



SIEM – Ein Praxisbericht

16. DFN Workshop 2009

Matthias Hofherr
Peter Wimmer

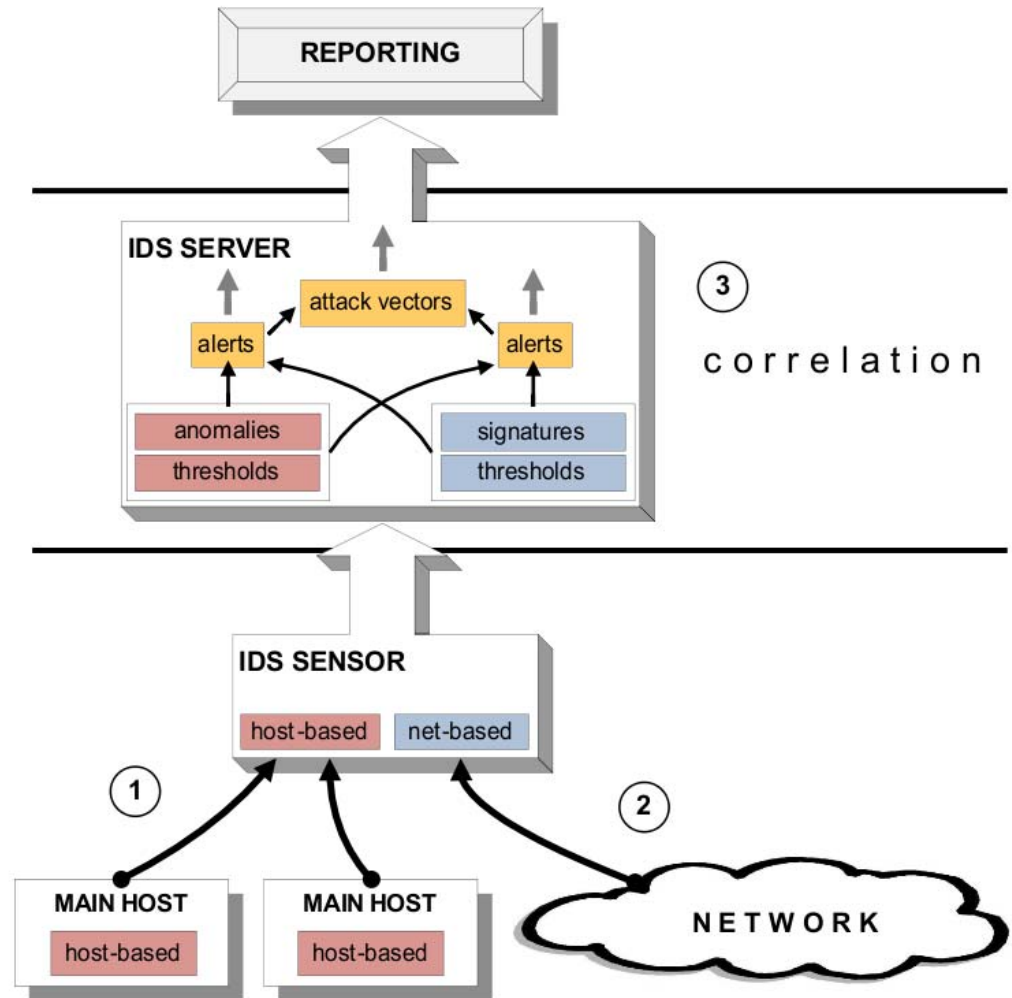


SIM und SEM

- Begriffsdefinition
 - SEM (Security Event Management)
 - Sammlung sicherheitsrelevanter Ereignisse
 - Darstellung in Echtzeit
 - SIM (Security Information Management)
 - Sammlung von Logdaten in Netzwerk
 - Analyse auf sicherheitsrelevante Vorfälle
 - SIEM
Zusammenführung von SIM und SEM

SIEM Architektur

- (1) SEM
(Host IDS)
- (2) SIM
(Network IDS)
- (3) Korrelation



SIM und SEM

- Warum sollte ich mir so etwas antun?
 - Compliance ... erfordert Monitoring (PCI, ISO27001 ...)
 - Erhöhung der allgemeinen Sicherheit (Haftung, Due Dilligence ...)
 - Arbeitersparnis im Alltag eines Information Security Officers

SIM und SEM - Voraussetzungen

- Die beste Correlation Engine ist nutzlos, wenn nichts geloggt wird (-> Windows Auditing)
- Das Netzwerk darf nicht bereits voll ausgelastet sein (Datenvolumen)
- Datenquellen müssen nicht-proprietäres Logformat unterstützen (SNMP, SMTP, syslog ...)

SIM und SEM - Datenquellen

- Unix syslog (Betriebssystem und Applikationen)
- Windows Event Log (idR Agent oder WMI)
- Router / Switch Logs
- AAA Server Logs (Radius, TACACS ...)
- Firewall Logs
- IDS / IPS Logs
- VPN Server Logs
- Anti Virus Logs
- Vulnerability Scanner Output
- ...

Kommerzielle SIEM: Erwartungshaltung

- Verteiltes System (Einsatz an mehreren Standorten)
- Hierarchisches System zur Last-Verteilung
- Unterstützung sehr vieler Datenquellen out of the box (nicht erst nach manueller Erstellung)
- Beliebig skalierbar auf allen Komponenten
- Unterstützung eines professionellen RDBMS als Backend
- Eskalation an bestehendes Ticket-System
- Unterstützung möglichst vieler Korrelations-Szenarien out of the box

Kommerzielle SIEM: Auswahl geeigneter Produkte

- detaillierte Anforderungsliste vor einem RFI
- Erstellung der Anforderungsliste zusammen mit Betreibern der überwachten Systeme (Akzeptanz!)
- Anforderungen sollten bereits ungefähre Kennzahlen (Events / Sekunde; MB / Sekunde; Anzahl der Datenquellen) enthalten
- Gewichtung der Anforderungen (Punktesystem)
- Definition der MUSS-Kriterien
- Festlegung von Schwellenwerten für Akzeptanz

Kommerzielle SIEM: RFQ

- Shortlist der bestplatzierten Kandidaten (Erfüllung aller MUSS-Kriterien vorausgesetzt)
- Erstellung einer detaillierten RFQ Ausschreibung auf Basis des RFI
- Spätestens hier: detaillierte Anforderungen und Kennwerte
- Einladung der Anbieter zur Präsentation
- Test der verbliebenen Kandidaten

Kommerzielle SIEM: Test / Proof of Concept

- Vorab: Erstellung eines Testkonzepts mit detaillierten Testfällen und Bewertungsmatrix
- Erwartete Reaktionen definieren
- Aufbau eines abgeschotteten Testnetzwerks
- Verwendung echter Datenquellen oder realistische Simulation
- Die Testdaten nicht vorab übergeben
- auf generische Lösungen drängen, wenn Testfälle nicht out-of-the-box unterstützt werden

Kommerzielle SIEM: Betrieb

- ein SIEM verursacht Betriebskosten (Wartung / Pflege / Tuning ...)
- Trotz aller Marketing-Versprechen („Turn-Key-Solution / Zero Overhead“): diese Kosten können immens sein
In der Testphase daher unbedingt Betriebs-Overhead prüfen
- Es wird ein Incident Handling / Incident Response Team benötigt, das Vorfällen tatsächlich nachgeht.
- Dieses Team muss in Incident Handling / Incident Response sowie auf dem Produkt der Wahl geschult werden

Kommerzielle SIEM: Lessons Learned

- Ohne Betriebs-Ressourcen ist ein SIEM Projekt nicht durchführbar
- Korrelation sollte primär anhand von existierenden Schwachstellen erfolgen, um False Positives niedrig zu halten
Verifizierung durch Vulnerability Scanner
- Erweiterbarkeit: bei großen Projekten sollte beim Hersteller eine Site License angefragt werden
- Kompressionsrate für Datenverkehr und Reduktion spielt eine sehr wichtige Rolle bei Enterprise-Rollouts
- Sofern vorhanden, sollte ein dediziertes Admin-Netzwerk genutzt werden
- Bestehende Eskalationsmöglichkeiten (Ticketsystem etc.) sollten genutzt werden, egal, was der Hersteller sagt

Open Source SIEM Lösungen

Ziele:

- Budget: 10.000 Euro
- Geringer Wartungsaufwand
- Implementierung von Metriken (KPIs)

Open Source SIEM: Werkzeuge

Netzwerk

- Snort Netzwerk-IDS
- p0f Passives OS-Fingerprinting
- arpwatcH Zuordnung MAC- zu IP-Adressen
- pads Passive Asset Detection System

Hosts

- ipmon Protokollierung gefilterter Pakete
- sshd, samba, openvpn, etc.
- Kernel kritische Meldungen

Open Source SIEM: Werkzeuge

Betriebsunterstützend:

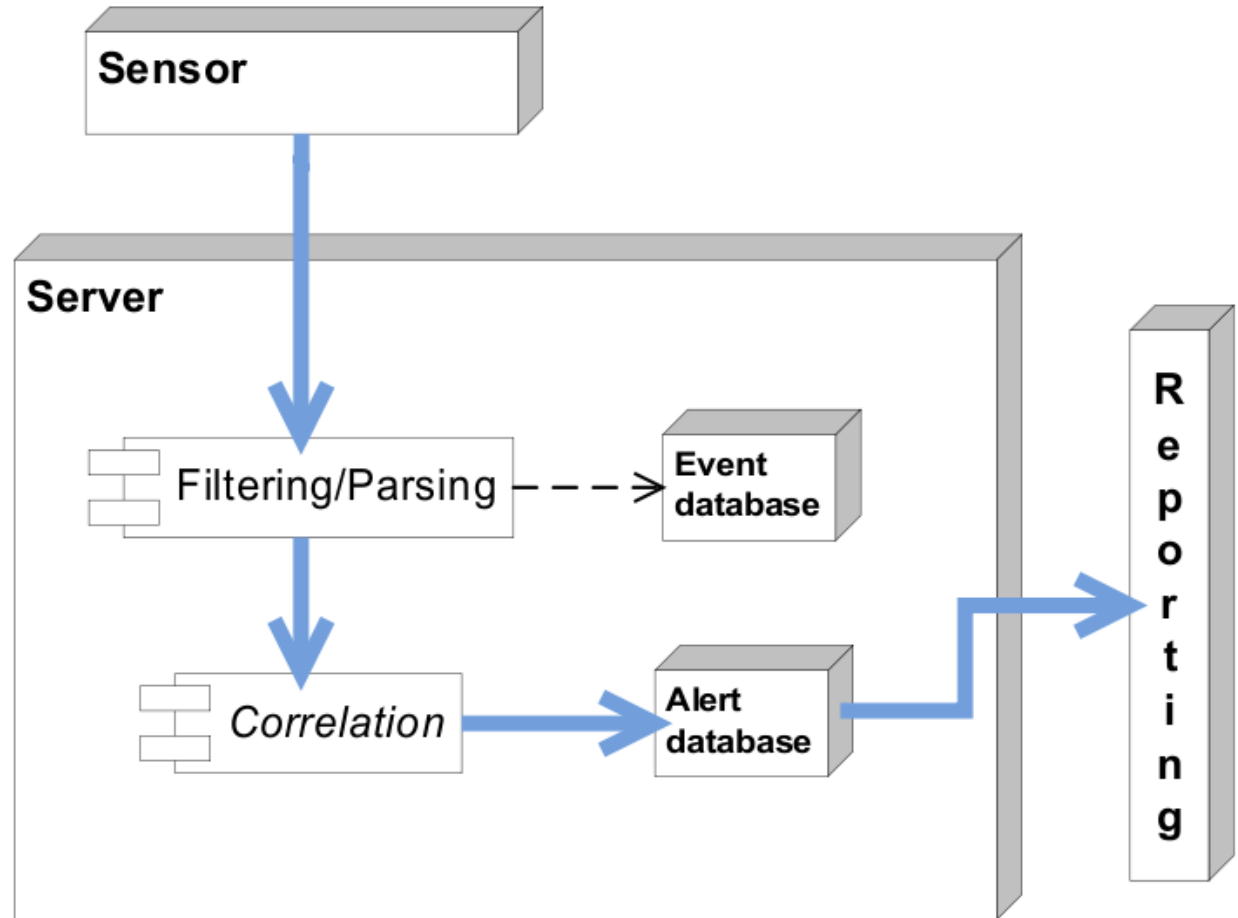
- SEC Simple Event Correlator
- syslog-ng zentraler Log-Host
- restartd Neustart fehlerhafter Prozesse

Open Source SIEM: Architektur

- Zentraler IDS-Server mit Datenbank
- IDS Sensoren je Standort

Informationsfluß

- Logs: zentraler syslog
- Snort: Datenbank



Open Source SIEM: Auswertung

- Filterung und Reduktion
 - Kategorisierung:
Status, Suspicious, Reconnaissance, Access, Compromise
 - Umwandlung in einheitliches Format
- Korrelation

Open Source SIEM: einheitliches Format

Parameter	Verwendung	Inhalte
<label>	Korrelation	INFO, SSP_BHV, RECON, ACCESS, COMPROM
<priority>	Korrelation	Snort Prioritäten
<sensor>	-	IP-Adresse Sensor
<generator>	-	Quell-Werkzeug
<source IP> <source Port> <destination IP> <destination Port>	Korrelation	Verbindungs-Details
<event ID>	Korrelation, Rückverfolgung	Eineindeutige ID
<original message>	-	Vollständige syslog-Meldung

Open Source SIEM: Korrelation

- Korrelation von Quelle, Ziel, Art des Ereignisses
- Zusammenfassung zu neuem Ereignis: „Alarm“
- Zustandsbasiert:
 - Anzahl und Kritikalität der Ereignisse
 - Weitere Ereignisse erhöhen, ausbleibende senken die Kritikalität eines Alarms

Open Source SIEM: Korrelation

SEC alerts

from: 2009-3-5 10:58:25 to 2009-3-12 10:58:25

[Refresh](#)

ID	message	priority	event source	starttime	endtime	source	destination	dport	count	comment	delete	incident?
92588617141	unusual activity	1	ipmon	2009-03-09 11:26:16	2009-03-09 11:30:22	10.1.1.1	9.149.21.191		6	add...	delete...	mark...
90335115507	unusual activity	1	ipmon	2009-03-09 11:26:45	2009-03-09 11:27:27	192.168.2.1	10.1.1.1		4	add...	delete...	mark...
90199021839	unusual activity	5	ipmon	2009-03-09 08:43:50	2009-03-09 11:19:49	10.1.1.1	149.9.0.108		1261	add...	delete...	mark...
91379246875	horizontal portscan	4	ipmon	2009-03-09 08:52:51	2009-03-09 11:14:12	10.1.1.1	(34 x)	9030	116	add...	delete...	mark...
93864273537	unusual activity	3	ipmon	2009-03-09 10:51:35	2009-03-09 11:01:23	10.1.1.1	67.159.30.124 142.177.91.133		27	add...	delete...	mark...
92133536480	unusual activity	1	snort	2009-03-09 10:01:49	2009-03-09 10:53:21	10.1.1.1	10.1.1.1		3	add...	delete...	mark...
94521067941	unusual activity	1	ipmon	2009-03-09 10:41:41	2009-03-09 10:42:02	194.77.85.25	194.77.85.31		8	add...	delete...	mark...
94299048244	unusual activity	1	ipmon	2009-03-09 10:32:24	2009-03-09 10:33:55	192.168.2.1	10.1.1.1		5	add...	delete...	mark...
91199995075	unusual activity	1	ipmon	2009-03-09 10:31:02	2009-03-09 10:31:12	10.1.1.1	9.149.21.191		3	add...	delete...	mark...
91863555396	unusual activity	3	ipmon	2009-03-09 09:26:15	2009-03-09 10:10:19	10.1.1.1	192.168.1.191		36	add...	delete...	mark...
92892328254	unusual activity	1	snort	2009-03-09 09:33:27	2009-03-09 09:42:08	10.1.1.1	10.1.1.1		6	add...	delete...	mark...
93583677875	unusual activity	1	ipmon	2009-03-09 09:29:26	2009-03-09 09:29:35	10.1.1.1	9.149.21.191		3	add...	delete...	mark...
91189633843	unusual activity	1	ipmon	2009-03-09 08:57:04	2009-03-09 08:57:57	192.168.3.1	10.1.1.1		7	add...	delete...	mark...
92445901385	horizontal portscan	2	ipmon	2009-03-09 08:44:01	2009-03-09 08:44:24	10.1.1.1	(6 x)	9030	6	add...	delete...	mark...
91860321782	unusual activity	1	ipmon	2009-03-09 05:14:00	2009-03-09 05:32:12	192.168.2.1	10.1.1.1		6	add...	delete...	mark...
90531436269	unusual activity	1	ipmon	2009-03-09 04:08:59	2009-03-09 04:09:30	192.168.3.1	10.1.1.1		7	add...	delete...	mark...
95980467747	unusual activity	1	ipmon	2009-03-09 03:03:53	2009-03-09 03:04:46	61.217.29.93	213.115.50.18		4	add...	delete...	mark...
92712855141	remote access fails	2	sshd	2009-03-09 02:43:27	2009-03-09 02:44:39	123.233.245.226	10.1.1.1	22	15	add...	delete...	mark...
92398499865	remote access fails	4	sshd	2009-03-09 01:47:23	2009-03-09 02:16:41	201.134.227.35	10.1.1.1	22	441	add...	delete...	mark...
94346512631	unusual activity	1	ipmon	2009-03-09 00:34:25	2009-03-09 00:34:43	192.168.2.1	10.1.1.1		3	add...	delete...	mark...

page: [0](#) [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [11](#) [12](#) [13](#) [14](#) [15](#) [16](#) [17](#) [18](#) [19](#) [20](#)

[Back to index](#)

Open Source SIEM: Korrelation

Beispiele für Korrelation

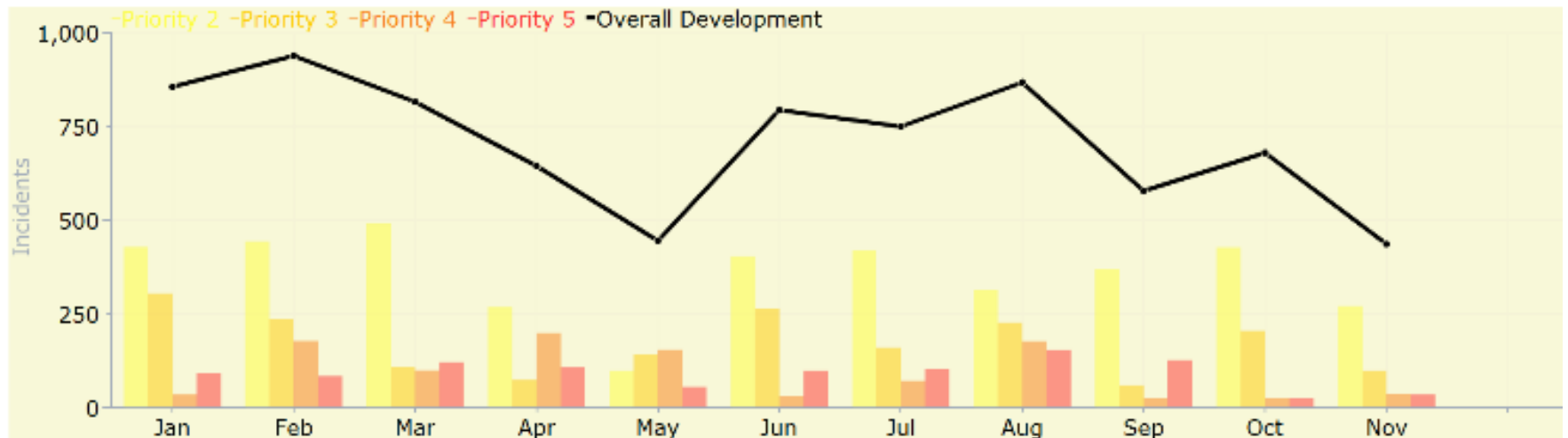
- Vertikale / horizontale Port Scans
- Lokale / entfernte fehlgeschlagene Authentifizierung
- Allgemeine Reconnaissance, Zugriffe, Kompromittierungen

Im Test / in der Planung

- Angriffsvektoren
- Historische Analyse

Open Source SIEM: Sicherheits-Metriken

- Key Performance Indikatoren (KPI) zur Bewertung des aktuellen und bisherigen Sicherheitszustandes



Open Source SIEM: Sicherheits-Metriken

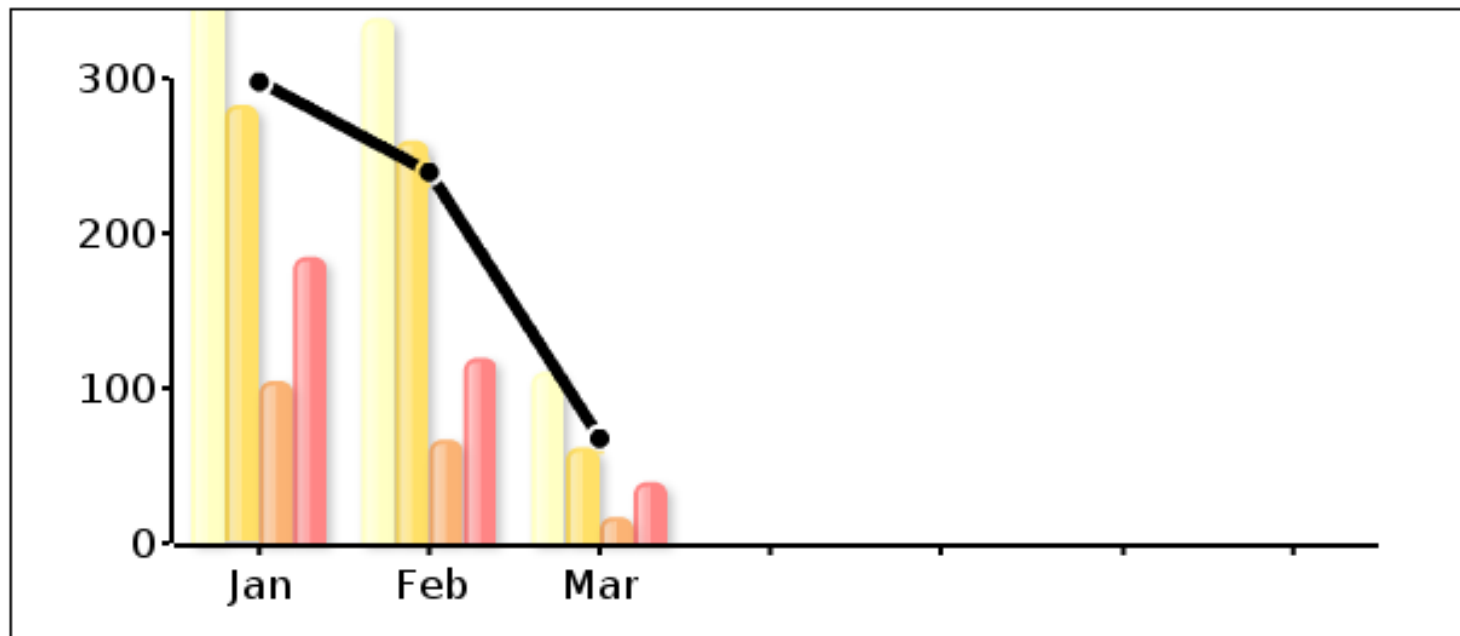
Metric GUI

[Generate PDF report](#)

Click on bars / line-dots / slices to jump to alert view.

Yearly Overview:

(2009)



Open Source SIEM: Sicherheits-Metriken

- Graphische Darstellung erleichtert Auswertung
- Verlinkung auf einzelne Ereignisse

Metric GUI

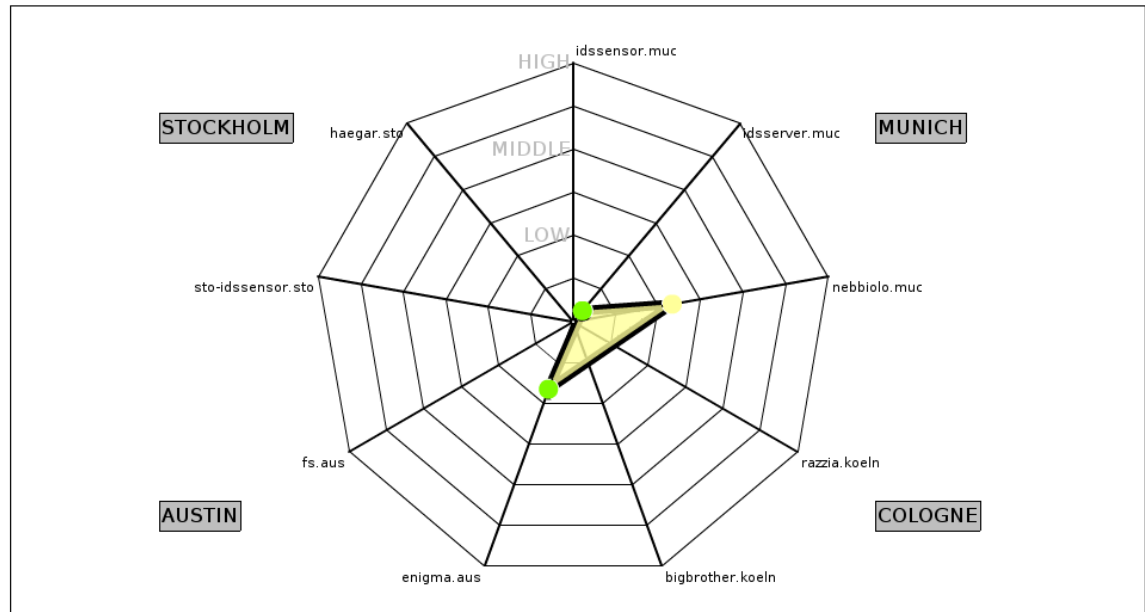
Have fun. :)

Click on bars / line-dots / slices to jump to alert view.

[Generate PDF report](#)

Failed Access Attempts

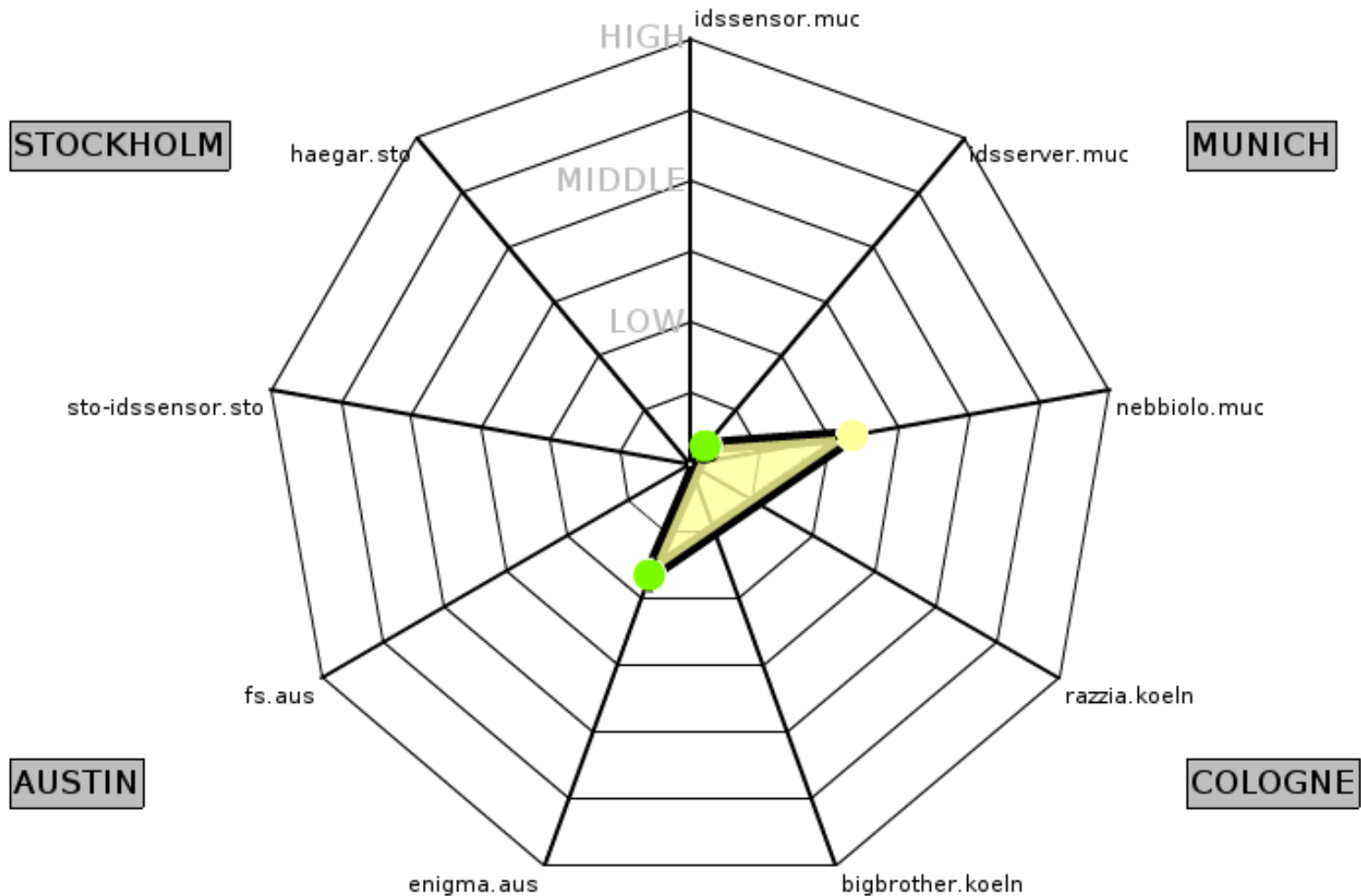
(Feb 1st 2009 - Feb 28th 2009)



Re-Select

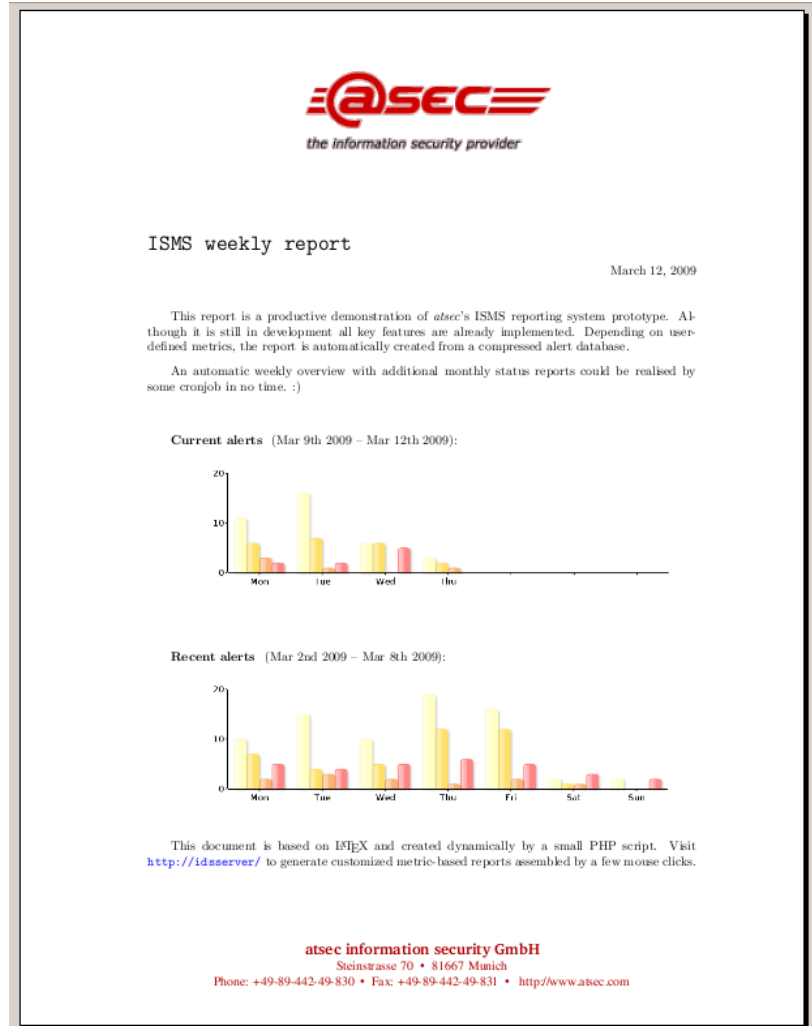
[Back to index](#)

Open Source SIEM: Metriken



Open Source SIEM: Reports

- Regelmäßiges „Management Summary“ des aktuellen Sicherheits-Levels
- per Mail als PDF
- als Nachweis der Entwicklung ggü. Geschäftsführung, Auditoren, ...



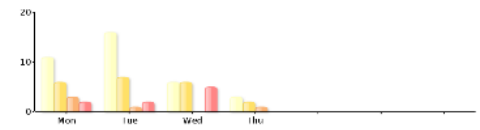
atsec
the information security provider

ISMS weekly report March 12, 2009

This report is a productive demonstration of *atsec's* ISMS reporting system prototype. Although it is still in development all key features are already implemented. Depending on user-defined metrics, the report is automatically created from a compressed alert database.

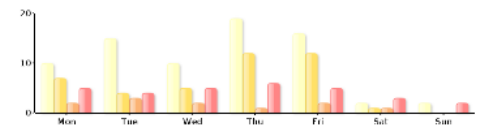
An automatic weekly overview with additional monthly status reports could be realised by some cronjob in no time. :)

Current alerts (Mar 9th 2009 – Mar 12th 2009):



Day	Alerts
Mon	10
Tue	15
Wed	5
Thu	5

Recent alerts (Mar 2nd 2009 – Mar 8th 2009):



Day	Alerts
Mon	10
Tue	15
Wed	10
Thu	18
Fri	15
Sat	5
Sun	5

This document is based on iFlix and created dynamically by a small PHP script. Visit <http://idserver/> to generate customized metric-based reports assembled by a few mouse clicks.

atsec information security GmbH
Steinstrasse 70 • 81667 Munich
Phone: +49-89-442-49-830 • Fax: +49-89-442-49-831 • <http://www.atsec.com>

Open Source SIEM: Ausblick

- Asset Liste
 - z.B. gefordert von ISO 27001
- Proaktive Warnung vor Schwachstellen
 - Festgestellte Schwachstellen -> Meldung an Administrator
- Anbindung an Trouble-Ticket System
 - zur Dokumentation der Bearbeitung
- Erweiterte Korrelation
 - Angriff – festgestellte Schwachstellen – Asset Liste

Fazit: Open Source und kommerzielle SIEM Lösungen

- Skalierbarkeit
- User Interface (Pflege der Regeln)
- Budget (Anschaffung / Betrieb)
- Reporting
(bei kommerziell: Compliance)
- Anpassung: out of the box / manuell