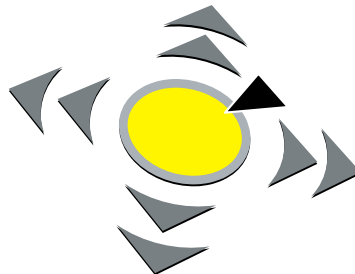


**Treffen der
der Fachgruppe SIDAR
Security – Intrusion Detection And Response
der Gesellschaft für Informatik (GI) e.V.**

Michael Meier

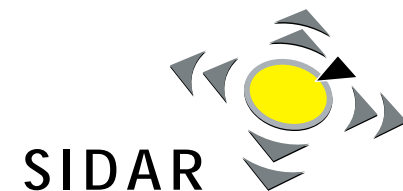
Technische Universität Dortmund
Informatik VI – Informationssysteme und Sicherheit

23. September 2008 – IMF 2008



Übersicht

- Vorstellung der Fachgruppe SIDAR
- Aktivitäten der Fachgruppe
- Ideen für weitere Aktivitäten



Themen

- Verwundbarkeiten
 - ◆ Systembeurteilung (z.B. Verwundbarkeits-Scanner)
 - ◆ Analyse (z.B. mittels Honeypot gesammelte Spuren)
 - ◆ Warnungen (z.B. von CERTs)
- Erkennung von
 - ◆ Einbrüchen (z.B. Intrusion-Detection-Systeme)
 - ◆ Malware (z.B. Viren-Scanner)
- Incident Management
 - ◆ Computer Emergency Response Teams (CERTs)
- Forensik
 - ◆ Verfolgen von Angreifern
 - ◆ Analyse (z.B. Coroner's Toolkit, Autopsy)

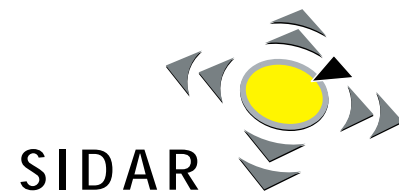
⇒ **Reaktive Sicherheit**

Vision

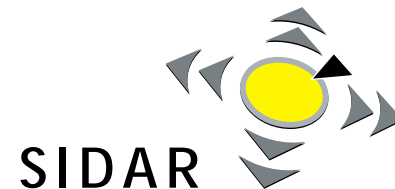
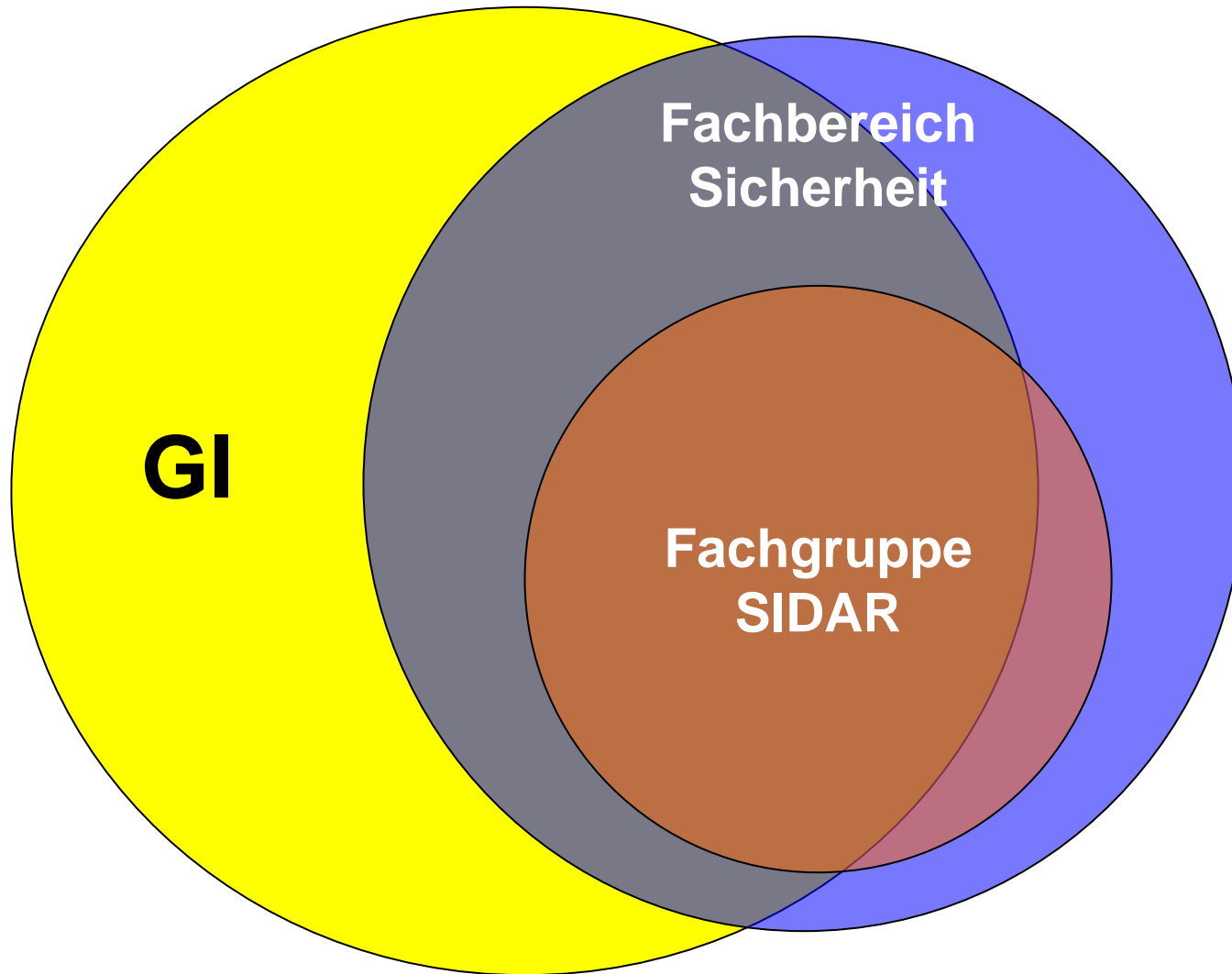
- Methoden und Werkzeuge zur Vorfallerkennung und -behandlung, die
 - ◆ nützlich,
 - ◆ benutzbar,
 - ◆ bekannt,
 - ◆ wohl akzeptiert bei Benutzern und Managern sind, sowie
 - ◆ unter Berücksichtigung ökonomischer und sozialer Aspekte angewendet werden.
- Reaktive, präventive und organisatorische Methoden und Prozeduren sollen integriert wirken.

Mission

- Anbieten einer unabhängigen und offenen Plattform für Experten und Wissenschaftler, die geeignete Methoden und Prozeduren entwickeln
- Voranbringen der nationalen und internationalen Diskussion sowie Vernetzung der Aktiven im Themenfeld
- Verbreitung von Wissen über Methoden und Prozeduren sowie Förderung der Bewusstseins ihrer Vorteile, ihres Nutzens und ihrer Kosteneffektivität
- Förderung und Entwicklung geeigneter Methoden und Prozeduren

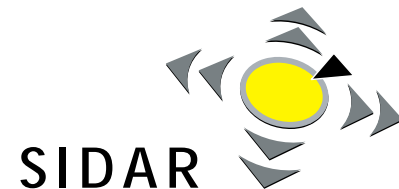


Die FG SIDAR, der FB Sicherheit und die GI



Aktuelles Leitungsgremium der FG SIDAR

- Thomas Biege (SUSE Linux GmbH)
- Dr. Ulrich Flegel (SAP)
- Sandra Frings (Fraunhofer IAO)
- Christian Gorecki (Universität Mannheim)
- Thorsten Holz (stellv. Sprecher) (Universität Mannheim)
- Dr. Pavel Laskov (Fraunhofer FIRST)
- Dr. Michael Meier (Sprecher) (Technische Universität Dortmund)
- Holger Morgenstern (ö.b.u.v. Sachverständiger)
- Dirk Schadt (SPOT)
- Sebastian Schmerl (BTU Cottbus)



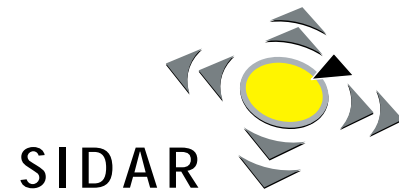
Ansprechpartner nach Themengebiet (unvollständig)

- Verwundbarkeitsanalyse
 - ◆ Marc Heuse (Baseline Security)
 - ◆ Oliver Göbel (RUS CERT/Universität Stuttgart)
- Intrusion Detection
 - ◆ Michael Meier (Technische Universität Dortmund)
 - ◆ Roland Büschkes (RWE)
- Malware
 - ◆ Toralv Dirro (McAfee)
 - ◆ Dirk Schadt (SPOT)
- Incident Management
 - ◆ Oliver Göbel (RUS CERT/Universität Stuttgart)
- Forensic
 - ◆ Dirk Schadt (SPOT)

Allgemeine Dienste

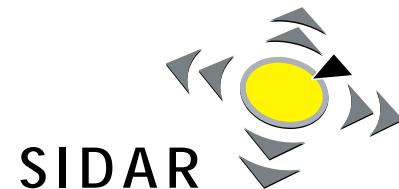
- Veranstaltungen
- Email-Liste
- Web Portal
 - ◆ Veranstaltungsmaterialien, etc.

<http://www.gi-fg-sidar.de>



Veranstaltungen

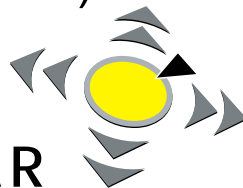
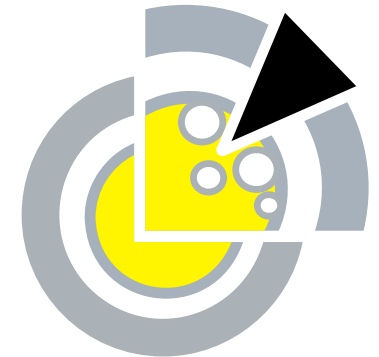
- Bisherige Veranstaltungen
 - ◆ DIMVA 2004-2008
 - ◆ IMF 2003, 2006-2008
 - ◆ SPRING 2006-2008
 - ◆ CIPHER 2006, 2007
 - ◆ PRIMA 2005
 - ◆ SKVU 2005
 - ◆ WSRS 2004
 - ◆ CTOSE 2003
 - ◆ Sicherheit 2003, 2005, 2006, 2008



DIMVA

Detection of Intrusion and Malware & Vulnerability Assessment

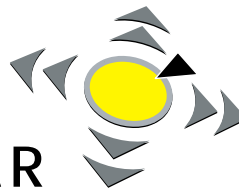
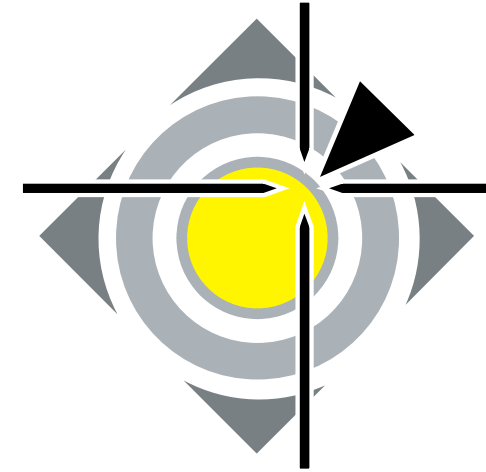
- Art der Veranstaltung
 - ◆ wissenschaftliche Konferenz
 - ◆ jährlich
 - ◆ 2 Tage
 - ◆ international (Dortmund, Wien, Berlin, Luzern, Paris, Mailand)
- Themengebiete
 - ◆ Intrusion Detection
 - ◆ Malware
 - ◆ Vulnerability Assessment
- Zielpublikum
 - ◆ Wissenschaftler
 - ◆ Industrieexperten
 - ◆ Veröffentlicht in Springer Lecture Notes in Computer Science (LNCS)
- Erweiterung
 - ◆ Kurzbeiträge in Proceedings (seit 2007)
 - ◆ Überlegung zu zusätzlichen Themen-Workshops



IMF

IT-Incident Management & IT-Forensics

- Art der Veranstaltung
 - ◆ Konferenz
 - ◆ jährlich
 - ◆ 2 Tage
 - ◆ international / findet in Deutschland statt
- Themengebiete
 - ◆ Incident Management
 - ◆ Forensics
- Zielpublikum
 - ◆ Experten aus Industrie, Verwaltung, CERTs und ISPs
 - ◆ Wissenschaftler
 - ◆ Veröffentlicht in GI Lecture Notes in Informatics (LNI)
- Erweiterung
 - ◆ Erweiterung um dritten Tag für Tutorials (seit 2007)

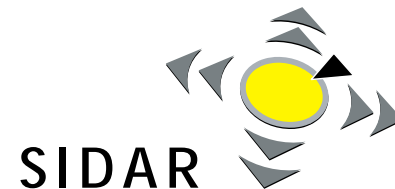
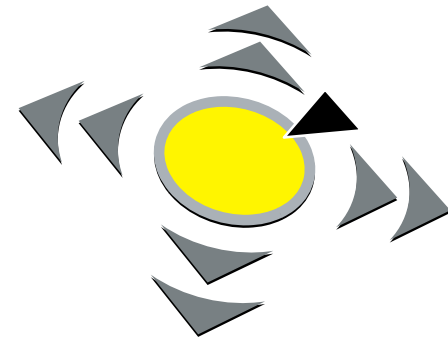


SIDAR

SPRING

Graduierten Workshop

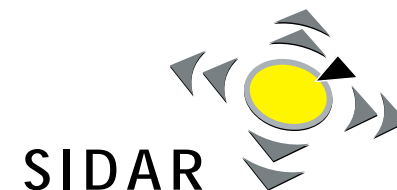
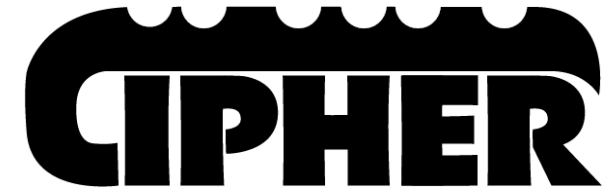
- Art der Veranstaltung
 - ◆ Graduierten Workshop
 - ◆ jährlich
 - ◆ 1 Tag
 - ◆ deutschsprachiger Raum (Berlin, Dortmund, Mannheim)
- Themengebiete
 - ◆ Intrusion Detection
 - ◆ Malware
 - ◆ Vulnerability Assessment
 - ◆ Incident Management
 - ◆ Forensics
- Zielpublikum
 - ◆ Nachwuchswissenschaftler (Diplomanden, Doktoranden)
 - ◆ Abstract-Sammlung veröffentlicht als Technischer Bericht
- Erweiterung
 - ◆ jährliche Serie (seit 2007)



CIPHER

Studierenden Wettbewerb

- Art der Veranstaltung
 - ◆ Capture the Flag Contest für Studierende
 - ◆ co-organisiert mit RWTH Aachen
 - ◆ jährlich
 - ◆ 1 Tage
 - ◆ international
- Themengebiete
 - ◆ Vulnerability Assessment
 - ◆ Incident Management
- Zielpublikum
 - ◆ Nachwuchswissenschaftler (Diplomanden)
 - ◆ Ergebnisse auf der DIMVA-Konferenz bekannt gegeben
- Erweiterung
 - ◆ US-freundlicher Zeitrahmen (seit 2007)
 - ◆ (wieder) eigenständig veranstaltet (seit 2008)



PRIMA (Regensburg, 6. April 2005)

Privacy Respecting Incident Management

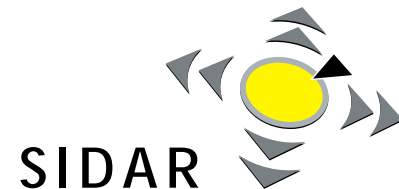
- Art der Veranstaltung
 - ◆ Satelliten-Workshop (Sicherheit 2005)
 - ◆ co-organisiert mit FG PET
 - ◆ 1/2 Tag
 - ◆ deutschsprachiger Raum
- Themengebiete
 - ◆ Privacy Aspects in
 - Incident Management
 - Intrusion Detection
- Zielpublikum
 - ◆ Experten
 - ◆ Wissenschaftler
 - ◆ Rechtsanwälte
- Erweiterung
 - ◆ einmalige Veranstaltung



SKVU (Bonn, 22. September 2005)

Sicherheit in Komplexen, Vernetzten Umgebungen

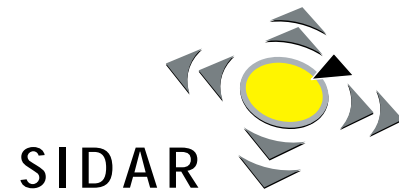
- Art der Veranstaltung
 - ◆ Satelliten-Workshop (Informatik 2005)
 - ◆ 1 Tag
 - ◆ deutschsprachiger Raum
- Themengebiete
 - ◆ Intrusion Detection
 - ◆ Forensik
 - ◆ Peer-To-Peer
 - ◆ Security Monitoring
- Zielpublikum
 - ◆ Wissenschaftler
- Erweiterung
 - ◆ einmalige Veranstaltung



WSRS (Ulm, 20. September 2004)

Workshop on Safety, Reliability, and Security of Industrial Computer Systems

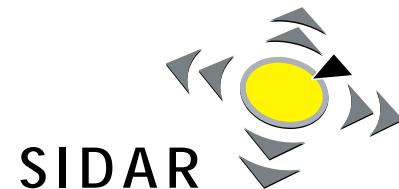
- Art der Veranstaltung
 - ◆ Satelliten-Workshop (Informatik 2004)
 - ◆ 1 Tag
 - ◆ International
- Themengebiete
 - ◆ Security
 - ◆ Reliability
 - ◆ Safety
 - ◆ of Industrial Computer Systems
- Zielpublikum
 - ◆ Wissenschaftler
 - ◆ Industrieexperten
 - ◆ Veröffentlicht in GI Lecture Notes in Informatics (LNI)
- Erweiterung
 - ◆ einmalige Veranstaltung



CTOSE (Stuttgart, 6. Mai 2003)

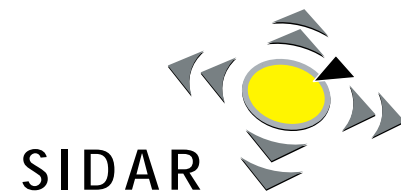
Cyber Tools On-Line Search For Evidence

- Art der Veranstaltung
 - ◆ Workshop
 - ◆ co-organisiert mit Verein zur Förderung produktionstechnologischer Forschung e.V. (FpF)
 - ◆ 1 Tag
 - ◆ deutschsprachiger Raum
- Themengebiete
 - ◆ Forensik
- Zielpublikum
 - ◆ Forensikexperten
- Erweiterung
 - ◆ einmalige Veranstaltung



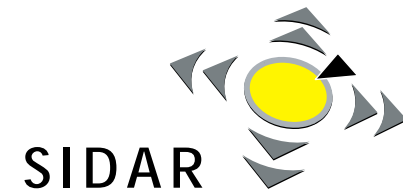
Veranstaltungen mit Beteiligung der Fachgruppe SIDAR

- Sicherheit – Schutz und Zuverlässigkeit (2003, 2005, 2006, 2008)
 - ◆ Tagung des GI Fachbereichs Sicherheit
 - ◆ alle 2 Jahre
- DFN-CERT Workshop
 - ◆ jährlich



Ideen für weitere Aktivitäten

- neue Spezial-Themen-Workshops
 - ◆ Spam
 - ◆ IT-Frühwarnung
 - ◆ ...
- Merchandising
 - ◆ SIDAR-
 - Tassen
 - Shirts
 - Caps
 - ...
- ...?



Ideen

Kontaktinformation

- Sprecher: Dr. Michael Meier
TU Dortmund – Informatik VI
44221 Dortmund
+49 231 755 6481
michael.meier{at}udo.edu
- Web: <http://www.gi-fg-sidar.de>
- Mail: info{at}gi-fg-sidar.de
- EMail-Liste: sidar{at}gi-fb-sicherheit.de
 - ◆ Subscription Info: <http://www.gi-fg-sidar.de/maillingliste.html>

