



## PRESSEMITTEILUNG

### **Intelligente Bedrohungsanalyse durch Big Data Security Intelligence Ansatz von canacoon**

Berlin, 08. Mai 2014 — Die Sicherheitsgefahren, denen heutige IT-Infrastrukturen ausgesetzt sind, sind zunehmend unüberschaubar. Viele Bedrohungen und Sicherheitslücken bleiben oft lange unentdeckt, was Schäden noch vergrößert. Moderne SIEM (Security Information and Event Management)-Systeme sind geeignet, um aus einer großen Menge Daten mittels vorgegebener Analysewerkzeuge und Regelsätze viele sicherheitsrelevante Vorkommnisse zu entdecken und zu melden. Leistungsfähige SIEM-Lösungen leisten somit einen Beitrag zum Schutz des Unternehmens. Ihr Nutzen und Erfolg beruht auf sehr breit gestreutem, produktspezifischem Know-how, einer durchdachten Installation, gründlicher Planung und vor allem viel Wissenshintergrund aus Angreifer- und Prozesssicht. Erst dieses Wissen führt zu dem Nutzen, den man typischer Weise aus SIEM-Systemen erwartet. Die Lösungen der canacoon GmbH setzen darüber hinaus auf algorithmengestützte Mustererkennungs- und Prognoseverfahren, auch als Data Mining bekannt. Hierbei werden IT-Security Technologien und Methodiken genutzt, die im Big Data Umfeld entwickelt wurden, um riesige Datenmengen zu managen und weitgehend ohne menschliches Zutun auszuwerten. canacoon hat hierfür nun den Ansatz Big Data Security Intelligence (BDSI) entwickelt. Dieser ermöglicht Unternehmen viel effektiver als unter Einsatz herkömmlicher SIEM-Systeme auf Veränderungen reagieren zu können, wie sie für Bedrohungen typisch sind, da selbstlernende Systeme Angreifer schneller erkennen. Bestimmte Verfahren erlauben sogar Prognosen von zukünftigen Angriffen und damit proaktive Maßnahmen, bevor erste Schäden zu verzeichnen sind.

#### **Angriff, Erkennbarkeit und intelligente Abwehr**

Kreative Hacker folgen einer gewissen aufeinander aufbauenden Logik. Es gibt Abhängigkeiten und Reihenfolgen, die eingehalten werden müssen, damit ein Angriff funktionieren kann. Kleine, technisch bedingte oder bewusst zur Verschleierung gedachte Variationen erschweren es allerdings klassischen, regelbasierten SIEM-Systemen, solche Attacken zu erkennen. Gleiches gilt für Änderungen innerhalb der Zielsysteme. Big Data



Security Intelligence von canacoon hat zum Ziel, neue Sicherheitslücken, die bisher nur mit deutlicher Verzögerung bemerkt wurden und ein Unternehmen daher oft lange Zeit verwundbar ließen, frühzeitig zu erkennen. Es liegt in der Natur der Materie, dass Angreifer immer ein Stück voraus sind. Mit Hilfe von Big Data Security Intelligence lässt sich dieser Abstand jedoch signifikant und effizient verringern, weil selbstlernende und Zusammenhänge erkennende Systeme potentielle und bestehende Risiken zielgerichtet aufspüren.

**Weitere Informationen:** <https://www.canacoon.com/BDSI>

**Bildmaterial:** <https://www.canacoon.com/presse/mediaservice/>

Zeichenzahl: 2.724

#### **Über canacoon**

canacoon ist spezialisiert auf die Erbringung von Beratungsdienstleistungen im Bereich von geschäfts- und lösungsorientierter Informations- und IT-Sicherheit. Zum Portfolio gehört die gesamte Kette von der Ermittlung und Definition von Anforderungen, über die Entwicklung von Strategien, Analyse und Konzeption von Prozessen und effektivem Change Management bis hin zur technisch fundierten Beratung für die geschäfts- und risikogerechte Absicherung von Architekturen und Systemen. Nähere Infos unter [www.canacoon.com](http://www.canacoon.com)

**Social Media:** Verbinden Sie sich mit canacoon per Xing:  
<https://www.xing.com/companies/canacoongmbh>

#### **Pressekontakt:**

canacoon GmbH  
Am Borsigturm 9  
13507 Berlin  
Stefan Tewes  
Tel. +49 171 1931796  
[stefan.tewes@canacoon.com](mailto:stefan.tewes@canacoon.com)

Stemmermann – Text & PR  
Hinter dem Rathaus 1  
23966 Wismar  
Tanja Stemmermann  
Tel. +49 3841 22 43 14  
[info@stemmermann-pr.de](mailto:info@stemmermann-pr.de)