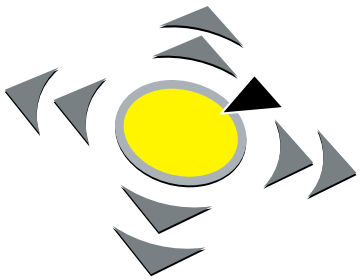
Treffen der der Fachgruppe SIDAR Security – Intrusion Detection And Response der Gesellschaft für Informatik (GI) e.V.

Michael Meier

Technische Universität Dortmund
Informatik VI – Informationssysteme und Sicherheit

15. September 2009 – IMF 2009



Übersicht

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

SIDAR

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 Managment
  - Computer Emergency Response Teams (CERTs)
- Forensik
  - Verfolgen von Angreifern
  - Analyse (z.B. Coroner´s Toolkit, Autopsy)

⇨ Reaktive Sicherheit

SIDAR

Vision

- Methoden und Werkzeuge zur Vorfallserkennung 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.

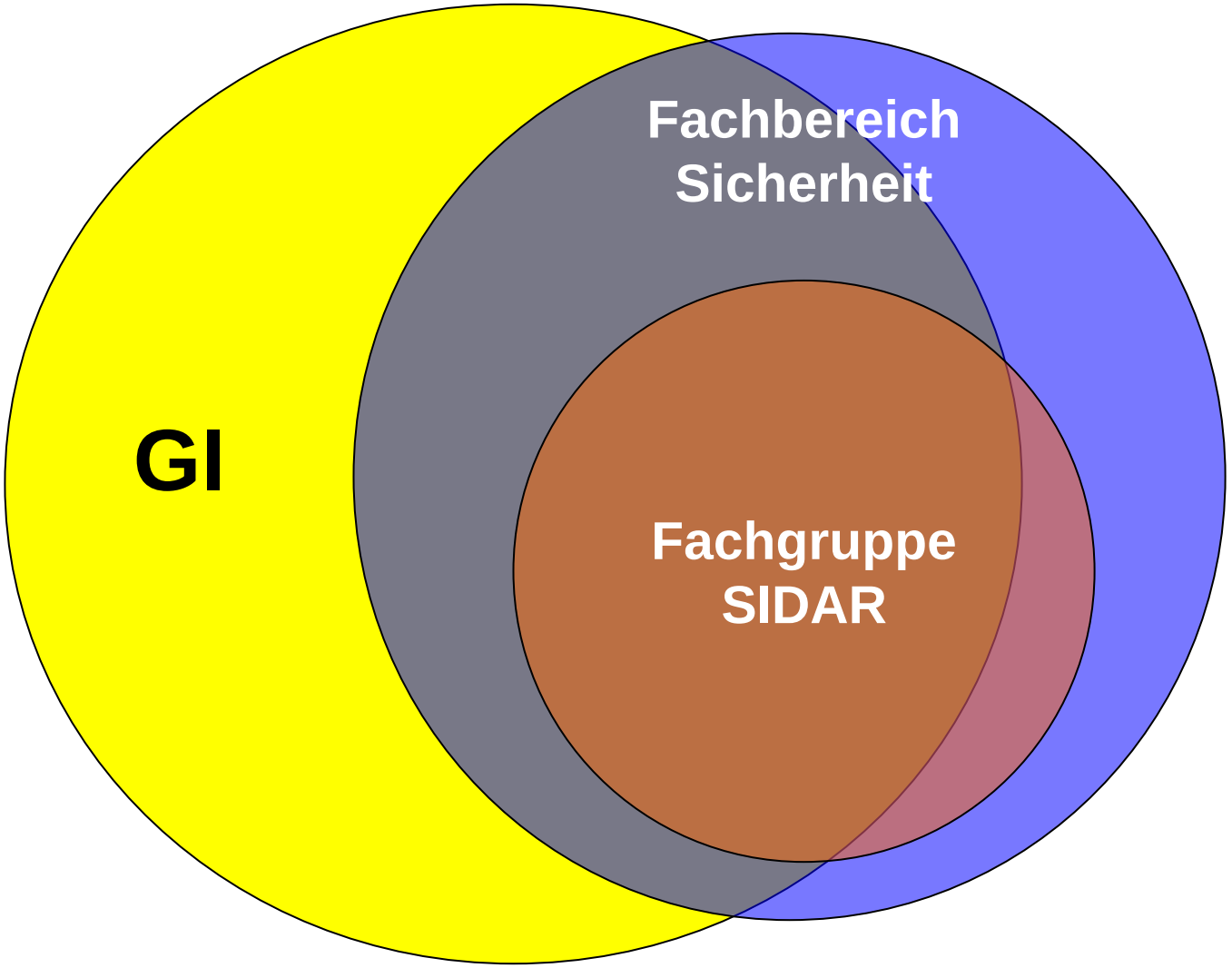
SIDAR

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

SIDAR

Die FG SIDAR, der FB Sicherheit und die GI



SIDAR

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) (Technische Universität Wien)
- Dr. Pavel Laskov (Uni Tübingen, Fraunhofer FIRST)
- Dr. Michael Meier (Sprecher) (Technische Universität Dortmund)
- Holger Morgenstern (ö.b.u.v. Sachverständiger)
- Dirk Schadt (SPOT)
- Sebastian Schmerl (BTU Cottbus)

SIDAR

Ansprechpartner nach Themengebiet (unvollständig)

- Verwundbarkeitsanalyse
  - Oliver Göbel (RUS CERT/Universität Stuttgart)
  - Oliver Heinz (Arago)
  - Marc Heuse (Baseline Security)
  - Claus Overbeck (Redteam Pentesting)
- Intrusion Detection
  - Roland Büschkes (RWE)
  - Ulrich Flegel (SAP)
  - Michael Meier (Technische Universität Dortmund)
  - Sebastian Schmerl (BTU Cottbus)

SIDAR

Ansprechpartner nach Themengebiet (unvollständig)

- Malware
  - Toralv Dirro (McAfee)
  - Christian Gorecki (Universität Mannheim)
  - Thorsten Holz (Technische Universität Wien)
  - Michael Meier (Technische Universität Dortmund)
- Incident Management
  - Sandra Frings (Fraunhofer IAO)
  - Oliver Göbel (RUS CERT/Universität Stuttgart)
  - Dirk Schadt (SPOT)
- Forensik
  - Christian Gorecki (Universität Mannheim)
  - Holger Morgenstern (ö.b.u.v. Sachverständiger)

SIDAR

Allgemeine Dienste

- Veranstaltungen
- Email-Liste
- Web Portal
  - Veranstaltungsmaterialen, etc.

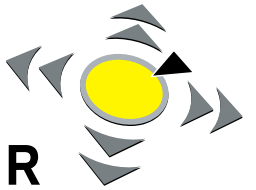
  http://www.gi-fg-sidar.de

SIDAR

Veranstaltungen

- Kommende Veranstaltungen in 2009 mit Beteiligung der FG SIDAR
  - INFORMATIK 2009 – Im Focus das Leben

    Workshop: Sicherer Umgang mit sensiblen Daten - technische Prävention und Reaktionen auf Datenschutzverletzungen
    - gemeinsamer Workshop der Fachgruppen CRYPTO, PET und SIDAR
    - Lübeck, 28.09.2009
  - SICK - Security In Communications networKs
    - 5th LCN Workshop on Security in Communications Networks
      held in conjunction with IEEE LCN 2009
    - Zurich, 20.10.2009

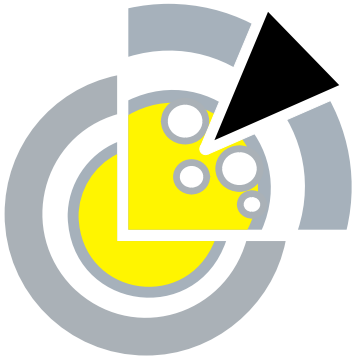


Veranstaltungen (2)

- Bisherige Veranstaltungen
  - DIMVA 2004-2009
  - IMF 2003, 2006-2009
  - SPRING 2006-2009
  - CIPHER 2006, 2007, 2009
  - PRIMA 2005
  - SKVU 2005
  - WSRS 2004
  - CTOSE 2003
  - Sicherheit 2003, 2005, 2006, 2008

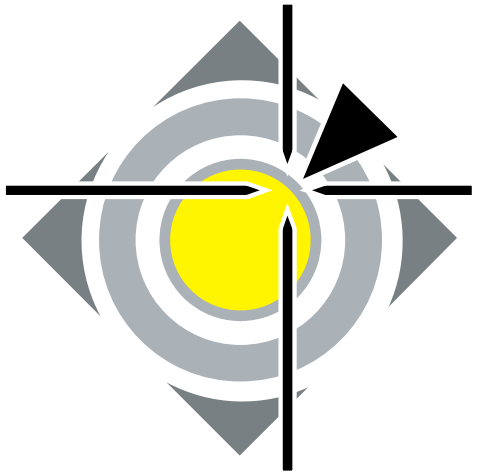
SIDAR

DIMVA
Detection of Intrusion and Malware & Vulnerability Assessment



- Art der Veranstaltung
  - wissenschaftliche Konferenz
  - jährlich
  - 2 Tage
  - international (Dortmund, Wien, Berlin, Luzern, Paris, Como (Mailand), **Bonn**)
- 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 bei IEEE Computer Society
- Erweiterung
  - Erweiterung um dritten Tag für Tutorials (seit 2007)

SIDAR

SPRING
Graduierten Workshop

- Art der Veranstaltung
  - Graduierten Workshop
  - jährlich
  - 1 Tag / 2 halbe Tage
  - deutschsprachiger Raum (Berlin, Dortmund, Mannheim, Stuttgart)
- Themengebiete
  - Intrusion Detection
  - Malware
  - Vulnerability Assessment
  - Incident Management
  - Forensics
- Zielpublikum
  - Nachwuchswissenschaftler (Diplomanden, Doktoranden)
  - Abstract-Sammlung veröffentlicht als Technischer Bericht
- Erweiterung
  - jährliche Serie (seit 2007)

SIDAR

CIPHER
Studierenden Wettbewerb

- Art der Veranstaltung
  - Capture the Flag Contest für Studierende
  - co-organisiert mit Lexi Pimenidis
  - 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)

SIDAR

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 Ascpects in
    - Incident Management
    - Intrusion Detection
- Zielpublikum
  - Experten
  - Wissenschaftler
  - Rechtsanwälte
- Erweiterung
  - einmalige Veranstaltung

SIDAR

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

SIDAR

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

SIDAR

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

SIDAR

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

-
-
-
-
-
-
-
-
-
-

SIDAR

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/mailingliste.html

SIDAR