Bundesministerium
Verkehr, Innovation
und Technologie

AUSTRIAN INSTITUTE OF TECHNOLOGY

1. Fachtagung FORTISSIMO

Eisenstadt, 26. November 2019

FFG
Forschung wirkt.

FORTE
arma et scientia
ex officio

Bundesministerium
Landesverteidigung

Bundesministerium
Verkehr, Innovation
und Technologie

AUSTRIAN INSTITUTE OF TECHNOLOGY

Cyber Attack Decision and Support Platform (CADSP)

Dr. Dr. Florian Skopik, florian.skopik@ait.ac.at

FFG
Forschung wirkt.

FORTE
arma et scientia ex officio

Bundesministerium
Landesverteidigung

STATUS QUO IN DER CYBER ABWEHR

- Ständig ändernde **Bedrohungslage**
  - APTs, DDoS mit hohen Bandbreiten, Ransomware
  - Immer mehr
  - Immer schneller
- Veränderte **Rahmenbedingungen**
  - Gesetzeslage: NIS RL, DSGVO, Cyber Security Gesetz
  - Neue Einrichtungen bei Behörden: CSC, CDZ
  - Neue Sektor-CERTs, z.B. E-CERT
  - Neue Pflichten (Meldepflicht der KIs, Audits, …)
- Fundierte **Grundlage zur Entscheidungsfindung** notwendig!
  - Umgang mit Bedrohungen: Risikobewertung durch Trendanalysen
  - Umgang mit Incidents
    - Bewertung von Handlungsoptionen im konkreten Anlassfall

AUSPRÄGUNG VON VITALEN CYBER INCIDENT RESPONSE FÄHIGKEITEN

PROBLEMSTELLUNGEN UND GAPS

- nur spezifische, aber keine universell einsetzbare Methodik zur **Identifikation von Prozessproblemen** im militärischen Cyber-Bereich,
- keine einheitliche Sicht auf involvierte Akteure und v.a. begründete **Rollenprofile für Cyber Incident Response** in militärischen Umgebungen,
- größtenteils manuelle, aber keine automatisierbare Methodik, um **Beiträge einfacher Sensorik Daten zu Entscheidungsprozessen** zu bestimmen,
- kein Ressourcen-optimiertes, zumindest teil-automatisiertes und integriertes **Lagebildkonzept** (Berücksichtigung Technik-Organisation-Mensch),
- nur manuelles, jedoch kein (teil-)automatisiertes, strategisches und **standardisiertes Incident Management** bei mil. Cyber Incidents,
- nur Einzellösungen für Teilbereiche, jedoch keine **abgestimmte offene Systemarchitektur**, um inhomogene Technologien u. Vendor-Lock-In zu vermeiden,
- keine einfache **Messbarkeit der Verbesserung des Lagebildverständnisses** und der Effizienz von Cyber Incident Response, sowie Benutzerakzeptanz.

ZIELE UND ERWARTETE RESULTATE

Abbildung CONOPS für BMLV

- Bedarfsträgerprozesse
- Organigramm beteiligter Akteure und ihre Rollen/Profile
- Relevanz von Fachdaten für unterschiedliche Akteure

CADSP Architektur

- Modulare, offene, tragfähige und erweiterbare Architektur mit standarisierten Schnittstellen

Machine Learning zur Datensammlung u. Bewertung

- Konzepte und Modelle zur Datensammlung und Analyse
- Katalog möglicher Datenquellen
- Erarbeitung geeigneter Analyse-Algorithmen

Implementierung eines PoCs

- Funktionaler Prototyp kompatibel zu existierender Toollandschaft
- Für ausgewählte BMLV Szenarien und als Grundlage weiterführender Human Performance Tests

Validierung der PoCs

- Spezifische Testpläne und Testmethodik
- Human Performance Tests zur Bestimmung der Effizienzsteigerungen
- User Acceptance Tests

Wissenschaftlicher Diskurs

- Einbringung allg. Konzepte, losgelöst vom BMLV Kontext, in die wissenschaftl. Community
- Vernetzung mit Stakeholdern quer über Europa

DAS PRIMÄRE ZIEL VON CADSP

- Die **wissenschaftliche Untersuchung**, **technische Konzeption und Validierung einer Cyber Attack Decision and Support Platform**
- zur Detektion und Abwehr von Angriffen aus den Cyberraum.
- Aufbauend auf dem Concept of Operations (CONOPS) BMLV-spezifischer Anwendungsfälle im Cyber Incident Reponse Bereich, sowie unter der Berücksichtigung der Ergebnisse diverser KIRAS Projekte im Lagebild-Bereich, soll im gegenständlichen Projektvorhaben die **Grundlage für die Realisierung** einer international führenden Cyber Attack Decision and Support Platform (CADSP) gelegt werden,
- sowie **Herausforderungen** (Technik-Organisation-Mensch) für die ggf. nachfolgende **Weiterentwicklung** zu einem Produkt, und breite **Einführung** desselben, frühzeitig **identifiziert** werden.

PROJEKTDATEN

- **FORTE** Projekt CADSP – Cyber Attack Decision and Support Platform
- **Laufzeit:** 01.11.2019 – 30.04.2021
- **Konsortialleitung:** Dr. Dr. Florian Skopik, AIT
- **Konsortium:**
  - AIT Austrian Institute of Technology
  - Frequentis AG
  - BMLV

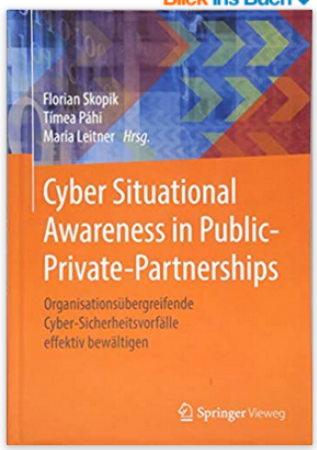
BUCHTIPP 1: LAGEBILD

Bücher Erweiterte Suche Stöbern Amazon Charts Bestseller & mehr Neuheiten Hörbücher Fremdsprachige Bücher Taschenbücher Fachbücher Schulbücher Angebote

Cyber Situational Awareness in Public-Private-Partnerships und über 8 Millionen weitere Bücher verfügbar für **Amazon Kindle**. Erfahren Sie mehr

‹ Zurück zu den Ergebnissen

Blick ins Buch



Alle 2 Bilder anzeigen

Dem Autor folgen

Florian Skopik ✓ Folgend

Cyber Situational Awareness in Public-Private-Partnerships: Organisationsübergreifende Cyber-Sicherheitsvorfälle effektiv bewältigen

Gebundenes Buch – 18. Oktober 2018

von Florian Skopik (Herausgeber), Tímea Páhi (Herausgeber), Maria Leitner (Herausgeber)

› Alle 2 Formate und Ausgaben anzeigen

Kindle 34,99 € | **Gebundenes Buch 44,99 €**

Lesen Sie mit unserer **kostenfreien App**

Lieferung Montag, 21. Okt.: Bestellen Sie innerhalb 8 Stdn. und 4 Min. per **Premiumversand** an der Kasse. Siehe Details.

22 neu ab 44,99 € | 5 gebraucht ab 22,96 €

Digitale Dienste werden für unsere Gesellschaft immer wichtiger, daher gelangen sie auch stärker ins Visier von Wirtschaftskriminellen, Spionen, Terroristen oder staatsfeindlichen Gruppierungen. Wie schützen sich Unternehmen und Staaten vor solchen Cyber-Attacken? Ein wichtiger Grundstein ist die Schaffung von Behörden, wie sie die EU-Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen (NIS) vorsieht.

‹ Mehr lesen

Falsche Produktinformationen melden

Die BILD-Bestseller
Entdecken Sie die 20 meist verkauften Bücher aus den Bereichen Belletristik und Sachbuch. Wöchentlich aktualisiert. Hier klicken.

Teilen

Neu kaufen
44,99 €
Alle Preisangaben inkl. deutscher USt. Weitere Informationen.

Kostenlose Lieferung

Auf Lager.
Verkauf und Versand durch Amazon.

Menge: 1

In den Einkaufswagen

Jetzt kaufen

Liefern an Florian - 2000 Stockerau

Gebraucht kaufen
22,96 €

Auf die Liste

Andere Verkäufer auf Amazon

27 Angebote ab 22,96 €

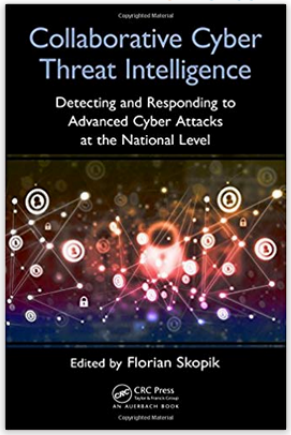
BUCHTIPP 2: CYBER THREAT INTELLIGENCE

Bücher Erweiterte Suche Stöbern Amazon Charts Bestseller & mehr Neuheiten Hörbücher Fremdsprachige Bücher Taschenbücher Fachbücher Schulbücher Angebote

Collaborative Cyber Threat Intelligence: Detecting and Re... und über 8 Millionen weitere Bücher verfügbar für **Amazon Kindle**. Erfahren Sie mehr

‹ Zurück zu den Ergebnissen

Blick ins Buch



Dieses Bild anzeigen

Dem Autor folgen

Florian Skopik ✓ Folgend

Collaborative Cyber Threat Intelligence: Detecting and Responding to Advanced Cyber Attacks at the National Level (Tayl70) (Englisch) Gebundenes Buch – 11. Oktober 2017

von Florian Skopik (Herausgeber)

1 Sternebewertung

› Alle 2 Formate und Ausgaben anzeigen

Kindle	Gebundenes Buch
51,30 €	68,64 €

Lesen Sie mit unserer **kostenfreien App**

Lieferung Donnerstag, 24. Okt.: Bestellen Sie innerhalb 22 Stdn. und 31 Min. per **Premiumversand** an der Kasse. Siehe Details.

9 neu ab 66,79 €

Threat intelligence is a surprisingly complex topic that goes far beyond the obvious technical challenges of collecting, modelling and sharing technical indicators. Most books in this area focus mainly on technical measures to harden a system based on threat intel data and limit their scope to single organizations only. This book provides a unique angle on the topic of national cyber threat intelligence and security information sharing. It also provides a clear view on ongoing works in research laboratories

‹ Mehr lesen

Falsche Produktinformationen melden

Die BILD-Bestseller
Entdecken Sie die 20 meist verkauften Bücher aus den Bereichen Belletristik und Sachbuch. Wöchentlich aktualisiert. Hier klicken.

Teilen

68,64 €
Alle Preisangaben inkl. deutscher USt.
Weitere Informationen.

Kostenlose Lieferung

Nur noch 1 auf Lager
Verkauf und Versand durch Amazon.

In den Einkaufswagen

Jetzt kaufen

Liefern an Florian - 2000 Stockerau

Auf die Liste

Andere Verkäufer auf Amazon

66,79 € In den Einkaufswagen
+ 1,00 € Versandkosten
Verkauft von: Book Depository DE

64,51 € In den Einkaufswagen
+ 4,99 € Versandkosten
Verkauft von: Blackwell's UK

BESTEN DANK FÜR IHRE AUFMERKSAMKEIT!

Florian Skopik, 26.11.2019

florian.skopik@ait.ac.at