DATA SHEET

Threat Simulator – Breach and Attack Simulation Platform

Continously Measure, Manage, and Improve your Cybersecurity Effectiveness

Problem: Underutilized Security Investments Due to Lack of Proper Security Metrics

With so many “bad guys” on outside trying to breach into your network, a multitude of insider threats and many emerging threats, there is no surprise organizations are facing the ideal conditions for a security breach. All those risk factors are combined with a big human element that assumes everything has been setup and configured properly to get the best outcomes from each security tool. So, the way usually organizations have responded to this problem was to throw more money at it, buying more new security tools increasing the management complexity.

But, the real problem behind all those things is that it has been extremely difficult to effectively measure your security posture. And when you can’t measure security, it becomes harder to manage and improve it.

The result is that you can’t quantify the risks to your business, or the return on your security investment, or understand how to optimize it.

Highlights

- Safe and cost-effective way to measure and validate your security effectiveness of your production network
- Patented recommendation engine provides clear, actionable insights on how to remediate identified gaps
- Enables you to perform automated breach and attack simulations on a regular basis
- Eliminates the assumptions that security controls are deployed and configured correctly
- Identify environment drifts
- Active validation of all phases of the Attack Life Cycle
- Reduces compliance audit time with data-driven evidence
- Prove security attacks are properly identified and reported
- Justify current and future IT spending
- Always up to date

Red Helix

KEYSIGHT TECHNOLOGIES

Solution: Proactive, Continous Security Validation

To ensure a strong defense, organizations need to embrace an offensive approach that employ breach and attack simulation software to continuously verify their Enterprise-wide security controls are working as expected and are optimized for maximum protection.

With Ixia's Threat Simulator, Enterprises can measure their security posture, gain insights into the effectiveness of their security tools and obtain actionable remediation steps to improve it.

With this data, you can start optimizing the existing security solutions so that you can improve your security without adding another expensive security solution.

Ixia Threat Simulator™ builds on 20+ years of leadership in network security testing to reveal your security exposure across public, private, and hybrid networks. The ongoing research of our Application and Threat Intelligence team ensures regular updates so you have access to the latest breach scenarios and threat simulations.

Key features

- Validation-as-a-Service through a Software-as-a-Service (SaaS) – consume it with your browser, no software to install, always up to date
- Offers a flexible cloud-based breach and attack simulation platform that scales as your network grow
- Actionable remediation recommendations help you improve and optimize your security controls
- Light, container-based software agents are infrastructure agnostic allowing operations on-premise, private and public clouds
- Minutes to the first security insight
- Fully managed "Dark Cloud" infrastructure to simulate external hackers, malicious hosts and C2C in the public domain
- It offers a modern, easy to use web-based interface
- Built-in integration with top network security controls and SIEM tools
- Diversified library of threat vectors, attack techniques and data exfiltration methods
- Out-of-box experience to simulate the full infection Killchain for popular breaches and APTs
- Scheduler to enable continuous security assessments across your Enterprise-wide network
- Elastically scales Threat Simulation agents
- SIEM-proxy agent facilitates communication with SIEM tools

- Built-in packet capture support
- Visual ladder diagrams complement the predefined security assessments
- Agent tagging supports user-provided metadata to each agent to better manage agents
- Agent grouping creates abstraction layers allowing simple and rapid validations of multiple network segments at once
- Flexibility to separate the control plane (management) and data plane interfaces, as an option

Product Capabilities

When it comes to network security, **your best defense is a good offense**. Ixia Threat Simulator™ is a breach and attack simulation platform that provides enterprise security teams with insights into the effectiveness of their security posture and actionable intelligence to improve it.

A cloud-native, serverless design

Ixia Threat Simulator is a completely cloud-based platform, delivered as a SaaS. At its core, it is an implicit microservices architecture orchestrated via APIs. This serverless design enables Threat Simulator to auto-scale on demand — eliminating the need for complex and costly data backhauls.

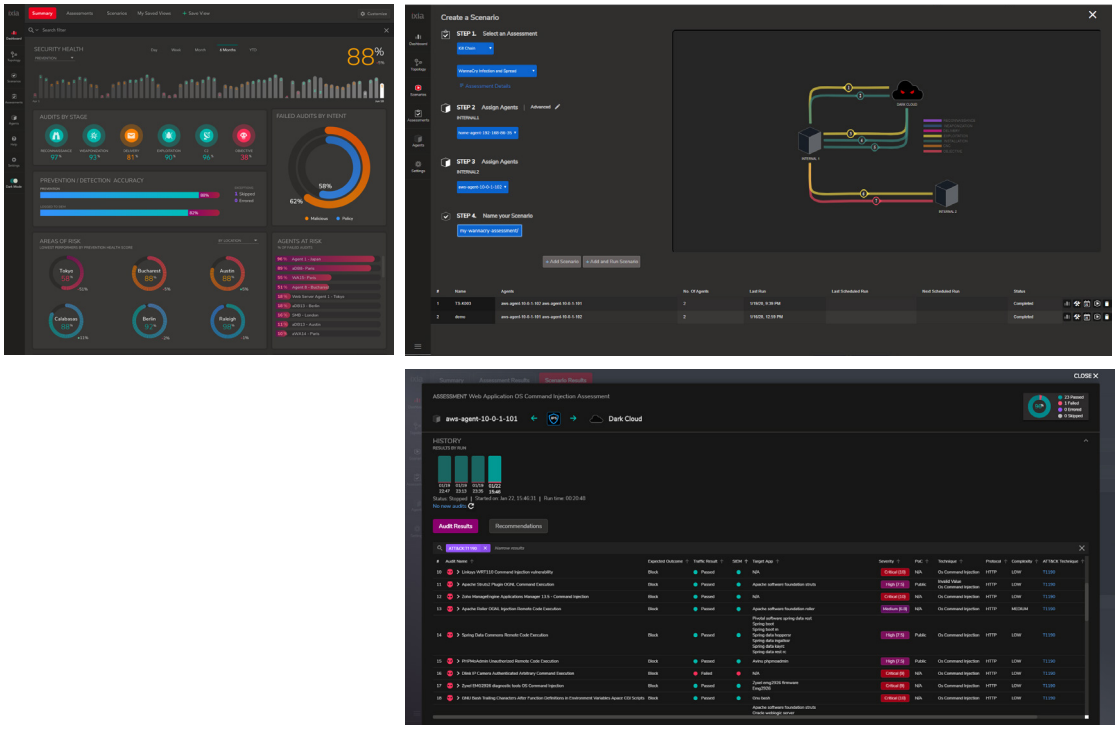
Delivered as a SaaS solution, Threat Simulator eliminates common anxieties with deployment, especially where network architectures are more complex. It offers a modern, simplified web user interface with great “out-of-the-box” experience.

Ixia Threat Simulator comprises three core components:

- A user-friendly web-based interface makes it easy to configure and run security assessment scenarios, identify drifts in your security posture and retrieve actionable remediations
- A “dark cloud” entity that spins up agents on demand to simulate threat actors in the public domain (e.g.: malicious websites, external hackers, C2C)
- Agents that are deployed on your Enterprise network; available in Docker-container format, they act as simulator “targets” or “attackers” inside your network, enabling safe, yet realistic attack and breach simulation scenarios (inside-to-outside, outside-to-inside and lateral movement)

Network security and enterprise tools ecosystem

Ixia's Threat Simulator has turnkey integrations with a large ecosystem of network security controls that makes it easy to get specific actionable recommendations to improve and manage your cybersecurity effectiveness. Integration with leading SIEM vendors enable end to end validation on how the prevention/detection works and identifies security sensors that may go dark. The bidirectional communication with the SIEM tools, provides the SOC team with push events that notify them during attack and breach simulations, so that they can quickly distinguish the simulated attacks from non-simulated ones.



Threat Simulator – Web User Interface (Dashboard, Scenario Builder, Detailed Results)

Specifications

Feature category	Feature
General features	• SaaS-based validation platform using safe attack and breach modeling that scales as your network grow • Modern, easy to use, web-based user interface • Actionable remediation recommendations help you improve and optimize your security controls • Prevention health score with historical trending to identify drift • Detection/Alerting health score with historical trending to identify drift • Distributed architecture with light software agents • Minutes to the first security insight • Built-in packet capture support • Topology viewer • Dashboards (Summary, Assessment, Scenario, Agents)
Attack and Breach Simulation	• Active validation of all phases of the **Attack Life Cycle** • Diversified and realistic library of techniques, threat vectors and kill chain modeling • Always safe – simulated attacks and breaches are only between Threat Simulator agents • Option to run attacks over encrypted or clear text • Security assessment for network security controls WAF, IDS/IPS, DLP, URL Filtering, Gateway Antivirus and Malware Sandbox • Active validation of both datacenter and perimeter-based security controls • IPv4 and IPv6 support
Threat Simulator Agent	• Light, container-based software agents require 1 vCPU, 512 MB RAM and 4 GB disk • Infrastructure agnostic allowing operations on-premise, private and public clouds • Runs on 32-bit or 64-bit x86 architectures • Flexibility to use a single interface for management/test traffic or dedicated test interfaces • Downloads and installs in < 2 min • IPv4 and IPv6 support

Specifications (Continued)

Feature category	Feature
SIEM Connector Agent	• Light, container-based software agents require 1 vCPU, 512 MB RAM and 4 GB disk • Runs on 32-bit or 64-bit x86 architectures • Downloads and installs in < 2 min • Acts as a proxy between the Threat Simulator SaaS backend and the SIEM tool • IPv4 and IPv6 support
SIEM Integrations	• IBM QRadar • Splunk
IDS/IPS Integrations	• CheckPoint Software • Cisco Systems (FirePower NGIPS, Cisco IOS IPS) • ForcePoint • Fortinet (Fortigate IPS) • IBM (Proventia IPS) • Juniper Networks (Juniper IDP) • McAfee (McAfee NSP) • Palo Alto Networks (Palo Alto IPS) • Snort • TrendMicro (TippingPoint ThreatProtection System) • Generic Vendor
WAF Integrations	• Akamai (Akamai WAF) • Amazon (Amazon WAF) • Barracuda (Barracuda WAF) • F5 (F5 BIG-IP ASM) • Fortinet (FortiWeb) • Imperva (Imperva WAF) • Microsoft (Azure WAF) • Radware (AppWall) • Rohde and Schwarz Cybersecurity (R&S WAF) • Trustwave (Core Rule Set) • Generic Vendor
GAV Integrations	• Fortinet (FortiClient) • Palo Alto Networks (Palo Alto NGFW)
Automation	Automation control with web-based API (RESTful API)
Availability	World-Wide

Ordering Info

Part number	Description
983-2011	IXIA, Threat Simulator BASIC BUNDLE (10 agents, 1-year subscription, SaaS) (982-2011)
983-2012	IXIA, Threat Simulator STANDARD BUNDLE (25 agents, 1-year subscription, SaaS) (982-2012)
983-2013	IXIA, Threat Simulator PLUS BUNDLE (50 agents, 1-year subscription, SaaS) (982-2013)
983-2014	IXIA, Threat Simulator PREMIUM BUNDLE (100 agents, 1-year subscription, SaaS) (983-2014)

Learn more at: www.redhelix.co.uk

For more information on Keysight Technologies' products, applications or services, please contact **Red Helix**

Red Helix

KEYSIGHT TECHNOLOGIES