November 16, 2017 – Company announcement

Press Officer:
Petra Sauer-Wolfgramm

Phone: +49 (0)4 31 / 39 93 - 525
Fax: +49 (0)4 31 / 39 93 - 999
E-mail: sauer-wolfgramm@consist.de

Security Information and Event Management: cost and benefit aspects

Is IT security without a SIEM still a valid option?

Kiel – IT security is a must. Every company understands this much. But that leaves the question of how to get to a suitable level of security? What's too much? What's not enough? Security information and event management (SIEM) systems are often cited in the context of a security strategy. At the SIEM workshop by Consist Software Solutions GmbH at this year's Rethink! Security in Hamburg, questions arose about how much sense SIEM makes and at what point its use actually pays off for a company.

Does every company need a SIEM?

IT security always likes to be determined at the technical component level: firewalls, intrusion detection, vulnerability scanners, virus scanners, anti-virus software, web filters. But security concepts also always have to involve processes and people for them to work. Without a doubt, a SIEM system can provide a high level of transparency about activities on the systems used. You can see at a glance where security-critical activities are taking place, trace them, document their processing, and get reports on the current situation: in today's complex system environments, that's a real help. In this context, the question that confronts companies is "Do I need a SIEM, and if so, what type?"

Consist Software Solutions GmbH
A Consist World Group Company

Falklandstrasse 1-3, 24159 Kiel, Germany
P.O. Box 93 28, 24152 Kiel, Germany

Press Contact:
Petra Sauer-Wolfgramm

Phone: +49 (0)4 31 / 39 93 - 525
Fax: +49 (0)4 31 / 39 93 - 999
E-mail: sauer-wolfgramm@consist.de
Internet: www.consist.de/www/en/press

Company location: Kiel
HRB Kiel No. 3983

Management:
Daniel Ries
Martin Lochte-Holtgreven

Threat

That depends on the threat situation and the evidentiary requirements imposed by legal regulations. Nearly 100% of all attacks are carried out with valid access data. On average, 40 IT systems are affected. Even more astoundingly, attacks are only discovered after an average of over 200 days, and the first notice of compromise comes from third parties in 67% of cases. The continuous monitoring of system accesses and data flows in your own IT is a key factor in detecting attacks or bad behavior by users (insider threats) quickly and handling them.

Simplification

To a certain degree, this kind of monitoring can be implemented using central log and permission management. For larger system landscapes, however, you should ask yourself whether automated processes wouldn't be more cost-effective, since they allow a reduction in manual checks. If a SIEM is used, IT security only needs to worry about suspicious cases (incidents) and can even investigate them directly in the SIEM.

Legal compliance

It may not be possible to meet legal requirements without a SIEM. The IT security laws still don't mandate one, but no later than the implementation of the EU General Data Protection Regulation in May of 2018, and especially for KRITIS companies, it will be difficult to comply with the increased requirements without automating the detection and notification processes. The monitoring of activities in compliance with both labor and data protection law is possible with a SIEM, since alarms for security incidents only take place when normal IT system usage is violated.

With a SIEM it is significantly easier to maintain transparency. The options for clarifying security incidents are more versatile and easier to manage. Modern methods like machine learning, user behavior analysis or threat lists provided by a SIEM make it possible to specifically generate incidents (alarms) on deviations and outliers. Less rule maintenance and fewer false alarms are the pleasant consequences.

This press release contains 3.208 characters (including spaces), with an average of 61 characters per line.

You can also find it at www.consist.de/presse

More information:

- About Consist: www.consist.de
- About SIEM: www.consist.de/en/products/compliance_security/splunk/

Company Portrait

Consist Software Solutions GmbH is a specialist in IT services and software. The IT service provider supports its customers throughout the entire software lifecycle, from development projects to maintenance in the operating phase, to supplementary big data and security products.

Projekte
Plan & Build
Managed Services
Run
Software
Produkte
Innovate

With more than 180 employees at the sites in Kiel, Berlin and Frankfurt, Consist is setting the benchmark for data analytics, IT security and managed services.

Founded in 1994 at the Kiel headquarters, the company continues its growth path, which makes Consist one of the most experienced IT service providers, thanks to proven mainframe competence and highly qualified specialists for innovative technologies. Awarded with the „Großer Preis des Mittelstandes" Consist again received the plaque of honor in 2016.

IT that works.

Year of founding:	1983 profit center of Krupp MAK 1994 spin-off under the name Mak DATA SYSTEM Kiel GmbH
Managing Directors:	Martin Lochte-Holtgreven, Daniel Ries
Sales, employees:	26 Mio. € (2016), 190 employees (01/01/2017)
Locations:	Kiel, Berlin, Frankfurt (Main), Braunschweig
Subsidiaries:	Consist ITU Environmental Software GmbH, Hamburg TeamWork GmbH, Kiel

Consist Software Solutions GmbH
A Consist World Group Company

Falklandstrasse 1-3, 24159 Kiel, Germany
P.O. Box 93 28, 24152 Kiel, Germany

Press Contact:
Petra Sauer-Wolfgramm

Phone: +49 (0)4 31 / 39 93 - 525
Fax: +49 (0)4 31 / 39 93 - 999
E-mail: sauer-wolfgramm@consist.de
Internet: www.consist.de/www/en/press

Company location: Kiel
HRB Kiel No. 3983

Management:
Daniel Ries
Martin Lochte-Holtgreven