Neue InSight-Plattform von AccessData vereint Enterprise Investigations, Cyber Security und e-Discovery

Neue InSight-Plattform von AccessData vereint Enterprise Investigations, Cyber Security und e-Discovery

In Echtzeit Sicherheitsbedrohungen erkennen, analysieren und lösen
Cyber-Security-Experte AccessData hat eine gemeinsame Arbeitsoberfläche für Legal-, Security- und Internal Investigations-Teams veröffentlicht. Die Plattform InSight kombiniert Netzwerk-, Endpoint- und Malware-Analyse, alle e-Discovery-Phasen sowie Reaktionsmaßnahmen in einer skalierbaren Lösung. Den technologischen Kern bildet die ThreatBridge Engine; außerdem ermöglicht die Integrierbarkeit mit SIEM(Security Information und Event Management)-Lösungen ein 360-Grad-Monitoring. Durch die ganzheitliche Einsicht in das Netzwerk inklusive mobiler Endgeräte lassen sich Bedrohungen umgehend erkennen, analysieren und lösen. Dabei können im virtuellen "War Room" Experten aus den Bereichen Compliance, Incident Reponse, Forensik, Recht, etc. gleichzeitig an Security-Vorfällen arbeiten.
IT-Abteilungen sehen sich mit immer komplexer werdenden Cyber-Angriffen konfrontiert und sind diesen schon jetzt kaum mehr gewachsen. Das liegt unter anderem auch an unzureichenden Security-Lösungen, die nicht miteinander verzahnt arbeiten. Immer mehr CISOs (Chief Information Security Officers) beschränken sich daher darauf, kompromittierte Systeme nur zu reparieren, ohne den Ursachen auf den Grund zu gehen. Dadurch können sich diese Vorfälle allerdings wiederholen, indem sie sich Schwachstellen zunutze machen.
Die Ursache finden
Dem wirkt die InSight-Plattform entgegen, die als erste am Markt verfügbare Lösung dieser Art die Erkennung, Analyse und Behebung von Security-Vorfällen bündelt. Sobald sie Bedrohungen ausmacht, stellt sie Informationen rund um Endpoint- und Netzwerk-Forensik, kontextuelle Daten und weitere Resultate übersichtlich zusammen. Darauf aufbauend lassen sich umgehend intensive Analysen durchführen. Die Lösung basiert auf Technologien aus Cyber Security-, Forensik- und e-Discovery-Produkten. Durch diese Kombination ist InSight in der Lage, Gefahren präzise zu erkennen. Darüber hinaus verschafft sie dem IT-Team transparente Einblicke in den kompletten Netzwerk-Traffic und Endpoint-Daten, inklusive aller vorhandenen Mobilgeräte.
Nahtlose Integration in Security-Umgebungen
Im Zusammenspiel mit anderen SIEM (Security Information and Event Management)-Produkten ermöglicht InSight ein 360-Grad-Monitoring. AccessData nennt dieses Vorgehen "Continous Automated Incident Response" (CAIR): eine permanente, automatisierte Vorgehensweise gegen Security-Vorfälle. Über eine bi-direktionale Kommunikation zwischen den Elementen lassen sich dabei sowohl über InSight als auch über die SIEM-Lösung Gegenmaßnahmen ergreifen. Für noch schnellere Reaktionen ist es möglich, wiederkehrende Schritte innerhalb der Plattform zu automatisieren.
"Die herkömmliche Incident-Response-Infrastruktur ist zumeist ein Flickenteppich bestehend aus Netzwerk-, Endpoint- und SIEM-Tools, die nicht ausreichend gut zusammenarbeiten', kommentiert Ben-Oni Golan, CSO und SVP Network Architecture bei IDT Telecom. "Verlässliche Sicherheit benötigt automatisierte Reaktionen in Echtzeit. Die Integration unserer vorhandenen SIEM-Lösung mit der AccessData InSight-Plattform hat unsere Reaktionszeiten von rund 12 Stunden auf nur knapp 2,5 Stunden verringert - das ist eine 80%-ige Reduzierung."
Vielfältige Mechanismen zur Gefahrenerkennung
Kern von InSight ist die ThreatBridge Engine, die verschiedene Informationsquellen nutzt, um gegen Attacken vorzugehen. Das Know-how speist sich u.a. aus Listen der gefährlichsten IP-Adressen weltweit (z.B. Norse Darklist), Tools für Malware-Scans und -analysen (z.B. ThreatGRID, VirusTotal, YARA) sowie OpenIOC, einem Framework für "Indicators of Compromise" (Kompromittierungsindikatoren). Über das Endpoint Threat Monitoring können CISOs Vorfälle aufzeichnen und mittels der Playback-Funktion nochmals ansehen.
Rechtsfälle strukturiert aufbereiten
Neben der Security-Komponente bietet InSight des Weiteren essenzielle e-Discovery-Funktionen. Integriert ist dazu unter anderem Summation von AccessData, eine professionelle Datenaufbereitungs- und Management-Software für Rechtsanwälte und Rechtsabteilungen. Über InSight lassen sich abteilungsübergreifend z.B. Daten sammeln und weiterverarbeiten, Beweissicherungsverfahren abwickeln, Fälle verwalten sowie Reviews durchführen.
Weitere Informationen über die InSight-Plattform sind unter http://accessdata.com/insight-platform/ zusammengestellt. Ein Video zur Funktionsweise ist im Youtube Channel von AccessData verfügbar.
Über AccessData:
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 Rechtanwaltskanzleien 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 .

Weitere Informationen:
AccessData Group
Nicole Reid
International Marketing Manager
1 Bedford Street
3rd Floor
London
E-Mail: nreid@accessdata.com
Internet: www.accessdata.com
Ansprechpartner (in Deutschland):
Abdeslam Afras
Regional Manager Continental Europe
E-Mail: aafras@accessdata.com
PR-Agentur:
Sprengel
 Partner GmbH
Nisterstraße 3
D-56472 Nisterau
 www.sprengel-pr.com
Ansprechpartner:
Olaf Heckmann
Marius Schenkelberg
Tel.: +49 (0)26 61-91 26 0-0
Fax: +49 (0)26 61-91 26 0-29
E-Mail: ms@sprengel-pr.com
<img src="http://www.pressrelations.de/new/pmcounter.cfm?n_pinr_=560474" width="1" height="1">

Pressekontakt

AccessData Group

84042 Lindon, UT

nreid@accessdata.com

Firmenkontakt

AccessData Group

84042 Lindon, UT

nreid@accessdata.com

Weitere Informationen finden sich auf unserer Homepage