RADAR SERVICES

Security Information & Event Management (SIEM)

DATASHEET

SIEM in a nutshell

The variety of cyber-attacks is extraordinarily large. Phishing, DDoS attacks in combination with ransomware demanding bitcoins or other cryptocurrencies to release the hacked system, exploitation of the maintenance access in almost real time, protracted profiling of employees' electronical behavior, and spying on vulnerabilities in the IT are just few examples of jeopardizing maneuvers for companies.

Such a variety requires efficient and advanced tools to detect attacks in a valuable manner, and that is what Security Information & Event Management (SIEM) is made for.

SIEM is one of the pillars in the field of IT risk detection: it represents the aggregation layer for different types of information, resulting from the IT of a customer and from the Radar risk detection modules. SIEM focuses on the collection and the analysis of logs from various sources within a network (e.g. server, clients, network devices, firewalls, applications) from the cloud environment with a clear aim, that is, to distinguish security-relevant events from other log data and to inform promptly in case of security flaws or potential risks.

Highlights of the RadarServices SIEM

RadarServices SIEM monitors logs across the IT infrastructure in the customer's environment. In detail,

1. Data collection

A highly scalable database captures real-time log events and network flow data. Using the most up-to-date technologies RadarServices' SIEM manages various common log formats as well as custom logs. The sources of such logs are:

- **Security events**: Events from firewalls, virtual private networks, intrusion detection systems, intrusion prevention systems etc.
- **Network events**: Events from switches, routers, servers, hosts etc.
- **Network activity context**: Layer 7 application context from network and application traffic.
- **User or asset context**: Contextual data from identity and access management products, vulnerability scanners etc.
- **Application logs**: Enterprise resource planning (ERP), workflow, application databases, management platforms etc.
- **Operating system information**: Vendor name and version number specifics for each network asset.

2. Processing

Log data from thousands of devices distributed across a network are aggregated and stored in their raw form. Then, they are categorized and normalized, so that the information of differently encoded log formats can be processed in the same way and further enriched. In this way, events that require further investigation or a prompt response are quickly identified.

3. Enrichment

Contextual information makes more effective the limited details of an event or a log. Therefore, information about user, asset and network is added to ease the comprehension of the consequences of an event. In this way, an improved situational and content awareness supports the decision-making process and accelerate the remediation measures.

4. Storage

A twofold strategy governs the data storage. At first (about 24 hours), the logs are stored on very fast PCI SSDs (the fastest SSD available at the moment) for the data processing, which guarantees high-performances. After that they are transferred to SATA HHDs (which perform slower) and they are still accessible for analyses. The usual storage time for log data is 3 months, but can be extended upon request.

5. Analysis

The RadarServices' Advanced Correlation Engine uses the normalized and enriched logs as input for the real-time analysis. This component comprises predefined and customized rules, policies and machine learning algorithms, so that the analyst can perform an in-depth analysis to detect false positives, anomalies and real alerts. Real-time Layer 4 network flow data and Layer 7 application payloads are captured by using deep packet inspection technology.

An interactive and user-friendly interface permits to visualize and investigate the events. In particular, the analyst can classify and rank alerts of anomalous patterns to highlight the actual attacks.

6. Collection

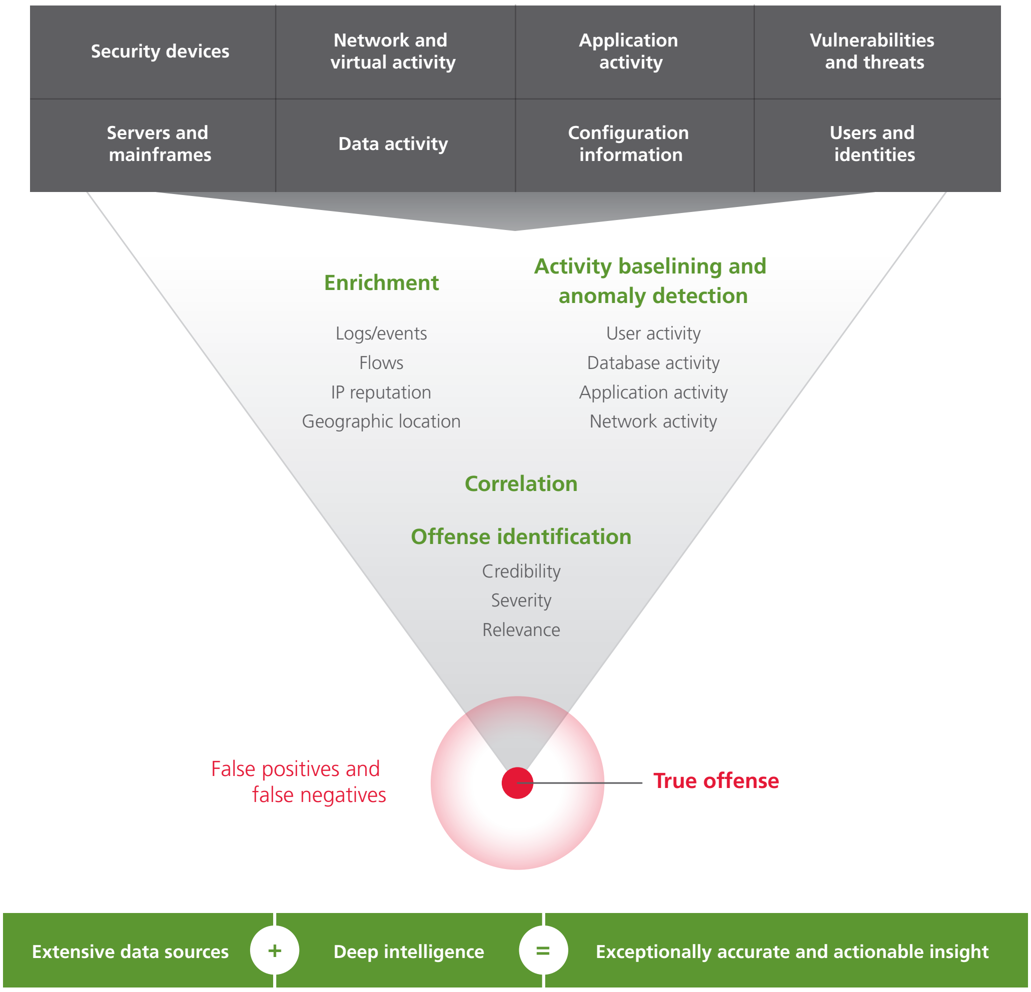
Machine Learning (ML) is crucial for processing drastically increasing amounts of input-data with a pre-defined set of Use Case Rules. Depending on the use case, the resulting events can be automatically delivered as incidents or presented to the SIEM-operator for further analysis. The Advanced Correlation Engine contains different ML algorithms such as Limit Learner (outlier-detection), Markov Learner, Zero-Variance Learner.

7. Aggregation and Correlation

The RadarServices Advanced Correlation Engine is able to analyze large volumes of event data. It comprises four correlation types, including rule-based, risk-based, standard deviation, and historical analysis. In this way, the Correlation Engine provides a real-time view of a broad spectrum of threats which may affect high-value assets. Moreover, preloaded correlation rules and dashboards allow to easily customize the existing rules according to the customer needs.

8. Alerting & Delivery to the Risk & Security Cockpit and customized result presentation

The RadarServices' Risk & Security Cockpit (RSC) is the reference point for risk and security information. It provides reports and statistics with various levels of details. Possible risks, security flaws and customizable events raise an alert which is immediately shown in the Cockpit and upon request it is forwarded to the customer via email or mobile phone. Moreover, the workflow framework included in the RSC allows an easy case management and the integration of customer processes and systems. Thus, any user can intuitively investigate the suspected incidents and make promptly the most suitable decision.



Conclusion

Out of millions of events RadarServices effectively and efficiently identifies those, which indicate

- abuse of IT and applications,
- attacks,
- internal fraud or
- other security threats.

What we offer

RadarServices offers the SIEM risk detection module as a stand-alone solution, in combination with other modules and together with the Radar Risk & Security Intelligence Team (RSI Team) in the form of a managed service.
Using its extensive experience, the RSI Team aggregates, inspects and analyzes the data collected by automated monitoring and detection modules to properly face risk and security information – with a particular focus on critical businesses and urgent responses. This approach allows to exclude false positives and false negatives and ultimately reduces the number of events reported to the customer.
The RSI Team reviews and correlates thousands of incidents daily; then, the findings are used to continuously enhance policies and rules of the automated correlation and risk detection. The Technical Writing Team enriches the findings description with clear and detailed instructions for mitigation and possible solution of the issue. Thus, RadarServices directly supports the IT risk management process in the customer's organization and contributes to continuous and always up-to-date risk evaluation. As a matter of fact, given the deep expertise of each team component in security audit, penetration testing, white-hat hacking and social engineering, the RSI Team plays the dual role of guide for the IT operations and advisor for strategic decisions.
Customers that turn to RadarServices during or after an attack on their IT, find the right expertise for firefighting and forensics on demand. Therefore, the RSI Team has also the competences to entirely support you as an external CERT team.

What we are proud to offer you

Recognized, classified and prioritized security flaws: Security flaws, possible risks and any information that needs an urgent response raise an alert which is immediately shown in the Cockpit and upon request immediately forwarded to you via email or mobile phone.

A complete incident workflow: The overall risk remediation workflow and the messaging/feedback system for the communication with the RIS Team allows an easy and effective coordination between you and us.

The possibility to automatically assign users to user groups (teams) as well as to dispatch incidents: Asset management functionalities provide an overview about what is really running in the network, from perimeter and corporate network to virtualized machines and cloud services. Assets are tagged according to a wide range of attributes such as network address, open ports, OS, installed software, found vulnerabilities to allow automatic selection of hosts for scanning or reporting. In fact, the Cockpit uncovers unexpected access points, web servers and other devices that may leave a network open to attack. Moreover, it gathers and identifies operating systems of each device, open network ports, active services on those ports, and installed certificates.

The customer's employee(s) responsible for remediation as well as the current status of the remediation process: The business process risk view presents the current threats of the IT security flaws to business processes. For example, a server with several vulnerabilities is not only a threat to the IT infrastructure, but also to the IT services provided by the server. Employees might be unable to send and receive emails, web portals might be inaccessible or the ERP system interrupted. Thus, communication by email becomes impossible, incoming orders via the web portal are not received or new stock levels cannot be entered in the ERP system. In this way, the presentation of IT risks and their influences on IT services and business processes in turn demonstrates clearly and understandably the effects and the overall context at a glance.

Benefits for You

- Accurate and fast identification of real threats from various gateways to enable a prompt incident respond.
- Optimal environment for the fulfillment of several compliance requirements in an efficient and scalable way.
- Customized rules, use cases, dashboards and reports fitting your organization's needs.
- Unified and centralized security event management and extraction of relevant security related patterns.
- Clear view of heterogeneous IT environments, data and security.
- Best-in-class correlation capabilities, analysis and reporting.
- Fast, powerful, scalable and highly flexible SIEM solution.
- Risk & Security Cockpit as the central and unified information platform.
- Optimization of existing security investments.
- Support for multitenancy deployments.

SIEM is the key for risk analysis and correlation and can be a decisive step in your holistic IT security. Find out more about other IT risk detection modules to complete your IT security monitoring:

https://www.radarservices.com/radarplatform/risk-detection-modules/

The European Experts
in IT Security Monitoring
and IT Risk Detection

RadarServices is Europe's leading technology company in the field of Detection & Response. In focus: The early detection of IT and OT security risks for corporations and public authorities offered as a Solution or a Managed Service. The cutting-edge, inhouse-developed technology platform is the basis used for building up a client's Security Operations Centre (SOC) or it is used in combination with our expert analysts, documented processes and best practices as SOC as a Service. The result: Highly effective and efficient improvement of IT and OT security and IT and OT risk management, continuous IT and OT security monitoring and an overview of security-related information throughout the entire IT and OT landscape of an organization.

RadarServices
Zieglergasse 6
1070 Vienna
Austria

Phone:	+43 (1) 929 12 71-0
Fax:	+43 (1) 929 12 71-710
Email:	sales@radarservices.com
Web:	www.radarservices.com