

Cyber Incident Response & Forensik 2023

Konferenz am 19. & 20. Oktober 2023

Hotel Ameron Königshof, Bonn

Vorträge von Experten zu allen wichtigen Themen rund um den Umgang IT-Sicherheitsvorfällen, Threat Hunting & Disaster Recovery

TOP-Themen

- First Response Preparation
- Digital Forensik
- Threat Hunting
- Backup & Disaster-Recovery
- IT Service Continuity
- Compliance & Communication



Cyber Incident Response & Forensik 2023

Konferenz am 19. - 20. Oktober 2023

Hotel Ameron Königshof, Bonn

Direkte Interaktion mit Ihrer Zielgruppe!

Mit treffgenauem Targeting laden wir Ihre Zielgruppe zu Ihrem Vortrag auf der Cyber Incident Response & Forensik 2023 Konferenz ein.

Wer sind die Besucher der Cyber Incident Response & Forensik 2023?

Die Besucher der Cyber Incident Response & Forensik 2023 sind Leitende und Verantwortliche der Bereiche IT-Sicherheit, Cybersecurity, Cloud Security, IT-Compliance, Data Protection & IT-Infrastruktur.

Es handelt sich um ein innovationsberechtigtes Publikum mit entsprechendem Informationsbedarf und vielfach konkreten Projektabsichten. Direkt eingeladen werden Personen der Zielgruppen aus Deutschland, Österreich und der Schweiz, aus mittelständischen und großen Unternehmen.

Wer kommt als Partner zur Cyber Incident Response & Forensik 2023?

Partner der Cyber Incident Response & Forensik 2023 sind Anbieter von Technologien oder fertigen Lösungen, die dazu beitragen, schnell und vor allem richtig auf IT-Sicherheitsvorfälle zu reagieren, Threat Response und Forensik zu gewährleisten. Die Partner verstehen die aktuellen Herausforderungen der Unternehmen und präsentieren bewährte Vorgehensweisen und innovative Lösungen.

Fachvorträge, Round Tables und Working Groups

Gegliedert in verschiedene Themenbereiche demonstrieren Sie in Ihrem Vortrag Ihre Kompetenzen. Wir halten für Sie einen Speaker oder Workshop Slot bereit!

An Ihrem Messestand können Sie zudem weitere Demos und Meetings in Eigenregie anbieten.

Networking mit Teilnehmern

In den Networking Pausen und beim Dinner am ersten Abend können Sie direkt mit anwesenden Teilnehmern in Kontakt treten oder sich dort für ein Gespräch verabreden.



Cyber Incident Response & Forensik 2023

Konferenz am 19. - 20. Oktober 2023

Hotel Ameron Königshof, Bonn

IT Security Partner vergangener Veranstaltungen


accenture

 **macmon**
intelligent einfach


CLOUDFLARE

okta

 **citema**
systems
Driving Digital Technologies

plusserver

LINK11


CROWDSTRIKE


pwc

 **FIREEYE** |  **MANDIANT**

SOPHOS
Die Evolution der Cybersecurity.

FORTINET

 **WatchGuard**

Cyber Incident Response & Forensik 2023

Konferenz am 19. - 20. Oktober 2023

Hotel Ameron Königshof, Bonn

Konferenz mit interaktive Gesprächsrunden

Allen Schutzvorkehrungen zum Trotz, steigt die Zahl der Cyberangriffe und IT-Sicherheitsvorfällig in Unternehmen, Behörden und Institutionen stetig an.

Die Angriffe werden immer ausgefeilter und werden oft zu spät bemerkt. Was ist im konkreten Fall zu tun? Welche Maßnahmen in welcher Reihenfolge? Wer muss wann, worüber informiert werden? Welche gesetzlichen Meldepflichten gibt es. Wie lässt sich der Schaden eingrenzen? Was ist alles betroffen und funktioniert die Wiederherstellung kompromittierter Bereiche im Krisenfall? Fragen, wie diese sollten geklärt sein und in einem Prozess und Ablaufplan dokumentiert sein, bevor es zu einem IT-Sicherheitsvorfall kommt. Ist ein zeitgemäßer First Response Action Plan vorhanden und wenn ja funktioniert dieser dann auch im Ernstfall? Gibt es außer einem Business Continuity Prozess auch einen IT-Service-Continuity Prozess, der zumindest einen Notbetrieb geschäftskritischer IT-Systeme gewährleistet? Wie sieht es mit der Sicherung von Beweisen aus? Wurden Disaster-Recovery Maßnahmen trainiert und erprobt oder existieren diese nur in Form einer Verfahrensanweisung und technischer Maßnahmen, welche nie getestet wurden?

Besonders interessant werden IT-Sicherheitsvorfälle im Umfeld hybrider IT-Systeme, wobei große Teile der IT in die Cloud verlagert wurden als SaaS, PaaS, IaaS, und bestimmte Teile aber noch selbst betrieben werden. Hier gestaltet sich Maßnahmen zu Abwehr und Ursachenforschung besonders komplex. Denn vielen Cloud-Nutzern sind die Besonderheiten der sog. „Shares Responsibility“ in der Praxis nur zum Teil bewusst. Wo beginnt und wo endet die Verantwortung des Cloud-Plattform / Service Betreibers und wo beginnt die der Nutzer. Insondere wenn sich dies über Dienste und Plattformen verschiedener Betreiber verteilt. Wie findet man bei IT-Sicherheitsvorfällen heraus, ob sich um Fehler oder Manipulation von Betreiberseite handelt, um externe Angreifer oder um Innentäter aus dem eigenen Haus? Handelt es sich um einen gezielten Angriff oder schlicht um Konfigurationsfehler?

Auch von der Seite des Gesetzgebers gibt es immer wieder Neuerungen und veränderte Richtlinienen, die weit über den empfohlenen IT-Grundschutz hinausgehen. Welche Unternehmen sind z.B. von der NIS-2-Richtlinie betroffen und was gilt für die Umsetzung in der Praxis?

Die rasenten Veränderungen im Bereich der IT-Sicherheit in Kombination mit dem akuten Mangel an qualifizierten Fachkräften machen es den Unternehmen schwer mit den aktuellen Entwicklungen Schritt zu halten. In vielen Fällen benötigen Unternehmen daher externe Unterstützung bei Sofortmaßnahmen, der Beseitigung von Schäden und der Wiederherstellung von IT-Systemen und Services.

Hier gilt es neben einem Incident Response Plan auch um den kontinuierlichen Aufbau einer ITSCM Organisation, sowie der richtigen Nutzung von Tool für das Threat Hunting und die Einbindung qualifizierter externer Partner.

Nutzen Sie die Cyber Incident Response & Forensik 2023 um Ihre Lösungen, Methoden und Expertise zu zeigen und mit dem entsprechenden Fachpublikum in Kontakt zu treten.



Cyber Incident Response & Forensik 2023

Konferenz am 19. - 20. Oktober 2023

Hotel Ameron Königshof, Bonn

Themen Schwerpunkte

Incident Response

- First Response Activities
- Preparation - Reaktionsstrategie
- Identification - Was ist betroffen
- Containment - Isolieren & Eingrenzen
- Eradication - Schäden beheben
- Communication - Wer muss wann informiert werden
- Threat Prevention & Resillience
- Manged Security Services

IT Service Continuity

- Aufbau einer ITSCM-Organisation
- Umsetzung von ITSCM Policies
- Verzahnung zwischen BCM und ITSCM
- Kontinuierliche optimierung von IT-Notfall Prozessen - GAP Analyse
- Testen von IT-Notfallplänen
- Umgang mit Riskoclustern
- Aktivierung im Ernstfall
- IT Recovery-Planung

Digital Forensik

- Spurensuche und Beweissicherung
- Analyse der Vorfallsindikatoren
- Rekonstruktion des Ablaufs
- Präventive IT-Forensik & Forensik Readiness
- Security Awareness
- IT-Sicherheitsschulungen für Remote Worker
- Meldepflichten und rechtliche Aspekte

Backup & Disaster-Recovery

- Sichere, automatisierte Backups entsprechen der ITSCM Policy
- Backup & Restore Training & Testing
- Disaster-Recovery-as-a-Service (DRaaS)
- Self-Service / Assisted / Managed
- Multi-Cloud-Verfahren und multiple Backups
- Restore Services aus der Cloud für die Cloud für AWS, Azure, Googel etc..



Cyber Incident Response & Forensik 2023

Konferenz am 19. - 20. Oktober 2023

Hotel Ameron Königshof, Bonn

Agenda 19. Oktober 2023

-
- 8:50 **Begrüßung und Eröffnung durch den Veranstalter**
-
- 09:00 - 09:45 **„Hacked! 72 hours of a CISOs nightmare“ - Rundenbasierte Simulation eines Ransomware-Angriffs**
-  **Florian Jörgens**
Chief Information Security Officer (CISO)
Group Corporate Governance
Vorwerk SE & Co. KG
-
- 09:45 - 10:30 **Partner-Slot**
-
- 10:30 - 11:00 **Coffeebreak**
-
- 11:00 - 11:45 **Partner-Slot**
-
- 11:45 - 12:30 **Cybersecurity Herausforderungen durch Quantencomputer - (wie) müssen wir uns vorbereiten?**
-  **Manfred Rieck**
Head of Quantum Tech Deutsche Bahn
Deutsche Bahn
-
- 12:30 - 13:30 **Mittagspause**
-
- 13:30 - 14:30 **Round Tables**
-
- 14:30 - 14:45 **Round Tables - Auswertung der Ergebnisse (15 min.)**
-
- 14:45 - 15:00 **Partner-Slot**
-
- 15:00 - 15.30 **Coffeebreak**
-
- 15:30 - 16:30 **Working Groups**
-
- 16:30 - 16:45 **Working Groups - Auswertung der Ergebnisse (15 min.)**
-
- ca. 17:00 **Ende des 1. Tages**

Cyber Incident Response & Forensik 2023

Konferenz am 19. - 20. Oktober 2023

Hotel Ameron Königshof, Bonn

Agenda 20. Oktober 2023

8:50 **Begrüßung und Eröffnung durch den Veranstalter**

09:00 - 09:45 **Vortrag**

09:45 - 10:30 **Partner-Slot**

10:30 - 11:00 **Coffeebreak**

11:00 - 11:45 **Partner-Slot**

11:45 - 12:30 **Vortrag**

12:30 - 13:30 **Mittagspause**

13:30 - 14:30 **Working Groups**

14:30 - 14:45 **Working Groups - Auswertung der Ergebnisse (15 min.)**

14:45 - 15:00 **Partner-Slot**

15:00 - 15.30 **Coffeebreak**

15:30 - 16:15 **Vortrag**

ca. 16:30 **Ende der Veranstaltung**

Cyber Incident Response & Forensik 2023

Konferenz am 19. - 20. Oktober 2023

Hotel Ameron Königshof, Bonn

Erweitertes Themenportfolio

- **Cyber Incident-First Response – Welche Maßnahmen bei der Entdeckung von Sicherheitsvorfällen entscheidend sind**
- **Cyber Issue Management - Informationsprozesse und Verantwortlichkeiten im Ernstfall**
- **IT-Risk Management als präventives und zukunftsgerichtetes IT-Schwachstellen Management**
- **IT-Continuity Management - Sinnvolle und praktikable Einbindung in das Notfall- und Krisenmanagement eines Unternehmens – Beyond BCM**
- **Security Orchestration Automated Response (SOAR) und Extended Detection and Response (XDR) implementieren und effektiv einsetzen**
- **IT-Service Continuity – Notfallmaßnahmen bei Ausfällen einzelner, geschäftskritischer IT-Services**
- **KI-gestützte Cloud Intelligence und Treat Prevention – Anomalien und unerlaubte Zugriffe automatisiert erkennen und Sofort-Maßnahmen einleiten**
- **Meldefristen und Informationsprozesse im Ernstfall – Wer muss wann, wie, über was informiert werden?**
- **Wiederherstellung von kompromitierten Daten und Systemen - Secure Cloud Back Ups und Disaster-Recovery-as-a-Service nach einem Vorfall**
- **Digitale Forensik – Was bei der „Spurensicherung“ und Analyse im Nachgang eines Einbruchs in Systeme wichtig ist**
- **Digitale Beweissicherung, gesetzliche Vorgaben, Speicherung und Aufbewahrung digitaler Beweise**
- **Forensik in virtualisierten Umgebungen, mit besonderem Augenmerk auf Cloud-Plattformen und die Introspektion virtueller Maschinen**
- **Wenn die Cyberversicherung nicht zahlen will – Wichtige Aspekte rund um die Nutzung von Cyberversicherungen klären vor einem Vorfall**

Cyber Incident Response & Forensik 2023

Konferenz am 19. - 20. Oktober 2023

Hotel Ameron Königshof, Bonn



Über Executive Insights

Wir sind ein unabhängiger Veranstalter von Wirtschaftskonferenz. Unsere themenspezifisch hochaktuellen Veranstaltungen richten sich an Fach- und Führungskräfte von Unternehmen im deutschsprachigen Raum. Unsere Teilnehmer kommen von Unternehmen wie,

AXA, Bankhaus Lenz, Carl Zeiss, Commerzbank, DAB Bank, Datev, Deutsche Bahn, Deutsche Leasing, DM-Drogerie-Markt, EnBW, Fiducia, Festo, Generali Versicherungen, Helvetia, Indeed, Lanxess, Metro, Miele, Otto Group, Porsche, REWE, Robert Bosch, Schaeffler, Rehau, R+V Versicherung, Swarovski, thyssenkrup, Uniper, Versicherungskammer Bayern, Wacker Chemie, Zeppelin Baumaschinen, Zurich Gruppe u.v.a.

Wir bringen mehr als zehn Jahre Erfahrung im Konferenz-Geschäft mit und profitieren von unserem umfangreichen Netzwerk. Wir kennen die Bedürfnisse unserer Kunden und unsere Kunden wissen das zu schätzen.

Mit der **Cyber Incident Response & Forensik 2023** erweitern wir unser Informations-Spektrum für Entscheidungsträger und Spezialisten ganz gezielt zum Thema:
Maßnahmen bei IT-Sicherheits- & Cybersecurity Vorfällen.

