NEHEMIAH SECURITY

SOLUTION SHEET

EQ

Model and Predict Cyber Operations with Automation

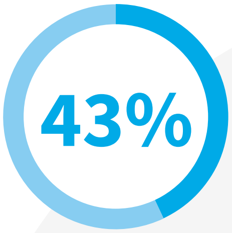
The Problem

With the rapid escalation of cyber threats, security leaders are under pressure to understand the strengths and weaknesses of their cyber defenses. This challenge is significantly magnified by the asynchronous and dynamic nature of threats. The best way to confidently understand and strengthen an environment's defenses is to test them against domain-specific attacks.

Many federal organizations and large enterprises must rely upon manual processes to configure and execute testing of their defenses. The problem is that these methods are time-consuming and not scalable. Without an automated solution, security teams lack sufficient resources to assess the effectiveness of their security defenses and to optimize their overall defensive posture.

> *"When designing armor, you have to understand what weapons your adversary is using to* **know whether your armor will actually withstand an attack***. This insight allows you to build a defense that can scale."*

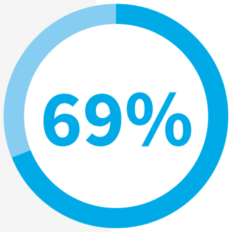
—Jason Syversen, CEO of Siege Technologies



of security operators do not / cannot measure their effectiveness[1]

$1.37 million

cost to organizations per year for time wasted responding to erroneous threat alerts[2]



of organizations say the process for capturing and analyzing intelligence is manual[1]

of the cyber data gathered can't be analyzed because security teams lack the resources[3]

[1] *SANS Institute. 2017. Future SOC: SANS 2017 Security Operations Center Survey*

[2] *Ponemon Institute. 2017. The Cost of Insecure Endpoints.*

[3] *Dark Reading. 2018. Security Automation: Time to Start Thinking More Strategically.*

A Cyber Quantification Framework

EQ leverages cyberwarfare tools to characterize and predict attack outcomes in a modeled environment. Through automation, this framework establishes scalable and repeatable testing to generate high-fidelity cyber data. Security teams leverage this functionality to perform “What if” scenarios, train security personnel, and strengthen defensive posture.

The EQ Philosophy: to ***experimentally validate*** *offensive intelligence to drive defensive advances*

EQ: How It Works

Experiment Modeling

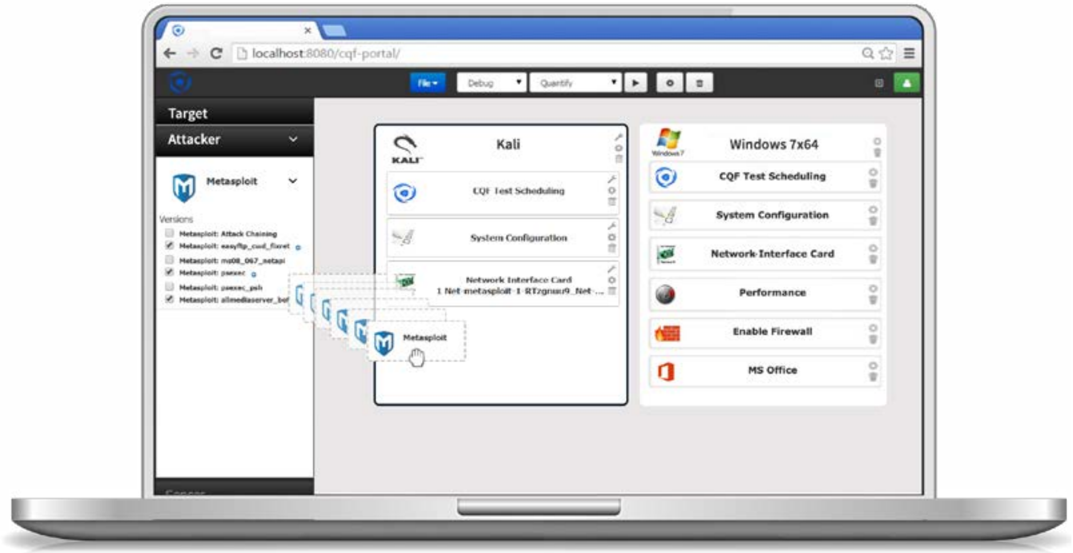
Engineer customized, large-scale tests in a configurable interface designed to abstract the complexities involved in the generation of intricate cyber environments. With this framework, experiments can be executed on virtualization servers. Automatically provision and test combinations of networked nodes, software configurations, attacks, and defenses.

Combinatorial Optimization

Utilize advanced mathematical algorithms to automatically generate test configurations and optimize experimentation. Pair combinatorial reduction with machine learning to enrich the fidelity and coverage of computed predictions. Reduce time needed by security operators to run a variety of experiments while increasing confidence in the results.

Data Collection and Analysis

Automatically process sensor data and calculate network-level metrics to evaluate the effectiveness of cyber defenses. Analyze results on the impact of various defensive solutions, software configurations, and security settings. Enable security teams with granular analyses to continually refine experiments and collect actionable data to strengthen resiliency.



About Nehemiah Security

Nehemiah Security works with enterprises around the world to elevate the security conversation and answer the question, “How does this impact my business?” Our mission is to empower security leaders to integrate their operations into the suite of functions corporations monitor and invest in every day.

Request a demo today. Call 571.321.5350 or email sales@nehemiahsecurity.com