SECURA SIEM/SOC ASSESSMENT SERVICE

GET INSIGHT INTO YOUR SIEM/SOC DETECTION CAPABILITIES

How confident are you that your SIEM detects important security events?

Many organisations struggle with their SIEM/SOC security monitoring and detection systems. The initial setup is costly and difficult, while initially a large number of alerts is generated, or maybe none at all. After fine-tuning the use cases, it becomes easier to manage and the number of false positives decreases. However, it is difficult to know if the systems see 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 are no security events taking place. It could also mean the Security Incident Event Management (SIEM) solution is malfunctioning or certain attacks are outside the detection capabilities. In order to evaluate and test the detective capabilities of a SIEM, **Secura provides a test platform named PurpleBox to (continuously) test and verify the functioning of the SIEM and provides the assurance that actual threats will not go unnoticed.**

This test platform is offered as an integral part of the service. Based on your use cases, infrastructure and third party hard/software, our consultants will install, configure and tailor PurpleBox to your technology stack and requirements. Next, together with your team, Secura will execute the use cases one-by-one, store them in PurpleBox, and verify the alarms are correctly triggered in your SIEM/SOC. Any missing alert is analysed in detail by using PurpleBox to continuously execute a specific use case. **The PurpleBox service provides direct and actionable insight into your SIEM/SOC detection capabilities.**

The test platform stores the test execution results and allows documenting findings for later reference. All configured use cases can be re-executed at a later date, which optionally allows for continuous teste or automated periodic validation.

In order to do **simulate cyber attacks**, the PurpleBox 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 log data source in the SIEM/SOC solution.

The simulated attacks are configured and matched to the use cases that must be detectable, but also contain scenarios 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 can be updated frequently by our team of specialists, who have extensive experience as penetration testers and Red Team members.

How to trigger a SIEM use case without harming your infrastructure?

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

- **syslog logging** (e.g. from a Linux server, a message that a someone logged on);
- **Windows event log** (e.g. from a remote desktop server that a user entered an incorrect password);
- **IDS/IPS** (via syslog otherwise, e.g. indicating a connection to an IoC or C2 server on the internet);
- **SNMP Traps**;
- **local agents** such as EDR suites, Proxies, Virus Scanners.

To trigger use cases, Secura generates the log signatures of security events, pretending to originate from the sources listed above. In other words, **Secura simulates a security event happening inside your network, without actually performing the activity that would have normally raised that event.** PurpleBox uses (existing or newly created) hosts in your own network infrastructure that are enrolled in the SIEM for the event creation. On each of these test systems Secura installs the PurpleAgent that is controlled by PurpleBox to simulate arbitrary security events.

Features

- Service in which **Secura installs and configures PurpleBox** to assess your SIEMs detecting capability.
- **Interactive session with your Blue Team** to ensure all alarms are triggered correctly.
- Pinpoint possible issues in use cases that are not triggered with the ability to run arbitrary retests.
- Ability to **test use cases that are difficult to trigger manually** (e.g. infection with certain malware, adding someone as an admin on a corporate domain controller, lateral movement in network, privilege escalation attacks).
- **Test for realistic scenarios** like: “can we detect that latest malware infection other companies report?”.
- **Encrypted storage** of test results and recorded data.
- **Accurate coverage** of common and sophisticated attacks.

Benefits

- Provides **direct insight in SIEM detection capabilities** in an in-depth assessment.
- Interactive session with Secura experts **increases the insights of your Blue Team.**
- **Get the most value** out of your SIEM solution.
- Extensive automation ensures minimal operational effort.
- Resulting implementation optionally remains available as a regression test set that can be run independently at any time for a reassessment or periodically for continuous scans.

Secura

> More than 30% of the client's use cases did not result in an alert from their SIEM solution.

Case Study

Secura executed this service at a client in the financial sector with over 3000 employees. They run a world leading SIEM solution and contacted us because they had the feeling they were missing events and alerts.

Secura executed over 100 (of their 150) use cases in an interactive session by simulating the corresponding security events. **It was found that more than 30% of the use cases**, although the security event was registered correctly, **did not result in an alert**. During the sessions, we were able to pinpoint and fix the issues. The automated retest confirmed that the issues had been fixed correctly.

Interested?

Would you like to learn more about our services? Contact us today:

Follow us:

☎ +31 88 888 31 00

✉ info@secura.com

secura.com