



Luzerner Praxisforum Security Outsourcing / MSS 23. März 2004

Managen, Monitoren, Rapportieren von Security-Services und SLA's

Thomas Lack, Geschäftsführer, GENESIS COMMUNICATION

**www.GenesisCom.ch
info@GenesisCom.ch**



Übersicht

- **GENESIS COMMUNICATION**
- **Was bietet sich an zum Outsourcen im MSS Bereich?**
- **Managed Security Monitoring**
- **Automatisiertes SLA Management**



GENESIS COMMUNICATION

Headquarter in Bern Branch office in Zurich

Bernstrasse 34, 3072 Ostermundigen / BE
Phone: +41 (0)878 883 111 Fax +41 (0)878 883 110

Binzstrasse 18, 8045 Zurich
Phone: +41 (0)878 889 111 Fax +41 (0)878 889 110

info@GenesisCom.ch, www.GenesisCom.ch

Mission Statement

Deliver innovative network, security, service and SLA management solutions to maximize the strategic value of the IT

Solutions in Network & Services & Security Management

- Innovative products & services
- Partnerships



Managen, Monitoren, Reporten von IT-Infrastruktur und IT-Services

SLA Management, Monitoring und Reporting

GENESIS COMMUNICATION
Products & Solutions

Netzwerk

- Device-Monitoring/Reporting
- Service-Monitoring/Reporting
- Service/Infrastruktur Dokumentation
- Analyse/Troubleshooting

Server & Applikation

- Server-Monitoring/Reporting
- Applikations Monitoring/Reporting
- End-to-End Monitoring/Reporting
- Service/Infrastruktur Dokumentation

Security

- (Managed) Security Monitoring
- Security Information Management (SIM)
- Security Assessment
 - Non-Intrusive Test
 - Log Analysis
 - Intrusive Test

Infrastruktur und Services



Managed Security Services

Wie der Name sagt, Managed Security bedeutet, dass ein Teil des Security Frameworks an eine oder mehrere Firmen ausgelagert wird. Die Auswahl und Kombinationsmöglichkeiten und Provider ist gross:

- „Perimeter Protection“ und Monitoring (managen der Firewalls, der Mail-Gateways, der Intrusion Detection Systeme (IDS's) oder der „Virtual private Networks“ (VPN's).
- Managed Security Monitoring
- Vulnerability-Assessment und Penetration-Tests
- Authentication
- Antivirus and Content Filtering
- Information Security Risk Assessment und Consulting
- Data Archiving and Restoration



Was Outsourcen im MSS-Bereich ?

Managed Perimeter Security

Managed Firewall, Gateway und VPN
Device Konfiguration & Management

Analogie:

- Zoll
- Panzertüre, Save

Managed Security Monitoring

7*24 Überwachung aller Meldungen
Alarms und Logs, und korrelieren mit
Vulnerabilities und Bedrohungslage

Analogie:

- Polizei
- Alarmanlage, Securitas

Firmen intern

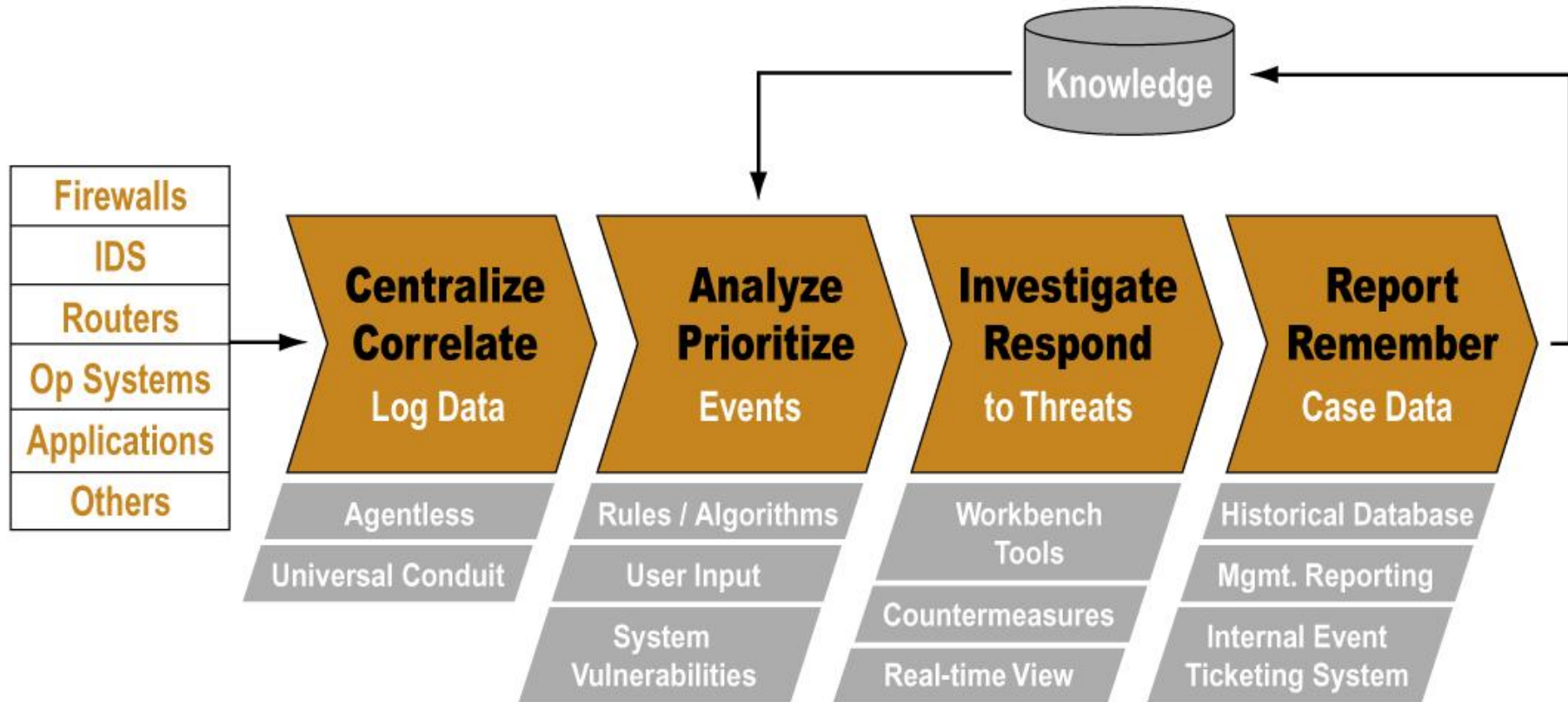
Interne Ressourcen auf
interne Security, Architektur
und Policy fokussieren

Andere Mgd.Sec.Serv:

- Vulnerabilities Scanning
- Penetration Testing
- Risk Assessment
- Consulting & Experten

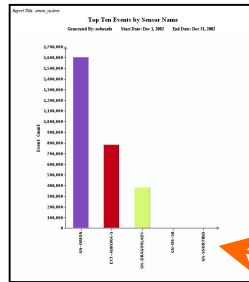


Tools Managed Security Monitoring





Tools Managed Security Monitoring



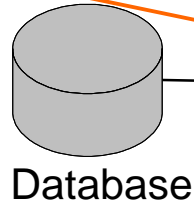
Reports

Real Time Alerts

ID	IP	Host Name	Source IP	Destination IP	Type	Action
590032549	82.49.202.158	82.49.202.158	82.49.202.158	82.49.202.158	accept	action="accept" ip="82.49.202.158"
590032549	82.49.202.158	82.49.202.158	82.49.202.158	82.49.202.158	accept	action="accept" ip="82.49.202.158"
590032549	82.49.202.158	82.49.202.158	82.49.202.158	82.49.202.158	accept	action="accept" ip="82.49.202.158"
590032549	82.49.202.158	82.49.202.158	82.49.202.158	82.49.202.158	accept	action="accept" ip="82.49.202.158"
590032549	82.49.202.158	82.49.202.158	82.49.202.158	82.49.202.158	accept	action="accept" ip="82.49.202.158"

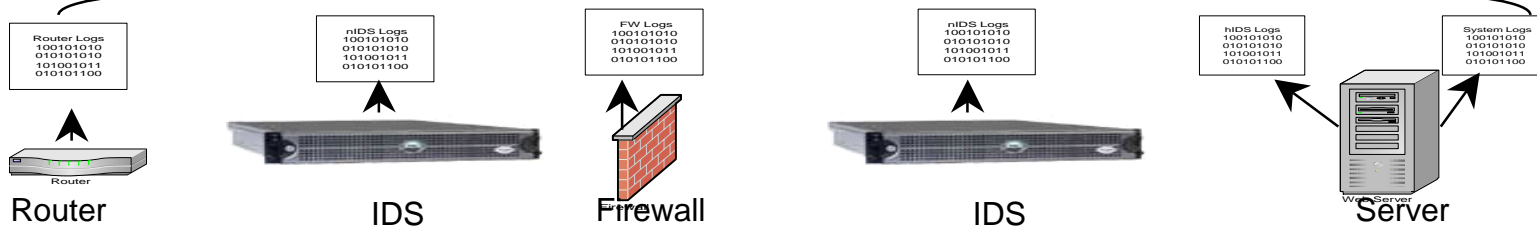
Data Normalization
Data Correlation

Forensics



Central Management System

Event Aggregation Module





Was bekomme ich vom „Managed Security Monitoring“ Provider?

Ein 7*24 Service wo:

- Technologie alle Security relevanten Log-Daten & Alarms korreliert, normalisiert, vorverarbeitet und zur Verfügung stellt
- Experten alle Security relevanten Log-Daten & Alarms auswerten
- Experten echte Attacken von falschen Alarmen separieren
- Experten die Gegenmassnahmen und die Eskalierung einleiten
- Ein komplettes Reporting, welches mich bei der Steuerung der Prozesse und bei der Planung und Entscheidungsfindung unterstützt.

Weekly Summary Report

Prepared for Company X

For the period 06/01/03 to 06/07/03

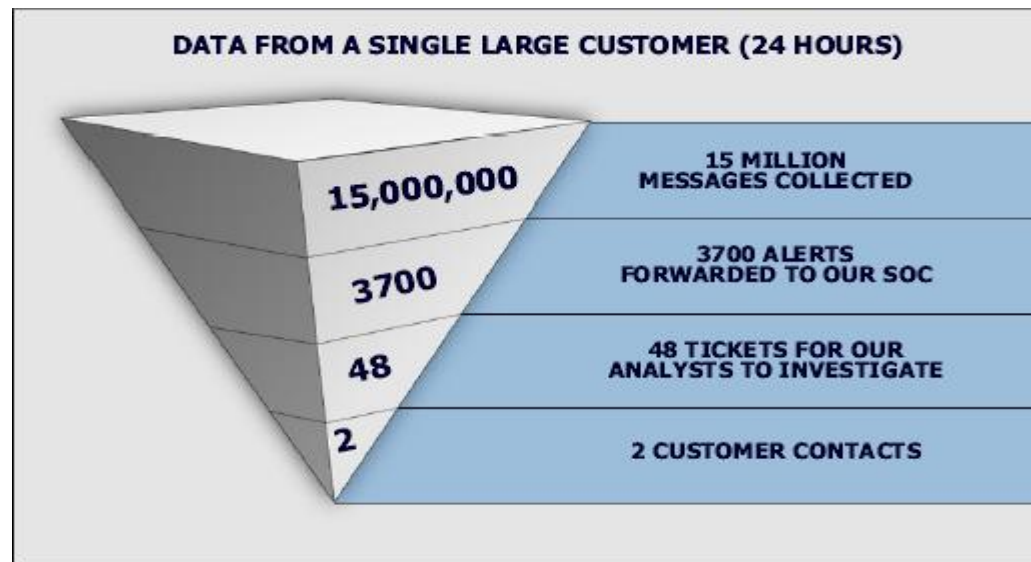
All timestamps listed in this report are in GMT

Monitoring Summary

- [Workload Reduction](#)
- [Problem Ticket Severity Breakdown](#)
- [Problem Ticket Status](#)
- [Tickets with Customer Interaction](#)
- [Top 10 Messages](#)
- [Top 10 Attacker IPs Non-RFC1918](#)
- [Top 10 Attacker IPs RFC1918](#)
- [Top 10 Destination IPs](#)
- [Top 10 Attacked Ports](#)



Was bekomme ich vom „Managed Security Monitoring“ Provider?



Problem Ticket Severity Breakdown

	Critical	Suspicious	Security Relevant	Interesting
Total security events monitored	0	23,684	6,115	352,127
Total tickets generated by Socrates	0	68	281	0
Total number of problem tickets warranting customer contact	0	12	14	0



Was bekomme ich vom „Managed Security Monitoring“ Provider?

Top 10 Attacker IPs Non-RFC1918

Attacker IP	Host Name	Event Count
66.80.130.23	ns1.megapath.net	6,633
12.31.202.5	does not resolve	4,818
206.13.30.12	dns1.sndgca.sbcglobal.net	2,502

Top 10 Destination IPs

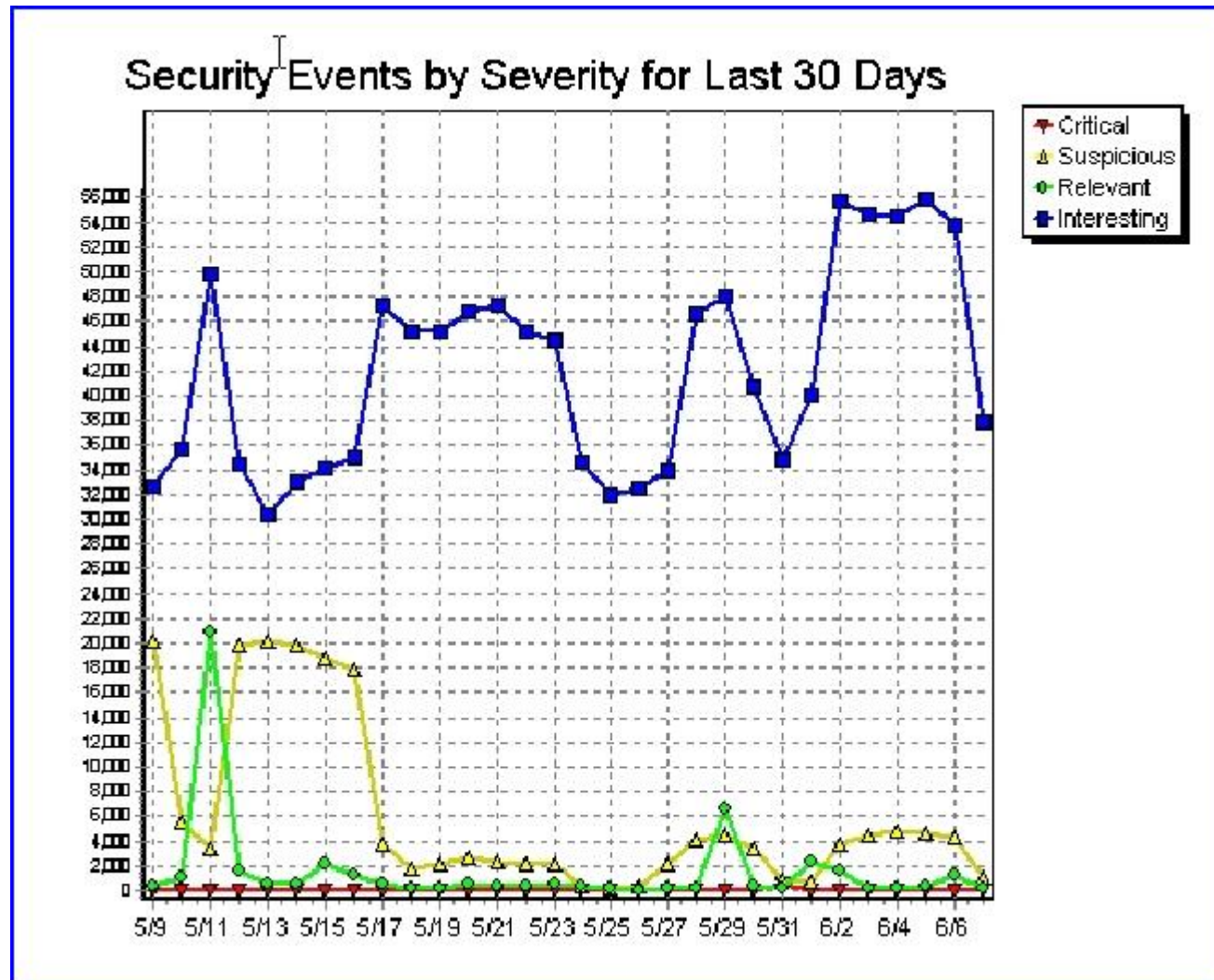
Destination IP	Host Name	Event Count
0.0.0.0	does not resolve	106,792
10.176.3.122	does not resolve	53,701
10.176.66.127	does not resolve	7,192
10.176.66.128	does not resolve	6,905
12.31.202.4	smtp-yyy-PIX	6,636
10.181.1.13	does not resolve	4,076

Top 10 Attacked Ports

Event Count	Port	Service	
		TCP	UDP
109,001	0	Reserved	Same as tcp
23099	80	http(World Wide Web HTTP)	Same as tcp
11,973	445	microsoft-ds(Microsoft-DS)	Same as tcp
9166	139	netbios-ssn(NETBIOS Session Service)	Same as tcp
7,212	2067	dlswpn(Data Link Switch Write Port Number)	Same as tcp

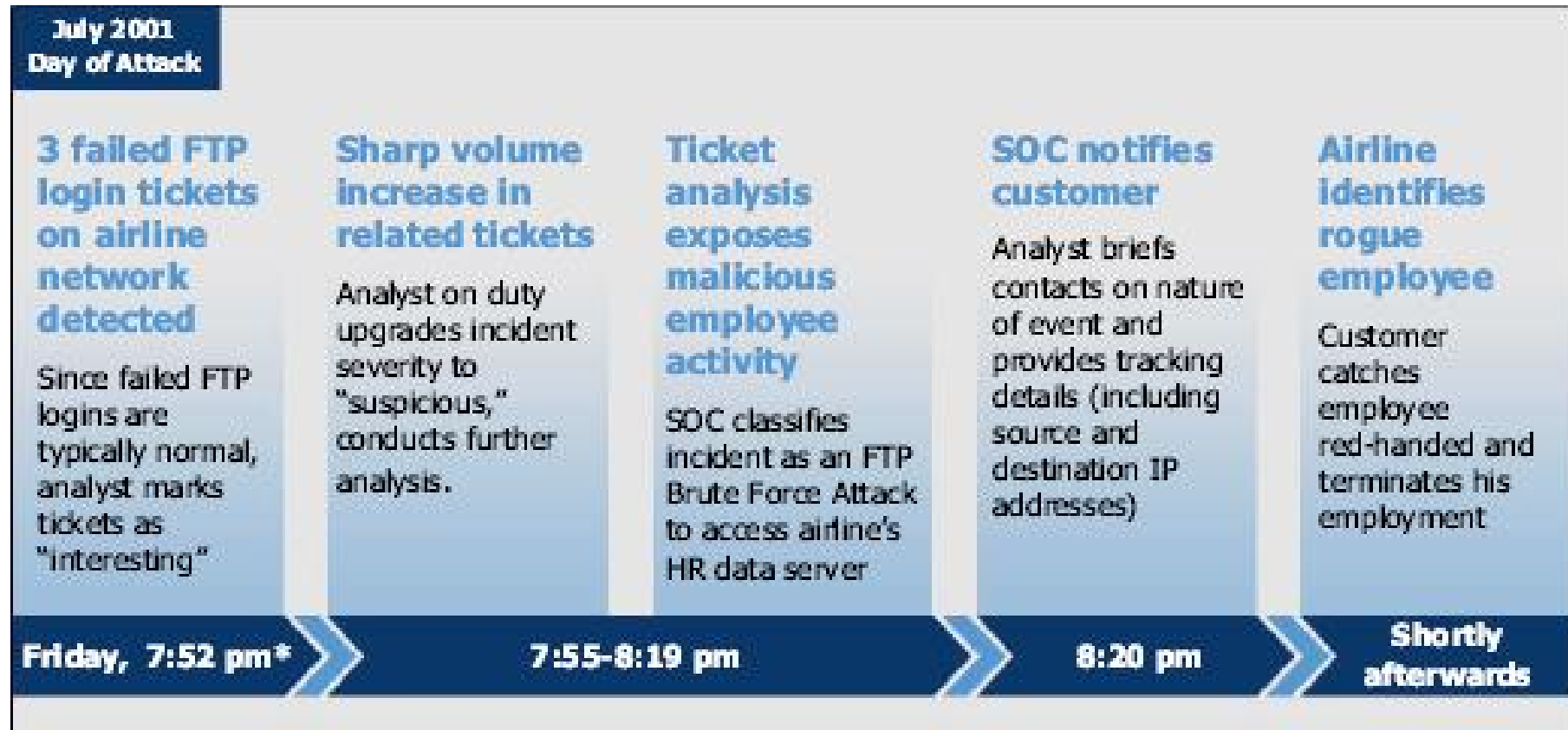


Was bekomme ich vom „Managed Security Monitoring“ Provider?



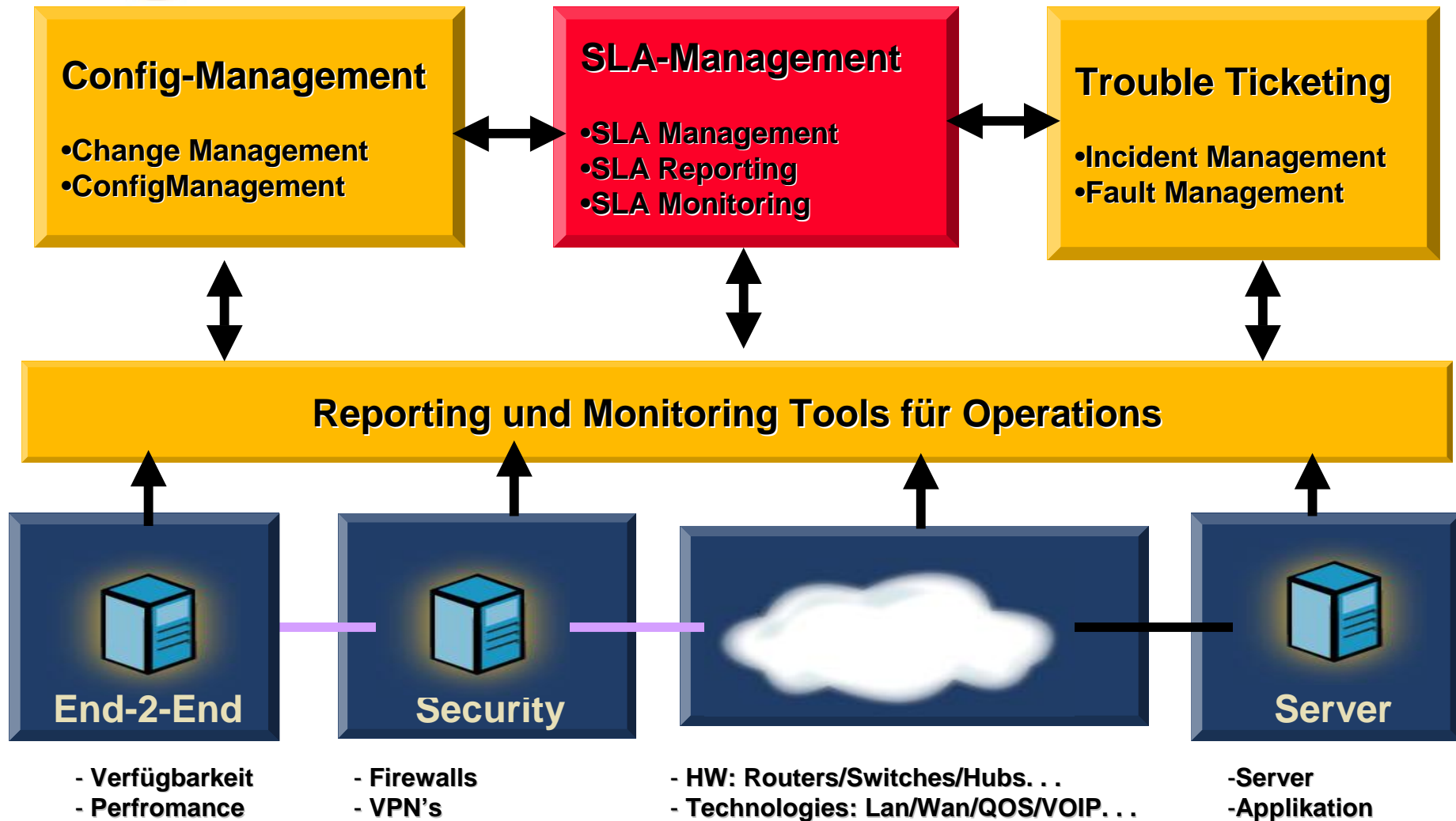


Was bekomme ich vom „Managed Security Monitoring“ Provider?





SLA Management Architektur





Was können wir messen?

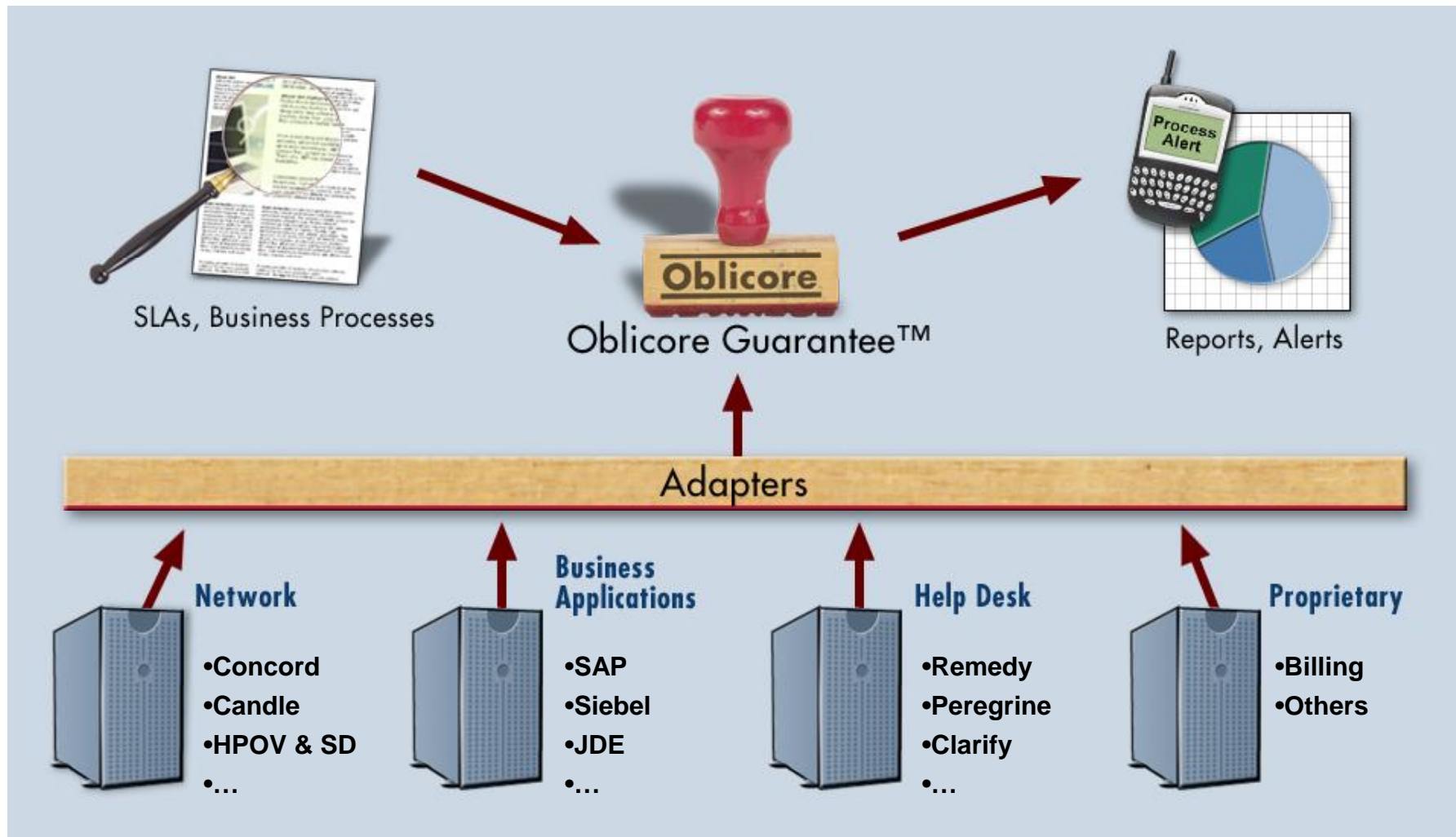
SLA Management und Verwaltung

- Repräsentation und Verwaltung der technischen Daten in Bezug zu den "Business Obligations"

Services	Device Management	Service Management	Konfigurations-Management	Problem Management
Managed Firewall Managed Gateway Managed VPN Managed Authentication	<ul style="list-style-type: none"> • Durchsatz • Fehlerrate • Bandbreiten Auslastung • Performance • Verfügbarkeit der Infrastruktur 	<ul style="list-style-type: none"> • Verfügbarkeit des Service • End-2-End Performance des Service 	<ul style="list-style-type: none"> • Response-Zeit für Changes (z.B. neuer Filter 12h nach Eintrag in CERT-Liste) 	<ul style="list-style-type: none"> • Anzahl Problem Tickets • Incident Response Time • Time to Repair



Beispiel einer automatisierten SLA Management Solution



- Contracts
- Contracts
- Exceptions
- Contract parties...
- Templates...
- SLALOM Scope
- Reports
- Alerts [10 new]
- Catalog
- Resources
- Administration

Contracts

▶ Add Contract

Name:

Contract Contract Party Service

Effective between: 31 and 31
DD/MM/YYYY hh:mm DD/MM/YYYY hh:mm

Status:
 Preliminary Pending Effective
 Not effective Archived

Order by:

Following:

▶ Search

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Displaying 1 - 7 of 7 results.

Dates presented in DD/MM/YYYY hh:mm format

				1. ACME Gold copy	Status: Preliminary		
				Effective: 01/01/2003 00:00 to 01/01/2004 00:00	Customer: ACME Inc		
				2. BBS-IM-CTS-1	Status: Preliminary		
				Versions: 16 (some overlap)	01/01/2004 00:00		
				Rules: 1 penalty formula apply.			
				Services: 4	01/01/2004 00:00		
				Time zone: CET	Customer: ACME Inc		
				4. Ben02 Sub LAN Silver	Status: Pending		
				Effective: 01/01/2004 00:00 to 01/01/2005 00:00	Customer: Benny Inc		

Status Management der SLA's

Versions Kontrolle der SLA's

Dashboard

Preferences
Logout

Oblicore Guarantee™ 2.1 - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address http://danzka/Oblicore.asp

Oblicore™ Contracts / Contracts

Contract Objectives

- General Details
- TimeSlots
- Penalties
- Export

Contract: ACME Gold copy
 Contract Party: ACME Inc (Customer)
 Effective: 01/01/2003 00:00 to 01/01/2004 00:00
 Version: 1 of 1 (Preliminary)
 Rules:

Services View Domains View TimeSlots View

- Exchange**
 - %Time Exchange Available BH
- Helpdesk**
 - % Incident Resolve Time > 4 H
 - % Incident Response Time < 15
 - Call Abandonment Rate
- LAN**
 - LAN Availability % BH
 - LAN Availability % Non BH
- SAP CRM**
 - %CRM Transactions Resp Time < 1s
 - %CRM Transactions Resp Time < 2s
 - Create alert profile
 - time crm available BH

W- Warning

Done

Wie Service Levels vom Kalender abhängen (z.B. 8x5 exkl. Feiertage und Wartungsfenster)

Wie wird gemessen (z.B. Verfügbarkeit in % anhand der Trouble-Tickets)

Service zum Kunden (z.B. Firewall Service)

Oblicore

Contracts / Contracts

Contracts

Compound TimeSlot

**+ INCLUDE Wochen/Jahres Kalender
- EXCLUDE Wochen/Jahres Kalender**

Contracts

Exceptions

Contract parties...

Templates...

SLALOM Scope

Reports

Alerts

Catalog

Resources

Administration

- Name: Cal GAA CCC
- Description: CCC Calendar & hours
- Timeslot:

Dashboard

Preferences
Logout

Previous 2003 Next

	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Hours
1													00:00-01:00
2													01:00-02:00
3													02:00-03:00
4													03:00-04:00
5													04:00-05:00
6													05:00-06:00
7													06:00-07:00
8													07:00-08:00
9													08:00-09:00
10													09:00-10:00
11													10:00-11:00
12													11:00-12:00
13													12:00-13:00
14													13:00-14:00
15													14:00-15:00
16													15:00-16:00
17													16:00-17:00
18													17:00-18:00
19													18:00-19:00
20													19:00-20:00
21													20:00-21:00
22													21:00-22:00
23													22:00-23:00
24													23:00-00:00
25													
26													
27													
28													
29													
30													
31													

00-10
10-20
20-30
30-40
40-50
50-00

Include
Exclude
Invert

- Contracts
- Reports
- Reports...
- New Report
- Favorites
- Analysis
- Impact Analysis
- Alerts [10 new]
- Catalog
- Resources
- Administration

Dashboard

Preferences
Logout



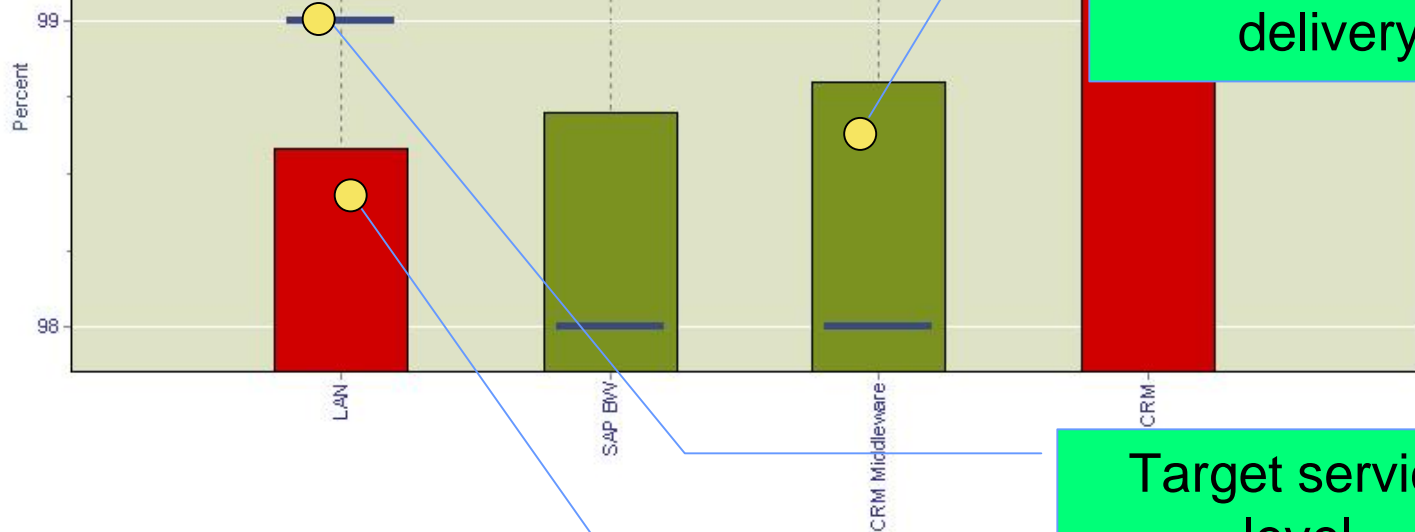
Favorite: [dropdown]

GENERATE

Zoom: Fit into page

Min % of Time Available vs. Target by Service

LAN	99	98.58
SAP BW	98	98.7
CRM Middleware	98	98.8
SAP CRM	99.5	99.37



■ Violation
 ■ Compliant
 — Target

■ Report type: Service Level vs. Target by Service
 ■ Time range: 01/01/2003 00:00 to 18/07/2003 08:56
 ■ Time zone: CET

◀ PREVIOUS
 NEXT ▶
 ▶ DONE
 ▶ REFRESH

Service over-delivery

Target service level

Service level violation

My Guarantee

All Contract Parties

- ACME Inc
 - ACME Gold
 - HK001
- Benny Inc
 - BEN01 HQ LAN Gold

All ...

ACME Inc

ACME Inc - Contracts

HK001 ACME Gold

All Contract Parties

Name	Severity	Changed at
ACME Inc	Critical	16/06/2003 22:44:54
Benny Inc	Major	17/06/2003 06:40:49

Dashboard visualisiert:

- Mgmt view der SLA's
- Status bez. SLA Einhaltung
- Root-Cause bei SLA-Verletzung

ACME Inc/HK001 - Rules & Penalties

Summary LAN availab... % LAN Resp Time < 250 Accum CRM availab... BW unavail... Accum CRM MW avai... Accum BW availab...

Aktuelle Service Delivery

ACME Inc/ACME Gold/LAN Availability % Non BH - Details

M: Calculated at: 17/06/2003 11:19:10

U: Current service level: 93.632%

Service level target: 95%

Current deviation: 1.43997%

Best predicted service level: 96.0527%

Best predicted deviation: -1.10811%

Worst predicted service level: 91.9942%

Worst predicted deviation: 3.16403%

Previous service level: 94.4627%

Voraussage bez. Service level

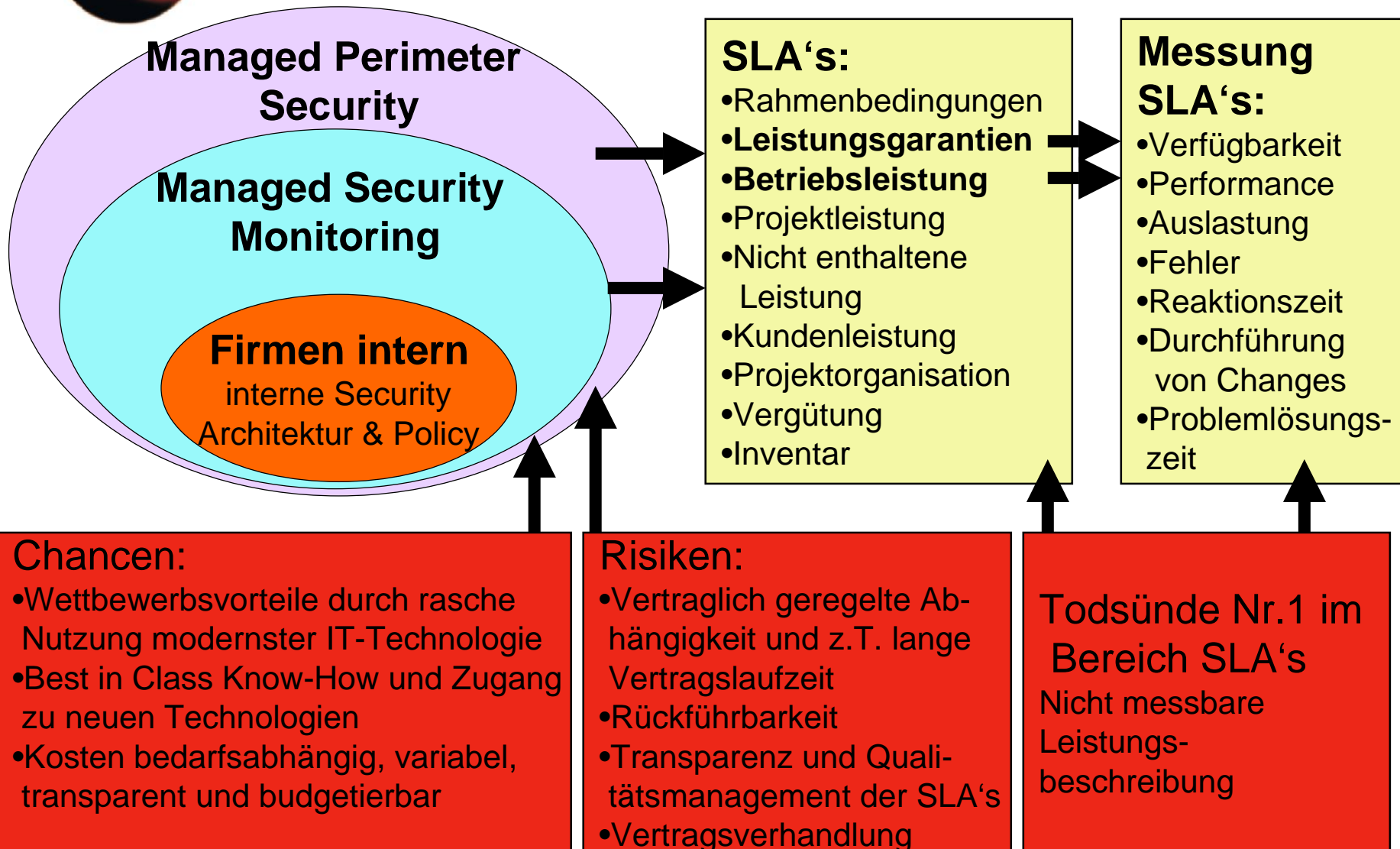
Historischer Service Level

Alarms

Severity	Time	Source
Minor	17/06/2003 06:40:49	Benny Inc/BEN01 HQ LAN Gold/...
Major	16/06/2003 22:44:54	ACME Inc/ACME Gold/%CRM Tre...
Minor	16/06/2003 22:40:24	ACME Inc/ACME Gold/% Incident
Minor	16/06/2003 22:40:19	ACME Inc/ACME Gold/LAN Avail...
Major	16/06/2003 22:40:14	ACME Inc/ACME Gold
Major	16/06/2003 22:40:14	ACME Inc/ACME Gold/LAN Avail...
Major	16/06/2003 15:55:55	ACME Inc/HK001/% LAN Resp Time < 250
Critical	16/06/2003 15:55:55	ACME Inc
Critical	16/06/2003 15:55:55	ACME Inc/HK001
Critical	16/06/2003 15:55:55	ACME Inc/HK001/Accum LAN availabili...



Zusammenfassung





www.GenesisCom.ch

Besten Dank

***Your address for
Network, Security, IT-
Service & SLA
Management Solutions***