EUROPE SPECIAL

ENTERPRISE SECURITY

WWW.ENTERPRISESECURITYMAG.COM

JULY - 2020

SIEM

EDITION

SECUINFRA

Maximizing the Utility of Next-Gen SIEM

Ramon Weil,
CEO and Founder

$15

SECUINFRA

Maximizing the Utility of Next-Gen SIEM

Every company, no matter the industry, either grazes or dives deep into the sphere of mission-critical information technology, invariably increasing the need for best-in-class information security tools. Even some of the most versatile information security tools prove insufficient when IT infrastructures are hacked, and there lies valid reasoning behind this conundrum. In most cases, the weakest link in IT security is the human mind, and the heuristic approaches it takes in operating these tools. While heuristics contribute majorly to why we are quick and efficient in terms of cognition, it sometimes leads to erroneous decisions that seem easily avoidable in retrospect.

Considering even the best SIEM tools on the market in 2020, one cannot expect the tool itself to detect, escalate, and remove known threats, despite its vastness and sophistication. The success or failure of such best-in-class tools depends almost entirely on the operator's know-how and analytical prowess, as the tool is only a means of achieving the said objectives.

And thus, in 2005—as SIEM entered mainstream IT—organizations were on the lookout for professionals who could better comprehend and leverage the value of this reasonably new digital security technology. While "security by obscurity" may have offered some value, it was often outweighed by the vulnerabilities associated with taking a non-standard approach. These firms required new tools and algorithms that were rigorously vetted by experts if they were to stay afloat in their markets.

Ramon Weil noticed opportunities in this demand for SIEM experts that the supply could not meet. He brought together certified experts with knowledge of relevant SIEM products to

ENTERPRISE SECURITY TOP 10

SIEM

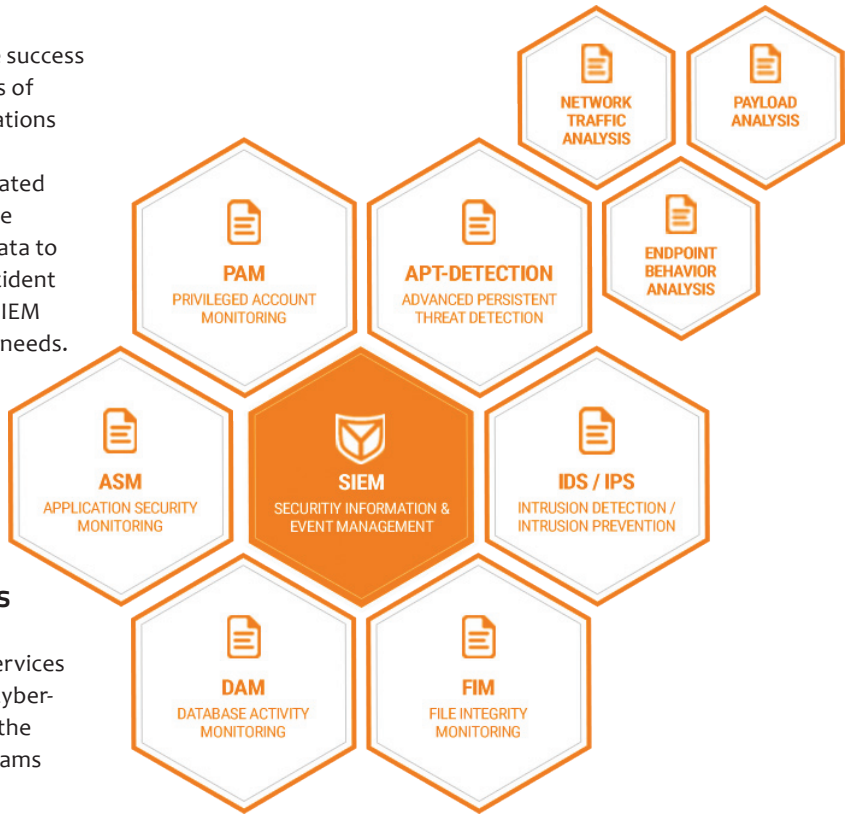
CONSULTING/SERVICE COMPANIES IN EUROPE 2020

> Our entire cyber defense service portfolio has a modular structure, which can be adapted to meet virtually any customer requirement

Ramon Weil,
CEO and Founder

combat prevalent security issues among clients. The success of this team would soon go on to lay the foundations of SECUINFRA—a digital fortress born to help organizations detect, analyze and defend against cyber-attacks.

The German cyber defense organization was created with the singular focus of spanning the industry-wide expertise gap in collecting, logging, and analyzing data to provide threat monitoring, event correlation and incident response functions with the delivery of end to end SIEM services and solutions, tailored to various customer needs. The past decade alone showcases a rich history where SECUINFRA worked with multiple clients in operating leading SIEM products such as ArcSight, Splunk, QRadar, Elastic, and developing use-cases, while molding a strategy that solves clients' security issues.



Expelling Threats via Intelligent Analysis

While adapting to newer trends in IT becomes more mission-critical with each passing day, using cloud services leave data structures more open and vulnerable to cyber-attacks. A persistent hacker can and will sneak past the company's defenses and latch their malignant programs onto the company's IT framework.

"The question is not *if* the company becomes compromised, but rather *when* does it get compromised? And sometimes, *since when* has it been compromised?" begins Ramon Weil, Founder and CEO of SECUINFRA. The cybersecurity experts at SECUINFRA help their customers employ suitable SIEM tools to detect and identify compromised infrastructures as quickly as possible to minimize organizational damage.

The company ensures that clients are never overwhelmed with multiple security alarms going off simultaneously in the eventuality of a cyber-attack. Instead, it analyzes cyber-attacks and compliance violations in detail and informs clients about the outcome of its analysis.

Since an attack sets off constant alarms that may disorient the IT team, SECUINFRA employs a status based SIEM approach when tackling such issues. When faced with such an eventuality, the attack is detected and analyzed by the organization such that only a minimal number of networks that display status changes are under scrutiny rather than the whole infrastructure. Paying heed to system statuses rather than single alarms can narrow down the list of systems suspected to be compromised. This is especially convenient when identifying the ones that have covered tunnels connected to the command control centre, or have multiple unsupervised accounts that touch confidential data created on them. "We combine all status changes with involved systems and accounts into one visualized overview per customer," iterates Weil.

At this juncture, a crucial question arises: How does this visualized overview prove beneficial?

Though a SIEM tool is excellent in detecting single misbehavior within the IT framework, the human mind excels in spotting patterns among these anomalies. SECUINFRA, with its SIEM Use-Case Framework (status change approach), prepares data in a way that the humans behind the screens can easily decode these connections. By carefully peering into and analyzing the client's IT system, and providing the appropriate use-cases from its library, SECUINFRA's innovative approach aims to return no false negatives and a maximum of only one false positive per week. Working alongside the client, SECUINFRA then gives out clear instructions for handling the situation and expelling the attacker from all affected systems, all the while supporting the client with the company's vast portfolio of modular, hybrid cyber defense services.

Data Management Is Key in Customer Synergy

When partnered with SECUINFRA, the client always has the last word when it comes to data management; all the relevant intelligence stays with the client, even post-engagement. This approach is in stark contrast with the traditional interaction between a SIEM provider and a client, where the latter faces a risk of losing sensitive data once

the partnership concludes. Such an ideology is reflected in SECUINFRA's Co-Managed SIEM service portfolio, where the firm's services amalgamate modularity, flexibility, and hybridization. "Our entire cyber defense service portfolio has a modular structure, which can be adapted to meet virtually any customer requirement," states Weil when discussing the company's stance on client engagement. A typical engagement begins with a two-day workshop where clients get an ideal comprehension of SIEM to understand what is possible with SIEM, and what is better handled by another security technology. The next stage of SIEM consulting, which takes around twenty days, involves collaborating with the client to discern their goals, requirements, framework conditions, and the current cyber defense maturity level. Upon defining appropriate SIEM log sources, use-cases, and the planned mode of operation, SECUINFRA's team of cyber defense architects draws upon their vast experience to provide the most appropriate SIEM product to meet their needs.

"SIEM demands end to end intelligence insight. Where there are no data, there's no detection of attacks," notes Weil. SECUINFRA's use-cases encompass the generation, flow, and interpretation of data from an attack. Adhering to audit log policies, the company provides its clients with appropriate log sources to detect and generate the necessary data, which then flows into the SIEM to be interpreted. With the right data available, the company's use case developer brings the much-needed "intelligence" into the SIEM.

This approach refers to defining and implementing algorithms based on the data to detect irregularities in the system. If log sources are not supported by default, SECUINFRA develops suitable connectors for the client. The development of these connectors requires specialist knowledge, and above all, much experience—both of which are readily available with the German SIEM service provider.

Reliable and efficient SOCs and CDCs

When the company was founded in 2010, it was focused purely on delivering SIEM services. However, after a few years, it was approached by a client from the financial sector who was at a crossroads of setting up a Security Operation Center (SOC) themselves or purchasing managed SIEM externally. With a team of veterans specializing in digital security, SECUINFRA formulated a simple, yet brilliant solution—a Cyber Defense Center (CDC) that could provide the best of both worlds to its client. "Setting up and operating SOCs and CDCs are our core competencies," adds Weil. Not only are the defense centers compliant with the stringent data protection laws of the GDPR but are also efficient in increasing or reducing resources based on the customers' needs. The company's hybrid services also give customers the leeway to decide the services to be provided on-premise and the ones that need to be provided remotely from the security company's Cyber Defense Centers in Frankfurt and Berlin.

One of the company's largest customers has over a billion security events coming in each day through their IT services. Although they do not regard SIEM as a core selling point, it is nevertheless required of them to offer managed SIEM while outsourcing projects. In SECUINFRA, however, they have found a reliable partner that has garnered expert knowledge, while being capable of providing unmatched professional support in the field of SIEM.

> We combine all status changes with involved systems and accounts into one visualized overview per customer

The Secret Sauce to Satisfied Clientele

"Our three values are trust, reliability, and loyalty. These values are the guidelines for our relationships among employees and with customers alike," says Weil. This philosophy has borne its fruits in the organization. With a loyal workforce, SECUINFRA has a low churn rate of cyber defense experts. They stay and gain expert knowledge over time, and grow from level 1 analysts to level 2 analysts to incident responders and forensic experts.

The clients—the backbone of SECUINFRA's success—are supported by a team of experts whose skills are unrivalled in their areas of specialty. The company's farsighted vision in prioritizing the creation of a stable, reliable relationship with its customers over tacky, aggressive sales techniques has always ensured maximum transparency and flexibility in its operations.

Starting right at educational workshops, moving on to product-neutral SIEM consulting, and designing its product independent Use-Case library based on SIGMA, SECUINFRA has stayed true on its course of providing exceptional SIEM services. Weil and his team aim to broaden the company's service horizons by adding complementary services and solutions such as Endpoint Detection & Response (EDR) and behavior-based analytics to detect better, analyze, and defend against cyber-attacks. Not resting on its laurels, SECUINFRA aims to expand its services outside Germany and Europe to the Middle East and Southeast Asia. ES