pennAware

Email Threat Simulator

Email Threat Simulator

Challenge your existing email protection mechanisms to identify security vulnerabilities that will be exploited in an attack and automatically fix them.

NO SERVER CONFIGURATION!

NO INSTALLATION!

NO SPECIAL PERMISSIONS!

Over 90% of successful data breaches are initiated by an email-based attack. These attacks are costing businesses $3 trillion per year and drives considerable technological investments, such as firewalls and anti-spam, to provide protection.

The Email Threat Simulator (ETS) module from PennAware provides regular testing of this technology environment to find and automatically fix vulnerabilities & provide remediation services.

EMAIL THREAT SIMULATION WORKFLOW

ETS is integrated with industry-leading IOC and Exploitation Frameworks, as well as manual sources, to constantly maintain an up-to-date set of attack types.

Using simulation logic, we generate an attack that sends more than 240 known and current attack vector types including ransomware, browser exploits, malicious code and attachments and file format exploits to the test mailbox and check their status.

This methodology allows PennAware ETS to conduct

real-world tests for cyber-security risks, instead of monitoring traffic between the server and client which is insufficient for Antispam, Antivirus & Email services.

REPORT, REMEDIATION & AUTO-FIXING

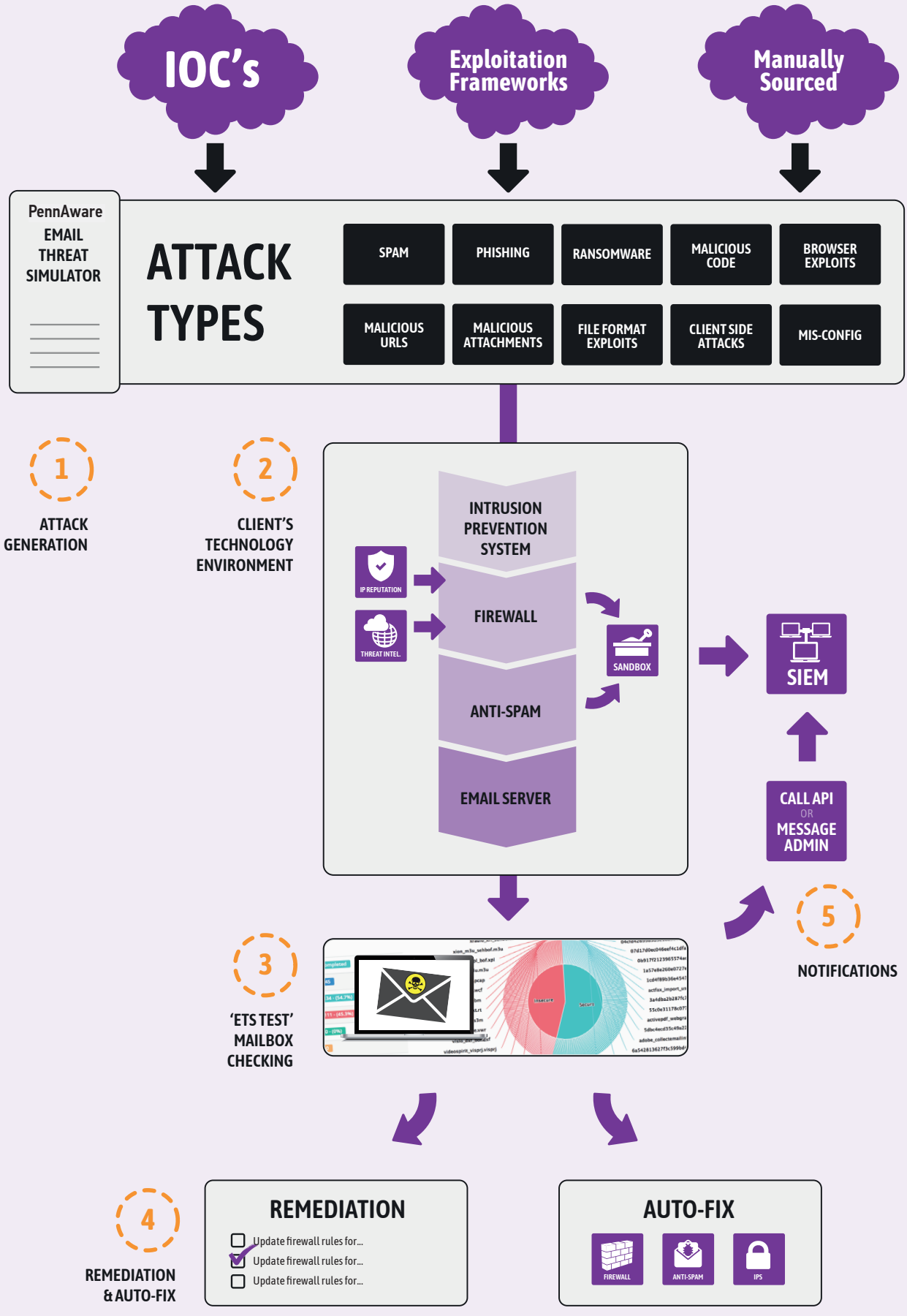
The report interface contains all the details of the simulation results. Successful attacks are reported as 'failed' and require immediate action.

PennAware ETS provides a list of remediation tasks necessary to remove vulnerability and our Auto-Fix features can automatically update the Firewall, Anti-Spam and Intrusion Prevention System (IPS).

ETS continues to generate attack simulations on a customisable schedule, and when new attack vectors are discovered, delivering a constant set of up-to-date results and providing useful guidance on additional measures of technological investment.

HOW IS PENNAWARE ETS DIFFERENT?

- Simple to configure and doesn't require any installation or complicated server-side setup
- Unlike known vulnerability scanning services, ETS tests missing/incorrect configuration options
- PennAware ETS provides 'real world' testing rather than testing active network devices by just moving traffic which is insufficient
- ETS reports intrusions via domain squatting and includes integrated cyber intelligence services.


IOC's
Exploitation Frameworks
Manually Sourced
PennAware EMAIL THREAT SIMULATOR
ATTACK TYPES
SPAM
PHISHING
RANSOMWARE
MALICIOUS CODE
BROWSER EXPLOITS
MALICIOUS URLS
MALICIOUS ATTACHMENTS
FILE FORMAT EXPLOITS
CLIENT SIDE ATTACKS
MIS-CONFIG
1
ATTACK GENERATION
2
CLIENT'S TECHNOLOGY ENVIRONMENT
INTRUSION PREVENTION SYSTEM
IP REPUTATION
THREAT INTEL
FIREWALL
SANDBOX
ANTI-SPAM
EMAIL SERVER
SIEM
CALL API OR MESSAGE ADMIN
5
NOTIFICATIONS
3
'ETS TEST' MAILBOX CHECKING
4
REMEDIATION & AUTO-FIX
REMEDIATION
Update firewall rules for...
Update firewall rules for...
Update firewall rules for...
AUTO-FIX
FIREWALL
ANTI-SPAM
IPS

Getting Started

- Create a test mail account – a test email address and password is all that is required for the service to work successfully. Alternatively use our browser plugin.
- Quick Scan option - with the one-click quick scan option attack vectors will be simulated in all categories.
- Advanced Scan option – with advanced scan you can configure profiles and create custom settings and schedules.

Arrange a free demo at www.pennaware.com

1 – Password is optional and ETS will operate without it. Providing a password allows PennAware ETS to automatically track the email status and generate reports

Powered by keepnet LABS

pennAware
www.pennaware.com