TANGIBLE METRICS

One of SecOps main goals is to address the gaps in their security posture and this process is known as **Continuous Threat Exposure Management**. Every decision made is meant to reduce the impact of potential attacks, but to accurately assess the outcome of your actions, you need to measure your progress with relevant metrics.

OpenAEV provides these numbers to its users via its **Prevention, Detection and Human Response widgets**. These are automatically generated after every breach and attack simulation and are necessary to make informed adjustments to your security solutions and processes so that the scores of your future tests improve as expected.

Use case outcomes

OpenAEV enables security teams to validate the readiness and effectiveness of the organization's security posture regularly in three ways:

FACT-BASED CASES

Leverage your own threat intelligence directly from OpenCTI to create the most relevant simulations

AUTOMATICALLY GENERATED SCENARIOS

Save time by generating atomic testing in few click and delivering immediate results.

REPEATABLE COST-EFFECTIVE SIMULATIONS

Rerun the simulations as often as you want! to track your progress over time (every month, week, day!)