

## "Die Zukunft der Cyber-Sicherheit liegt darin, den Bedrohungskontext zu verstehen

Kommentar von Craig Carpenter, Chief Security Strategist bei AccessData, zur Übernahme von ThreatGRID durch Cisco <br /><br />"Die Zukunft der Cyber-Sicherheit liegt darin, den Bedrohungskontext zu verstehen"<br />Die Übernahme von ThreatGRID durch Cisco bestätigt eine aktuelle Entwicklung in der IT-Security-Landschaft, die zeigt: Die Zukunft der Cyber-Sicherheit liegt nicht nur im reinen Aufspüren von Bedrohungen, sondern auch darin, den Kontext zu verstehen, dessen es zum Aufspüren raffinierter Angreifer bedarf. Denn diese haben in der Vergangenheit präventive Abwehrmaßnahmen umgangen. Fest steht auch, dass das Aufspüren einer Bedrohung nicht genug ist. Allein große Unternehmen bekommen täglich Hunderte oder Tausende von Sicherheitswarnungen. <br />Infolgedessen haben Chief Information Security Officers (CISOs) erkannt, dass es gleichermaßen wichtig ist, die Intensität und den Kontext von Bedrohungen zu betrachten. Ziel ist es, nur noch wenige Warnungen von einer entsprechenden Lösung zu erhalten. Etliche Warnungen erweisen sich jedoch als zu ungenau. ThreatGRID bietet das nötige Wissen, um den Kontext zu erfassen und diesen im Anschluss auf die Lösungen und Services von Cisco anzuwenden. <br />Kunden erwarten mehr<br />Die Erweiterung des Cisco-Portfolios um die solide Bedrohungsanalyse von ThreatGRID ist ein cleverer Schritt und zugleich Teil einer größeren Entwicklung. Bedeutende Anbieter wie Cisco und FireEye begreifen allmählich, dass Kunden mehr erwarten als nur Lösungen für ein Puzzleteil, etwa Datenverkehr im Netzwerk ohne Endgeräteabdeckung oder Störungserfassung ohne automatisierte Reaktion. <br />Die Sicherheitsindustrie erlebt gerade eine tektonische Verschiebung und steuert auf eine vollständig integrierte TDR-Lösung (Threat Detection <br> Response) zu, um ein breites und tiefgehendes Bewusstsein der Situation für alle wesentlichen sichtbaren Punkte (Netzwerk, Endgeräte, Protokollierungseinrichtungen) zu erlangen. Die ganzheitliche Kontrolle über sämtliche Produkte innerhalb und außerhalb von Unternehmensnetzwerken, die mit einer erweiterten Bedrohungsanalyse ausgestattet sind, sorgt für einen guten Überblick. Leider dauert es mehrere Jahre, um diese Lösungspakete in geschlossene Plattformen zu integrieren, in denen eine Bedrohungsanalyse ihr volles Potenzial entfalten kann. <br />Die angestrebte ultimative Vision von geschlossenen und integrierten Plattformen an Stelle von einzelnen Produkten ist wichtig. Gemäß Berichten zur Untersuchung von Datenpannen wie etwa dem Verizon Data Breach Investigation Report (DBIR) erfolgt die Mehrheit der Angriffe - von der Infiltrierung bis hin zum Datendiebstahl - innerhalb von Sekunden, Minuten oder Stunden. Unternehmen, die sich für eine Security-Plattform entschieden haben, sollten in der Lage sein, Bedrohungen zu verstehen und automatisierte Maßnahmen zu ergreifen, die die Dauer von Angriffen erheblich verkürzen. Dadurch entfallen eine Vielzahl erforderlicher manueller Prüf- und Reparaturschritte, bevor die Angreifer ihr Ziel erreichen. Durch die erfolgreiche Cyberspionage und die immer häufigeren Hackerangriffe ist es für die Sicherheitsindustrie nun an der Zeit, Continuous Automated Incident Resolution (CAIR) als Lösung für diese Ära des kontinuierlichen Kompromisses anzunehmen. <br />Über AccessData:<br />Die AccessData Group ist seit 25 Jahren Wegbereiter für Entwicklungen im Bereich der digitalen Ermittlungen und entsprechender Unterstützung in Rechtsstreitigkeiten. Die Produktfamilie besteht aus Stand-Alone- und Enterprise-Class-Lösungen mit dem Fokus auf Digital Forensik, E-Discovery und Cyber Security. Hierzu gehören unter anderem die Produkte FTK, SilentRunner, Summation und das CIRT Security Framework. Sie ermöglichen digitale Untersuchungen jeder Art, wie z.B. Computerforensik, Vorfallsanalyse, Hosted Review Services, rechtliche Nachprüfungen und Compliance-Audits. Mehr als 100.000 User, die weltweit im Gesetzesvollzug, in Regierungsbehörden, Unternehmen und Rechtsanwaltskanzleien etc. tätig sind, vertrauen bereits auf die AccessData Software-Lösungen. AccessData ist zudem Anbieter für Trainings und Zertifizierungen in den Bereichen digitale Forensik und Rechtsstreitigkeiten. Weitere Informationen unter [www.accessdata.com](http://www.accessdata.com) <br /><br />AccessData Group<br />Nicole Reid<br />International Marketing Manager<br />1 Bedford Street<br />3rd Floor<br />E-Mail: [nreid@accessdata.com](mailto:nreid@accessdata.com)<br />Internet: [www.accessdata.com](http://www.accessdata.com) <br />London<br />Ansprechpartner (in Deutschland):<br />Abdeslam Afras<br />Director, EMEA <br> India<br />E-Mail: [aafra@accessdata.com](mailto:aafra@accessdata.com) <br />

### Pressekontakt

AccessData Group

84042 Lindon, UT

[nreid@accessdata.com](mailto:nreid@accessdata.com)

### Firmenkontakt

AccessData Group

84042 Lindon, UT

[nreid@accessdata.com](mailto:nreid@accessdata.com)

Weitere Informationen finden sich auf unserer Homepage