# SECURA PURPLEBOX

*Secura delivers world-class security test tools. Secura PurpleBox is a modular and secure test platform, enabling you to execute a number of simulated attacks, modeled after the MITRE ATT&CK Matrix for Enterprise. With this test tool, you can probe your Blue Team, SIEM or SOC detection capabilities.*

## THE CUTTING-EDGE SOC TEST TOOL

**Secura has worked in information security and privacy for nearly two decades. This is why we uniquely understand the challenges that you face like no one else and would be delighted to help you address your information security matters efficiently and thoroughly. We work in the areas of people, processes and technology. For our customers we offer a range of security testing products and services varying in depth and scope.**

### SECURA PURPLEBOX

Many organizations struggle with their SOC/SIEM security monitoring and detection systems. Initially, they generate a large number of alerts, or none at all. After fine tuning the use cases, it becomes more easy to manage and the number of false positives decreases. However, it is difficult to know if the systems are seeing the events you want to know about.

When a security operations center (SOC) does not alert you to any security events, it could be there is no security event taking place. It could also mean the SOC is malfunctioning or certain attacks are outside the detection capabilities. The Secura PurpleBox provides a test platform to continuously test and verify the functioning of the SOC and provides the trust that real events will not go unnoticed.

The Secura PurpleBox is a modular and secure test platform enabling you to execute a number of simulated attacks, modeled after the MITRE ATT&CK Matrix for Enterprise. The platform is designed such

that it can be easily connected into your network and run the attacks as an internal adversary. With this test tool, you can probe your Blue Team, SIEM or SOC detection capabilities.

The test platform stores the test execution details, which can later be correlated with the events detected by the SOC. The test platform allows you to continuously test and probe your SOC by periodically scheduling the supported attacks.

## HOW TO TRIGGER A SIEM?

SOCs and SIEMs get their security event information from various sources. The most important being:

- Syslog logging;
- Windows event log;
- IDS/IPS (via syslog or otherwise);
- Their own sensors;
- SNMP Traps;
- Local agents.

These events are generated from the PurpleBox. In order to play out SIEM use cases, the PurpleBox is able to provide simulated events via these channels. Examples of attacks that can be simulated are vulnerability scans, brute forcing, privilege escalation, malware behavior and application level attacks.

## FEATURES

- Easily configurable and connected to a network;
- 'Phone home': the ability to automatically and securely indicate where to access the test platform (e.g. the latest IP address);
- Provide command line, API and web-based access to configure, script and execute test runs. Each test run specifies which use cases are in scope as well as the list of 'targets'. This interface also allows to retrieve the test execution details;
- Schedule the execution of the test sets;
- Change identification details towards the network (e.g. hostname, MAC address);
- Encrypted storage of test results and recorded data;
- Optional 4G connection to allow external/out-of-band management;
- Remote update capabilities (triggered from client).

## BENEFITS

- Continuously Assess your detective capabilities by periodically testing of a Blue Team/SIEM/SOC solution;
- Accurate coverage of common and sophisticated attacks;
- Extensive automation ensures minimal operational effort.

## WHAT'S INSIDE

In order to do simulate cyber-attacks, the appliance contains an event engine, a Windows target system and a management interface. The event engine can send out various attacks, including attacks to the windows target system. This target system must be enrolled as a data source in the SOC/SIEM solution.

The simulated attacks are configured and matched to the use cases that must be detectable, but also contain scenario's that deviate from these use cases, because a real attack is not always going to follow a predefined use-case and you will also want to know about the detective capabilities of other cases or the newest attacks.

The simulated attacks are updated frequently by our team of specialists, who have extensive experience as penetration testers and Red Team members.

**INTERESTED?**

Would you like to learn more about our services?
Please do not hesitate to contact us.

Follow us on

Vestdijk 59
5611 CA Eindhoven
Netherlands

Karspeldreef 8
1101 CJ Amsterdam
Netherlands

**T** +31 (0)40 23 77 990
**E** info@secura.com
**W** www.secura.com