

# Inhalt

<b>The challenge of electronic evidence: The European response</b> (Neil Mitchison).....	9
---	---

<b>Effiziente Bearbeitung von Abuse-Beschwerden</b> (Dr. Ernst Bötsch, Dr. Petra Einfeld, Wolfgang Hommel).....	13
--	----

1	Motivation .....	13
2	Ansätze zur Automatisierung .....	14
3	Workflow-Management .....	15
4	Überblick über das Abuse-System .....	17
5	Komponenten des Abuse-Systems .....	19
5.1	Input-Handler .....	19
5.2	Message-Analyzer .....	19
5.3	Storage-Mediator.....	21
5.4	Mail-Interface.....	21
5.5	Maintenance-Tool .....	21
5.6	Plugin-Server.....	22
5.7	Die graphische Benutzeroberfläche.....	22
6	Prototypische Implementierung.....	24
7	Zusammenfassung und Ausblick.....	24

<b>IT-Incident Management durch externe Dienstleistung – Die Lösung aller IT-Incident Management Probleme?</b> (Roland Wagner).....	27
--	----

1	Motivation .....	27
2	Sicherheitsstruktur von IT-Netzwerken.....	28
3	Werkzeuge zur Datenreduktion .....	31
3.1	IBM Risk Manager.....	31
3.2	ISS Site Protector mit Fusion Modul.....	32
3.3	SESA von Symantec .....	33
3.4	Netcool von Micromuse .....	33
4	Managed Security Service als externe Dienstleistung .....	34
4.1	Activis Managed Security Services.....	34
4.2	Controlware Managed Security Services .....	34
4.3	IBM Managed Security Services.....	35
4.4	Symantec Managed Security Services.....	35
5	Anforderungskatalog an einen Managed Security Service.....	35
5.1	Liste mit Anforderungen .....	36
5.2	Gewichtung der Liste .....	39
6	Zusammenfassung.....	40
7	Literaturverzeichnis.....	42

<b>Eine Informationsbasis für zeitoptimiertes Incident Management</b> (Peter Scholz, Ramon Mörl) .....	43
---	----

1	Einleitung und Motivation.....	43
---	--------------------------------	----

2	Herausforderungen des Incident Managements.....	45
3	Analyse der Vertrauensketten außerhalb des Unternehmens.....	47
4	Risikomanagement entlang von Wertschöpfungsketten.....	49
	4.1 Stand der Technik und Innovation .....	50
	4.2 RiskNodes und RiskCharts.....	52
	4.3 Ein Unternehmensebenen übergreifender Verfeinerungsbegriff.....	53
5	Analyse der Incidentauswirkungen innerhalb des Unternehmens .....	54
6	Zusammenfassung .....	55
7	Literaturverzeichnis .....	56

## **Informationslogistische Ansätze für CERTs**

(Caroline Neufert, Dr. Christoph Thiel)..... **57**

1	Einleitung .....	57
2	Informationslogistische Komponenten eines CERT.....	58
3	Ein informationslogistisches Framework .....	60
	3.1 Modellierung nutzerspezifischer Informationsbedarfe.....	61
	3.2 Architektur des Frameworks .....	61
	3.3 Praktische Erfahrungen .....	64
4	Zusammenfassung .....	64
5	Literaturverzeichnis .....	64

## **Visual Problem-Solving Support for New Event Triage in Centralized Network Security Monitoring: Challenges, Tools and Benefits**

(Markus Stolze, René Pawlitzek, Andreas Wespi) ..... **67**

1	Introduction .....	67
2	SOC Operators' Problem-Solving Task .....	68
3	SOC Problem-Solving Support .....	70
	3.1 New Event Triage Support.....	70
	3.2 Strange Event Analysis Support.....	71
	3.3 Pattern Assessment Support.....	71
	3.4 Alert Management.....	71
	3.5 False Alarm Management .....	71
4	Visual Support for New Event Triage .....	71
5	Related Work.....	74
6	Summary and Discussion .....	75
7	Acknowledgments .....	76
8	References .....	76

## **Post Mortem Analysen mit OpenSource Software**

(Matthias Hofherr) ..... **77**

1	Einsatz von OpenSource Software in der Vergangenheit.....	77
2	Das Sleuth Kit .....	78
3	Autopsy .....	79
4	Die Laboranalyse mit Sleuth Kit und Autopsy .....	79
	4.1 Case Management .....	79
	4.2 Suchfunktionen .....	81
	4.3 Hash Datenbanken .....	81

4.4	Sorter.....	82
5	Ergänzende Analyse Programme.....	82
5.1	Dateisystem-Analyse.....	82
5.2	Steganographie.....	83
5.3	Viren.....	83
5.4	Pornographie.....	83
5.5	Eigene Erweiterung: Hashsummen-DB.....	84
6	Fazit.....	84
7	Referenzen.....	86

## **Integrationsplattform zur systemübergreifenden Erfassung und forensischen Analyse von Spurenlägern**

(Christoph Fischer) .....	<b>87</b>	
1	Zielsetzungen.....	87
2	Digitale Spuren.....	87
2.1	Definition der Spurenlägen .....	87
2.2	Erfassung.....	88
2.3	Auswertung.....	89
2.4	Realisierung.....	89
3	Vorführung des Prototypen .....	91
4	Quellen .....	92

## **Forensik: Einbettung in präventive und reaktive Unternehmensprozesse**

(Nils Magnus) .....	<b>93</b>	
1	Einleitung und Motivation.....	93
2	Computer Forensik.....	93
3	Allgemeine Kenntnisse.....	95
3.1	Betriebssystem .....	96
3.2	Prozesse und Hauptspeicher.....	96
3.3	Dateisystem.....	96
3.4	Logfiles .....	97
3.5	Netzwerkzugriffe.....	97
4	Werkzeuge und Methoden.....	98
4.1	Werkzeuge.....	98
4.2	Rückverfolgung.....	99
4.3	Gerichtsverwertbarkeit.....	99
5	Organisatorisches .....	100
6	Fazit.....	102
7	Literaturverzeichnis.....	102
8	Über den Autor.....	103

## **Elektronische Beweise!**

(Reinhold Kern) .....	<b>107</b>
-----------------------	------------

<b>Einführung in die IT-Forensik</b> (Dietmar Mauersberger).....	<b>109</b>
1 Historie.....	109
2 Disziplinen.....	109
3 Forensik.....	110
4 Ausblick .....	110
<b>GI-Edition Lecture Notes in Informatics.....</b>	<b>111</b>