ENTERPRISE PERFORMANCE MONITORING NETEYE 4
Unified Monitoring und Security Information und Event Management
- NTOP and Würth Phoenix are long term partner (over 10 years)
  - Network monitoring and visibility
  - Integrate ntopng enterprise in NetEye 4
  - Vision NetEye 4 SIEM
Attacks are inevitable
La scomposizione del mercato

Campioni: 166 grandi imprese
Percentuale aziende che dichiara una crescita del budget
The term **Security Information Event Management (SIEM)**, coined by Mark Nicolett and Amrit Williams of Gartner in 2005.

Describes the product capabilities of:
- **gathering**, **analyzing** and **presenting** information from network and security devices
- identity and access management applications
- vulnerability management and policy compliance tools
- operating system, database and application logs
...and external threat data.

SIEM is a term for software and products services combining security information management (SIM) and security event manager (SEM).
- The acronyms SEM, SIM and SIEM have been sometimes used interchangeably.
- The segment of security management that deals with real-time monitoring, correlation of events, notifications and console views is commonly known as Security Event Management (SEM).
- The second area provides long-term storage, analysis and reporting of log data and is known as Security Information Management (SIM).
<table>
<thead>
<tr>
<th>Domain</th>
<th>Data sources</th>
<th>Timing</th>
<th>Collector</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>Pcap, netflow, ipfix, DPI</td>
<td>Real time packet processing</td>
<td>nProbe, n2disk, Packetbeats, Logstash</td>
</tr>
<tr>
<td>Host</td>
<td>Syslog, system state</td>
<td>Real time, Asynchronous</td>
<td>Safed, Auditbeats, Logstash, Winlogbeats</td>
</tr>
<tr>
<td>Database</td>
<td>JDBC, File export</td>
<td>Real time, Asynchronous</td>
<td>Safed, Logstash</td>
</tr>
<tr>
<td>Application</td>
<td>Logs</td>
<td>Real time, Event based</td>
<td>Beats, Logstash</td>
</tr>
<tr>
<td>Cloud</td>
<td>Logs, API</td>
<td>Real-time, Event based</td>
<td>Beats, Logstash</td>
</tr>
<tr>
<td>Container</td>
<td>Logs, eBPF</td>
<td>Real time packet processing</td>
<td>nProbe, Logstash</td>
</tr>
<tr>
<td>On Premise</td>
<td>Infrastructure (as a Service)</td>
<td>Container (as a Service)</td>
<td>Platform (as a Service)</td>
</tr>
<tr>
<td>---------------------</td>
<td>--------------------------------</td>
<td>--------------------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>Functions</td>
<td>Functions</td>
<td>Functions</td>
<td>Functions</td>
</tr>
<tr>
<td>Applications</td>
<td>Applications</td>
<td>Applications</td>
<td>Applications</td>
</tr>
<tr>
<td>Data</td>
<td>Data</td>
<td>Data</td>
<td>Data</td>
</tr>
<tr>
<td>Runtime</td>
<td>Runtime</td>
<td>Runtime</td>
<td>Runtime</td>
</tr>
<tr>
<td>Middleware</td>
<td>Middleware</td>
<td>Middleware</td>
<td>Middleware</td>
</tr>
<tr>
<td>Container</td>
<td>Container</td>
<td>Container</td>
<td>Container</td>
</tr>
<tr>
<td>Orchestrator</td>
<td>Orchestrator</td>
<td>Orchestrator</td>
<td>Orchestrator</td>
</tr>
<tr>
<td>O/S</td>
<td>O/S</td>
<td>O/S</td>
<td>O/S</td>
</tr>
<tr>
<td>Virtualization</td>
<td>Virtualization</td>
<td>Virtualization</td>
<td>Virtualization</td>
</tr>
<tr>
<td>Servers</td>
<td>Servers</td>
<td>Servers</td>
<td>Servers</td>
</tr>
<tr>
<td>Storage</td>
<td>Storage</td>
<td>Storage</td>
<td>Storage</td>
</tr>
<tr>
<td>Networking</td>
<td>Networking</td>
<td>Networking</td>
<td>Networking</td>
</tr>
</tbody>
</table>

© Würth Phoenix

… more than software
SIEM FLOW

- Data Collection
- Extract Normalize
- Enrich Context
- Dashboards
- Reporting
- Correlation Alerts

IP DNS FILE Threat Intelligence
Examples of context

• Add geo-location information
• Get information from DNS, Thread Intelligence
• Get User details (Department, Policy)

Add context aids in identifying

• Access from foreign locations
• Suspect data transfer (location, volume, …)
• Suspect network activities
LOG MANAGER SOLUTION DESIGN

Beats
- FILEBEAT
- WINGLOGBEAT
- PACKETBEAT
- AUDITBEAT

nBox (nProbe)

SAFED
- Web Proxies
- EDR / EPP
- IDS /IPS / NMS
- CRM- SFA

rsyslog

Logstash
- Workers (2+)

Elasticsearch
- Master Nodes (3)
- Data Nodes (2+)
- ML Nodes (2+)

Kibana

Grafana

Tornado

iciNGA 2
Alerting Notification

NetFlow
IPFIX

Digital signed files for revision and integrity

© Würth Phoenix
LOG MANAGER INSIGHT INPUT – FILTERS - OUTPUT

Logstash

Centralized Configuration Management

Inputs
- Beats
- ... (Beats)
- JDBC
- ... (JDBC)
- TCP
- UDP
- HTTP

Filters
- Extract Fields
- Geo Enrich
- Lookup Enrich
- DNS Lookups
- Pattern Matching
- ArcSight Codec
- ... (ArcSight Codec)

Outputs
- Elasticsearch
- ... (Elasticsearch)
- Kafka
- RabbitMQ

Persistent Disk Based Queues

Safed

Beats

nBox (nProbe)

RDBMS

Elasticsearch

Kafka

Redis Messaging Queue

© Würth Phoenix

... more than software
LOG MANAGEMENT: LOG-IN/LOG-OUT ACCESS AUDITING

© Würth Phoenix
### Why SIEM Projects Often Fail?

#### Lack of Planning
- No defined scope

#### Faulty Deployment Strategies
- Incoherent log management data collection
- High volume of irrelevant data can overload the system

#### Operational
- Lack of management oversight
- Assume plug and play

"Security is a process, not a product"
VISION NETEYE SIEM

- Log collection
- Log Analysis
- Event Correlation
- Log Forensic
- IT Compliance
- Application Log Monitoring
- Object Access Auditing
- Container Log Monitoring

- Compliance
- Security
- Operations

- Real-time Alerting
- User Activity Monitoring
- Dashboard
- Reporting
- File Integrity Monitoring
- System & Device Log monitoring
- Object Access Auditing
- Cloud awareness
THANK YOU!