

---

## - Hiwi-Stelle -

### Entwicklung eines modularen sFlow-Kollektors

---

<b>CASED</b>	<p>Das neue Forschungs- und Entwicklungszentrum für IT-Sicherheit CASED (Center for Advanced Security Research Darmstadt) stellt sich mit seinen starken Partnern – der Technischen Universität Darmstadt, dem Fraunhofer Institut für Sichere Informationstechnologie und der Hochschule Darmstadt – einer immensen Herausforderung: In einer einzigartigen Kooperation von Informatikern, Ingenieuren, Physikern, Juristen und Betriebswirten, mit internationalen Forschungszentren und Industriepartnern, werden zukunftsweisende IT-Sicherheitslösungen erforscht, entwickelt und in die Anwendung und wirtschaftliche Verwertung gebracht.</p>						
<b>Hintergrund</b>	<p>Die Forschungsgruppe Internetsicherheit untersucht Möglichkeiten der Verwendung von Netzwerk-Flowdaten – 5-Tupel bestehend aus Quell- und Ziel-IP Adressen, Quell- und Ziel-Ports, Layer 4 Protokoll ID sowie Informationen über die Intensität des Datenverkehrs (Bit/s, Pakete/s) – zur Botnetz- und Anomalie-Detektion. Bei sFlow handelt es sich um eine Technologie und ein Dateiformat, mit dem Netzwerkverkehr in Echtzeit stichprobenartig von Netzwerkkomponenten (Routern, Switches) an Kollektoren exportiert werden kann. Der Umfang (Anzahl Bytes) der exportierten Daten ist hierbei konfigurierbar.</p>						
<b>Aufgabenstellung</b>	<p>Im Rahmen dieser Tätigkeit soll ein sFlow-Kollektor zum Empfangen und Speichern von sFlow Datagrammen (UDP) entwickelt werden. Hierbei steht insbesondere die Entwicklung einer modularen Architektur im Vordergrund, die das Integrieren von Verarbeitungskomponenten und somit das Abbilden diverser Pipelines zur Datenanalyse unterstützt. Nach erfolgreicher Entwicklung des Kollektors soll ein Modul zur Erzeugung Netflow-äquivalenter Daten auf Basis der empfangenen sFlow-Daten implementiert werden. Ferner soll die Möglichkeit bestehen, die erzeugten Netflowdaten über ein Netzwerk zu versenden.</p>						
<b>Voraussetzungen</b>	<ul style="list-style-type: none"><li>• Kreatives, eigenständiges und engagiertes Arbeiten</li><li>• Kommunikationsbereitschaft</li><li>• Gute Programmierkenntnisse (z.B. C, Perl, Ruby)</li><li>• Gute Kenntnisse gängiger Internetprotokolle</li><li>• Linux-Kenntnisse sind vorteilhaft</li><li>• Sehr gute deutsche und/oder gute englische Sprachkenntnisse</li></ul>						
<b>Starttermin</b>	<ul style="list-style-type: none"><li>• Ab sofort</li><li>• Ab 8 Stunden / Woche, Heimarbeit möglich</li></ul>						
<b>Kontakt</b>	<table><tr><td><b>Sebastian Abt</b></td><td>CASED</td></tr><tr><td>sebastian.abt@h-da.de</td><td>Mornwegstraße 32</td></tr><tr><td>06151.16-8416</td><td>64293 Darmstadt</td></tr></table>	<b>Sebastian Abt</b>	CASED	sebastian.abt@h-da.de	Mornwegstraße 32	06151.16-8416	64293 Darmstadt
<b>Sebastian Abt</b>	CASED						
sebastian.abt@h-da.de	Mornwegstraße 32						
06151.16-8416	64293 Darmstadt						