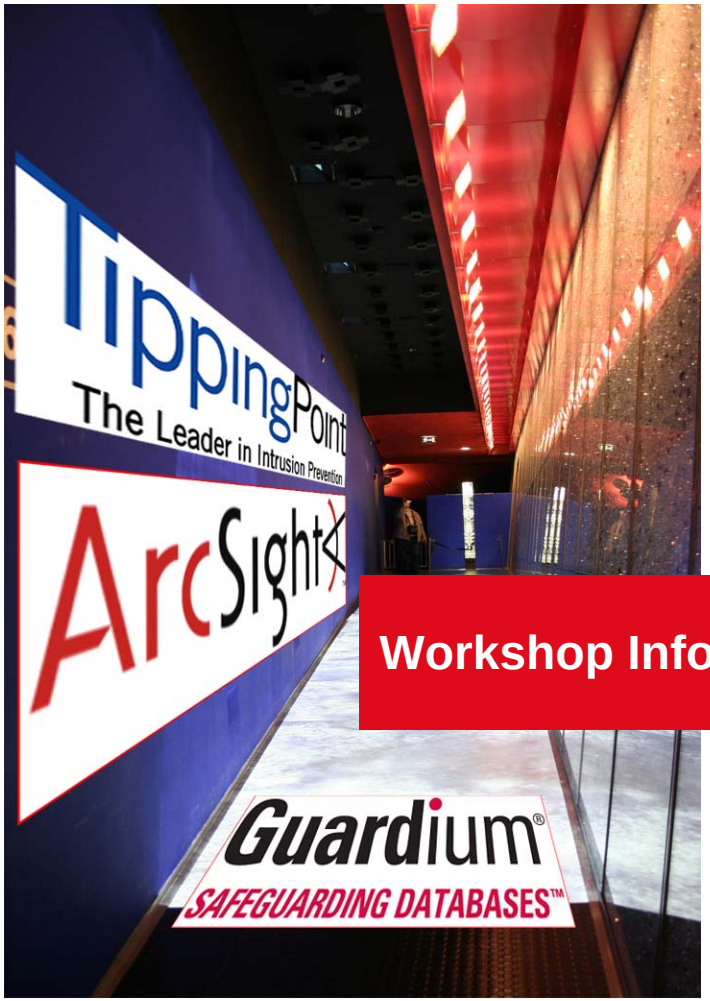
axivia



Workshop Informationssicherheit

Aktuelles Top-Thema:

- **Security Information Management**
- **Security Event Monitoring**
- **Intrusion Prevention**
- **Datenbanküberwachung**

Die IT-Landschaften werden täglich komplexer und die Zahl der zu überwachenden Daten und Systeme wächst permanent. Oft bleiben neben dem Tagesbetrieb keine Ressourcen um präventiv Log-Einträge oder (Sicherheits)ereignisse zu analysieren, zu bewerten und zu managen. Dies geschieht wenn überhaupt oft reaktiv nach einer Störung oder einem Ausfall. Systematische Auswertung findet in der Regel nicht statt und somit werden Symptome eines drohenden Ausfalls oder eines Sicherheitsvorfalles nicht erkannt und deren Eintritt nicht durch frühzeitig eingeleitete Maßnahmen verhindert.

Parallel dazu erhöht sich der Druck seitens Gesetzeslage und Verträgen mit Kunden oder Partnern permanent. Oft werden Informationen über diese Anforderungen nicht von der Unternehmensführung zur IT übermittelt. Falls doch, gilt es sich einvernehmlich mit den Datenschutzbestimmungen und den derzeit in der Organisation eingeführten Regelungen zur Protokollierung und Auswertung auseinanderzusetzen um Rechtsverstöße zu vermeiden.

Seehotel Niedernberg

Montag, 27.10.2008 ab $9^{\underline{15}}$ Uhr

Teil1:

- **Logging, Reporting, Event-Management**
- **Neues vom ISO27001 Standard**
- **ArcSight Lösungsportfolio**
- **Gesetzliche Anforderungen, Rechtssicherheit und Datenschutz**

Teil2:

- **ArcSight – Logger und ESM**
- **Best of Class IPS mit Tipping Point**
- **Guardium: Datenbanküberwachung**

Wenn anschließend die Anforderungen klar definiert sind, gilt es nun mit geeigneten Regelungen und zu guter Letzt natürlich mit technischen Hilfsmitteln und Systemen eine Lösung für diese Aufgabenstellungen zu finden.

Hierzu gibt es eine Fülle von Produkten auf dem Markt. Doch nur wenige sind in der Lage, nahezu alle Anforderungen im Bereich von Logging, Reporting und Event Management abzudecken. Wir geben Ihnen einen tiefen Einblick über die Möglichkeiten, welche Ihnen die **ArcSight** Produkte bieten.

Zur Prävention gehört heute in eine moderne Sicherheitsinfrastruktur die Intrusion Prevention Technologie um proaktiv Angriffe oder Anomalien in Echtzeit zu kontrollieren. Wie lange schon ist dieses Thema zwar bekannt, doch auch heute sind nur ganz wenige Anbieter solcher Systeme in der Lage, mit nahezu keinerlei „False-Positives“, Gbit-Durchsatz und ohne merkliche Latenzzeitverluste zu arbeiten. Wir zeigen Ihnen die Best of Class Produkte von **Tipping Point.**

Guardium ist Lösungsanbieter im Bereich der Datenbanküberwachung. Die Zugriffskontrolle auf bestimmte Daten ist aufgrund von Gesetzen oder vertraglichen Anforderungen bekannt. Bei Datenbankzugriffen ist das Durchsetzen entsprechender Richtlinien mit herkömmlichen Mitteln fast unmöglich, ebenso wie die Überwachung der Zugriffe und Verhinderung von Missbrauch. **Guardium** bietet hier effektiven Schutz.

Anmeldung zum Tagesseminar

am 27.10.2008

im Seehotel Niedernberg

Bitte beachten: Die Anmeldungen werden in der Reihenfolge des Eingangs berücksichtigt!

Die Teilnahme am Workshop ist **kostenlos**.
Jeder Teilnehmer erhält Informationsmaterial.

Informationen zum Veranstaltungsort finden Sie unter
http://www.seehotel-niedernberg.com/

Name / Vorname

Firma / Position

Telefon / Telefax

E-Mail

Datum / Unterschrift

axivia GmbH - Industriering 7 - 63868 Großwallstadt 06022/262700 – info@axivia.de

09 15 Uhr Registrierung

09 30 Uhr Begrüßung der Teilnehmer
Reinald Kempf, axivia GmbH

09 45 Uhr Logging, Reporting, Event Management
Einführung und Begriffsklärung

- Security Information Management (SIM)
- Security Event Managmnt./Monitoring (SEM)
- Typische Log-Quellen, Architektur
- Normalisierung, Aggregation, Korrelation
- Alerting, Monitoring, Reporting (realtime)

10 15 Uhr Neues aus ISO27001:2005

- ISO27002: Code of Practice
- ISO27004: Measurement: (Draft)
- ISO27005:2008: Risk Management

Zusammenhänge mit den Themen des Tages
Reinald Kempf, axivia GmbH

10 30 Uhr ArcSight Lösungsportfolio
SIM und SEM in einer Lösung?

- ArcSight Lösungselemente und Architektur
- Logger und ESM, Appliances
- Solution Packs (PCI, SOX, ISO27001)
- Connectors und Agents
- ArcSight GUI-Konsole und Web-Interface

Sandra Jungtaeubl, ArcSight

11 15 Uhr Kaffeepause

11 30 Uhr Gesetzliche Anforderungen, Rechtssicherheit und Datenschutz

- Gesetzliche Kontrollpflichten zur Notfall- und Haftungsprävention
- Datenschutz bei Protokollierung, Monitoring und Auswertung
- Umgang mit aggregierten Daten
- Gesetzl. Pflicht zum int. Kontrollsystem (IKS)
- Bezüge zum gesetzl. Risikomanagement
- IT-Compliance und Informationssicherheit

Horst Speichert, esb Rechtsanwälte

12 30 Uhr Mittagspause

13 30 Uhr Arcsight – Enterprise Security Manager
Unternehmenssicherheit auf einem Blick

- ArcSight Logger und ESM
- ArcSight Solution Packs
- Funktionsweise und Vorteile
- Echtzeitanalyse
- Trendauswertungen
- Echtzeit-Alerting & Reporting

Live Demo

- ArcSight & Compliance
  Beispiele für PCI und ISO27001
- Live-Demo ArcSight ESM

Alfred Köbler, Westcon Security

14 30 Uhr Kaffeepause

14 45 Uhr Best of Class IPS mit Tipping Point
Intrusion Detection und Prevention

- Lösungsüberblick
- Begriffsdefinition
  -Intrusion Detection
  -Intrusion Prevention

Live Demo

- Echte Gbit-Performance?
- Zentrales Management
- Monitoring vs. active Blocking
- Echtzeit-Alerting
- False Positives? Nein Danke.
- Tipping Point und Compliance
- Live-Demo Tipping Point IPS und SMS

Live Demo

Ralf Stadler, Tipping Point

15 45 Uhr Datenbanküberwachung mit Guardium
Compliance auch für Datenbanknutzung?

- Application User Monitoring
- Privileged User Monitoring
- Auto-Discovery und Application-Mapping
- Klassifikation der Datenbankinhalte
- Verhinderung externer Angriffe

Live Demo

- Monitoring , Richtliniendurchsetzung
- Audit & Report
- Live-Demo

Xy Guardium

16 30 Uhr Fragen und Antworten

16 45 Uhr Ausklang in der Lounge