RAISING YOUR CYBER RESILIENCE

Secura
A BUREAU VERITAS COMPANY

SIEM/SOC Assessment

Are your Security Operations Centre (SOC) and your Security Incident Event Management (SIEM) solution working as they should? Or is your detection missing threats? The SIEM/SOC Assessment tests this.

With the SIEM/SOC Assessment you can:

Verify your detection

Does your security monitoring and detection system detect actual threats? We help you check this.

Improve your detection rate

The assessment reduces the number of false positives that lead to genuine threats being overlooked.

Validate claims of your SOC

Do you have an external SOC provider? This assessment can validate claims they make.

Why choose the SIEM/SOC Assessment?

When your **Security Operations Centre (SOC)** does not alert you to any security events, you have no way of knowing what is happening. This poses a risk. It could be there are no security events taking place. It could also mean your **Security Incident Event Management (SIEM)** solution is malfunctioning. There could be all kinds of technical reasons for SIEM/SOC malfunctioning, but the result is the same. Your analysts are effectively blindfolded and groping in the dark.

There is only one way to verify if your detection is working as it should, and that is to test it. Our Red Team members and pentesters know exactly how to mimic adversarial behavior, and can use these skills to challenge and test your SOC and your SIEM solution. The SIEM/SOC Assessment helps you to strike the right balance between sensitivity (catching every possible threat) and specificity (avoiding false alarms). Let us help you improve your detection.

How the SIEM/SOC Assessment works:

Detection: 'use cases'

Detection relies on use cases to find relevant anomalies. A use case could be: 'alert us when a large amount of data is transferred outside of office hours.' These rules are meant to detect typical adversarial behavior.

Executing use cases

To test your capabilities, our experts execute use cases one-by-one. To do this, we simulate a security event happening inside your network, often without actually performing the activity that would have normally raised that event. This could be for instance by sending attack signatures over the network, or by performing suspicious actions on servers.

Are the alerts triggered?

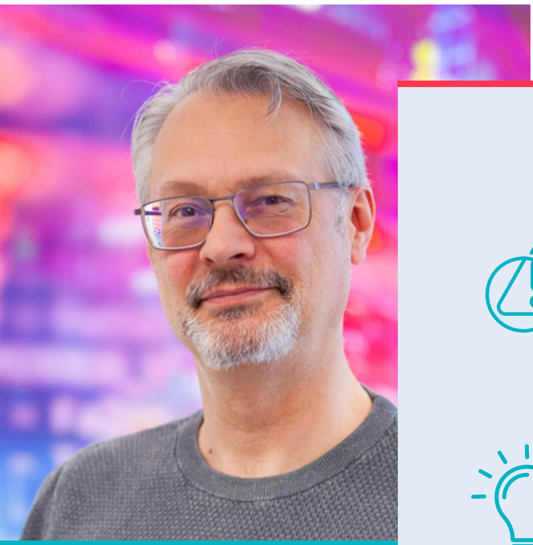
Together with your team or your provider's team, we verify that the alerts are correctly triggered. Any missing alert is analyzed in detail and a root cause is determined if possible. This information can help you significantly improve your detection.

Secura
A BUREAU VERITAS COMPANY

About Secura / Bureau Veritas

Secura is a leading cybersecurity company. We help customers all over Europe to raise their cyber resilience. Our customers range from government and healthcare to finance and industry. We offer technical services, such as vulnerability assessments, penetration testing and red teaming, but also provide audits, forensic services and awareness training.

Secura is a Bureau Veritas company. Bureau Veritas (BV) is a publicly listed company specialized in testing, inspection and certification. BV was founded in 1828, has over 80.000 employees and is active in 140 countries.



Example case | SIEM/SOC Assessment

What problem did the customer have?

A client in the Dutch public sector use a third party detection provider. They contacted us because they had a feeling they were missing events and alerts.

Result

During the SIEM/SOC Assessment we found that only 30% of TTPs covered by the client's use cases were actually detected, even though the related security events were registered correctly. Many critical TTPs were not detected at all. We were able to pinpoint and fix many of the issues together with the SOC team. The client's detection capabilities were dramatically improved.

BUREAU VERITAS 1828

Interested?

Contact us today to start raising your cyber resilience.

✉ info@secura.com

☎ +31 (0) 88 888 3100

secura.com