CyCognito präsentiert erweitertes Exploit Intelligence-Modul für seine External Attack Surface & Risk Management Plattform auf der it-sa 2022 in Nürnberg

Sandbox Virtual Lab: Branchenweit erste Sandbox-Testumgebung, die in External Attack Surface & Risk Management-Lösung integriert ist - für eine sichere Remediation

-- CyCognito-Plattform ermöglicht proaktive, kontinuierliche und automatisierte Überwachung der externen Angriffsfläche, die Unternehmen über aus dem Internet erreichbare Assets bieten

-- Wie das externe Cyber-Risiko beherrschbar wird, zeigt CyCognito auf der führenden IT-Sicherheitsmesse in Halle 7, Stand 7-603

PALO ALTO/NÜRNBERG, 25. Oktober 2022 --- Auf der it-sa in Nürnberg präsentiert CyCognito, Marktführer für External Attack Surface & Risk Management (EASM), ein erweitertes Exploit Intelligence-Modul für seine leistungsstarke EASM-Plattform, mit der IT-Sicherheitsteams die kritischsten Cyberrisiken in ihrer externen Angriffsfläche priorisieren und schneller entschärfen können. Dieses Add-on nutzt die Datenbanken von CISA (U.S. Cybersecurity and Infrastructure Security Agency) und vom FBI sowie weitere Threat-Intelligence-Quellen und bezieht auch beobachtete Aktivitäten von Angreifern mit ein. CyCognito identifiziert präzise die Cyber-Bedrohungen mit dem für das individuelle Unternehmen höchsten Gefahrenpotenzial und ermöglicht ein gezieltes Risikomanagement.

Ein Highlight des neuen Exploit Intelligence-Moduls ist die branchenweit erste integrierte Sandbox-Testumgebung für EASM. Dank dem Sandbox Virtual Lab können Security-Verantwortliche simulieren, ob sich ein bestimmtes Asset kompromittieren lässt, wie Angreifer dafür vorgehen würden und welche Auswirkungen das ganz konkret hätte. Darüber hinaus ermöglicht die Sandbox das Testen von über das Internet erreichbaren Assets, um ein ordnungsgemäßes Patching sicherzustellen.

Sandbox Virtual Lab konzentriert sich aktuell auf die kritische Sicherheitslücke in der Java-Logging-Bibliothek Log4j, die immer noch eine der am weitest verbreiteten Bedrohungen ist. Die Simulation von Threats wie Log4Shell, ProxyShell, ProxyLogon und ZeroLogon wird in den kommenden Monaten möglich sein.

"Das Exploit Intelligence-Modul von CyCognito füllt die Lücke zwischen Threat Intelligence und Vulnerability Management", erklärt Dr. Georg Hess, Regional Sales Director DACH bei CyCognito. "Unsere Plattform identifiziert nicht nur Schwachstellen in betroffenen Assets, sondern gibt klare Empfehlungen, welche davon mit welcher Priorität behoben werden sollten - im Sinne eines konsequenten Risikomanagements. Denn manche Schwachstellen sind für Angreifer attraktiver als andere. Und weil sich die externen Cyber-Angriffsflächen von Unternehmen immer komplett unterscheiden, beleuchtet die CyCognito-Lösung ganz gezielt die individuelle externe Angriffsfläche - und das aus den gefundenen Schwachstellen resultierende Gefahrenpotenzial. Wir freuen uns darauf, unsere leistungsfähige Plattform und das erweiterte Exploit Intelligence-Modul dem Fachpublikum auf der it-sa in Nürnberg vorzustellen."

Mittels der CyCognito-Plattform und dem Erweiterungsmodul Exploit Intelligence lässt sich die Mean Time to Remediation (MTTR), die durchschnittliche Zeit zur Behebung einer Schwachstelle, der risikoreichsten über das Internet erreichbaren Assets eines Unternehmens drastisch verkürzen - und damit wertvolle Zeit und Geld sparen. Die Sicherheitsteams erhalten mit der mächtigen Erkennungs- und Mapping-Engine und der integrierten Exploit Intelligence direkt umsetzbares Wissen und klare Handlungsempfehlungen. Damit können sie schnell und einfach Fixes für die wichtigsten Schwachstellen ihres Unternehmens entwickeln, testen und einsetzen - um Angreifern keine Chance zu geben.

Funktionen und Vorteile im Überblick:

-- Schnelle Remediation: Die Lösung identifiziert die Schwachstellen in Assets, die über das Internet erreichbar sind, und macht die Sicherheitsteams auf das unternehmensindividuelle Risiko aufmerksam. So lassen sich die Reaktions- und Behebungszeiten von Monaten auf Tage reduzieren.

-- Curated Intelligence: CyCognito zeigt, welche Schwachstellen wie intensiv von Angreifern in freier Wildbahn ausgenutzt werden, und ob, wie und wo diese Schwachstellen in der unternehmenseigenen externen Angriffsoberfläche vorhanden sind.

-- Schnelles Impact-Assessment: Eine einfache Folgenabschätzung ist möglich dank eines kompletten Überblicks über alle potenziell gefährdeten Assets und ihren Status - geschützt oder anfällig.

-- Verifizieren und handeln - mit Sicherheit: Im Virtual Sandbox Lab lassen sich Exploits in Assets in sicherer Umgebung testen, um das tatsächliche Risiko für einen IT-Stack zu bestimmen.

-- Threats schneller entschärfen: Integration in SIEM/SOAR, Ticketing-Tools und Remediation-Prozesse für eine optimale Mitigation/Gefahrenabwehr.

CyCognito auf der it-sa 2022 in Nürnberg

Interessierte können sich vom 25. bis 27. Oktober auf der it-sa in Nürnberg in Halle 7, Stand 7-603 über CyCognito, das neueste Exploit-Intelligence-Modul und die External Attack Surface & Risk Management-Plattform informieren. Im kostenlosen Workshop "External Attack Surface & Risk Management: Wenn Offensive zur besten Defensive wird" zeigt CyCognito am 26. Oktober um 14:30 Uhr im NCC Ost, Raum Stockholm, wie Unternehmen ihre IT-Sicherheit deutlich optimieren können. Zudem können sich Besucherinnen und Besucher im Rahmen einer Live-Demo von der Leistungsfähigkeit der Lösung überzeugen.

ca. 4.800 Zeichen

Pressekontakt

Dr. Haffa & Partner GmbH

Herr Philipp Moritz
Karlstraße 42
80333 München

haffapartner.de
postbox@haffapartner.de

Firmenkontakt

CyCognito

Herr Dr. Georg Hess
Karlstraße 42
80333 München

https://cycognito.com
georg@cycognito.com

Über CyCognito
CyCognito ist Marktführer bei External Attack Surface & Risk Management und zählt viele Fortune-2000-Unternehmen zu seinen Kunden. Von der CyCognito-Plattform profitieren aber nicht nur große Unternehmen und Konzerne, sondern auch der Mittelstand. Die Plattform erlaubt ein proaktives, kontinuierliches Management der potenziellen Angriffsfläche, die ein Unternehmen über seine mit dem Internet verbundenen Assets bietet, und hilft, die damit verbundenen Risiken zu steuern und zu minimieren.
Kontinuierliches Monitoring inklusive einem weitreichendem automatisiertem Security Testing - ohne Input seitens des Kunden - zeigt regelmäßig die jeweils vollständige Angriffsfläche einschließlich "blinder Flecken" auf. Dazu gehören beispielsweise vergessene Cloud-Assets und nicht mehr genutzte oder fehlerhaft konfigurierte IT/IoT-Infrastrukturen. Das ist jedoch nicht alles: Dank relevanter Priorisierung und umfassender Integration in bestehende Security-Prozesse und -Plattformen (SOC, SIEM, SOAR, Ticketing-Systeme) können Unternehmen mit CyCognito effektiv jeweils die zehn Security-Lücken schließen, die 90 Prozent des gesamten externen Cyber-Risikos ausmachen.

Der Hauptsitz des Unternehmens ist heute in Palo Alto. Ursprünglich stammt CyCognito aus Israel, wo sich unter anderem die R&D-Abteilung befindet.

https//www.cycognito.com

Anlage: Bild