Check Point Software schützt vor Cloud-Bedrohungen mithilfe neuer Security Analytics-Lösung

CloudGuard Log.ic bietet Bedrohungsschutz und umfangreiche Sicherheitsinformationen in der Public Cloud, sodass IT-Teams alle IaaS- und PaaS-Assets einsehen, Cloud-Aktivitäten verstehen und Bedrohungen einfach untersuchen können

SAN CARLOS, Kalifornien – 12. Juni 2019. Check Point® Software Technologies Ltd. (NASDAQ: CHKP), ein weltweit führender Anbieter von Cyber-Sicherheitslösungen, veröffentlicht CloudGuard Log.ic, eine Software, die Cloud-nativen Bedrohungsschutz und Sicherheitsinformationen bietet. Mit CloudGuard Log.ic können Kunden jeden Datenfluss und jeden Audit-Trail in den vielschichtigen Cloud-Umgebungen sehen und Cloud-Daten sowie -Aktivitäten schneller verstehen, um forensische Untersuchungen zu beschleunigen.

CloudGuard Log.ic erkennt Cloud-Anomalien, blockiert Bedrohungen wie auch Eindringlinge und liefert kontext-reiche Visualisierungen, um eine gründliche Untersuchung von Sicherheitsvorfällen in Public Cloud-Infrastrukturen, wie Amazon Web Service (AWS), zu ermöglichen. Log.ic wird Teil der Check Point CloudGuard-Familie aus Cloud-Sicherheitsprodukten.

Eine Umfrage zur Sicherheit in der Cloud, die von CyberSecurity Insiders für Check Point durchgeführt wurde, ergab, dass die grössten Bedenken, mit denen IT-Organisationen zu kämpfen haben, die Compliance (34 Prozent) und die mangelnde Transparenz der Infrastruktur-Sicherheit (33 Prozent) sind. Während die Mehrheit der Unternehmen angibt, dass ihre Cloud-Instanzen nicht gehackt wurden (54 Prozent), wussten alarmierende 25 Prozent der Befragten nicht, ob ihr Unternehmen getroffen wurde oder nicht. 15 Prozent der Unternehmen bestätigten, dass sie mindestens einen Cloud-Sicherheitsvorfall erlebt haben.

Das Herzstück von CloudGuard Log.ic ist eine Enrichment-Engine, die Daten aus einer Vielzahl von Quellen, wie VPC Flow Logs und AWS CloudTrail, sammelt, um ein starkes Sicherheitsbewusstsein in Public Cloud-Umgebungen aufzubauen. Security- und DevOps-Teams können diese schlüsselfertige Lösung nutzen, um die Reaktion auf Vorfälle und die Suche nach Bedrohungen zu beschleunigen, Sicherheitsrichtlinien zu überprüfen und diese über mehrere Konten hinweg durchzusetzen. CloudGuard Log.ic kann auch in SIEM-Lösungen von Drittanbietern, darunter Splunk und ArcSight, integriert werden.

„Einer der Hauptunterschiede in Cloud-Umgebungen ist die ephemere Natur der Elemente“, sagt Fernando Montenegro vom Marktforschungsunternehmen 451 Research: „Während Workloads und Instanzen von virtuellen Maschinen, Containern oder serverlosen Funktionen ausgeführt werden, können Informationen, die bisher als statisch galten, wie IP-Adressen, nicht mehr zuverlässig verwendet werden. Wir sehen definitiv einen Bedarf an aktuelleren Sicherheits-Tools, die neue Konzepte ab Werk verstehen und Informationen aus Flow-Logs, Load Balancern und anderen Cloud-nativen Komponenten ergänzen. Dadurch erhält die IT-Abteilung eine detailliertere Sicht auf Ereignisse, die ein genaueres Verständnis der Umgebung und eine strengere Durchsetzung der Sicherheitsregeln ermöglicht.“

Einige der wichtigsten Funktionen von CloudGuard Log.ic:

- Fortschrittliche Bedrohungsabwehr durch Interaktion mit Check Points branchenführenden ThreatCloud Intelligence-Feeds über bösartige IPs.

- Einfache Erstellung benutzerdefinierter Warnmeldungen, die durch verdächtige Netzwerk- und Benutzeraktivitäten, Compliance-Verletzungen und fehlerhafte Sicherheitskonfigurationen ausgelöst werden.

- Die Zuordnung zu Benutzern, Gruppen und Rollen wird analysiert, um auch verbundene Ereignisse zu beobachten, da Konfigurationsänderungen verfolgt und mit der Person oder Rolle korreliert werden.

- Die Berichterstattung über wichtige Ereignisse, Statistiken und Datenverkehr kann definiert und für direkte Berichte in E-Mails und verschiedenen ITMS-Tools, wie ServiceNow, PagerDuty oder Jira, geplant werden.

- CloudBots Auto-Remediation-Funktionen können verwendet werden, um automatisch auf bestimmte Warnungen vor bösartigen Aktivitäten zu reagieren und weitere Schritte, wie Quarantäne oder Tagging, für zusätzliche Untersuchungen zu automatisieren.

„CloudGuard Log.ic bietet unseren Unternehmenskunden einen leistungsstarken Einblick und Kontext in alle Aktivitäten innerhalb ihrer Cloud-Umgebung, kombiniert mit Feeds, die böswillige Absichten identifizieren oder Intrusion Detection betreiben, um Mega-Gen-V-Cyber-Sicherheitsangriffe zu verhindern“, erklärt Itai Greenberg, VP Product Management and Marketing, Check Point Software Technologies: „Mit der Erweiterung der Produktfamilie um CloudGuard Log.ic bietet Check Point seinen Kunden auch künftig die neuesten Sicherheitsprogramme zur Erkennung und Abwehr fortgeschrittener Bedrohungen in der Cloud.“

CloudGuard Log.ic ist ab sofort verfügbar. Mehr Informationen über die Lösung finden Sie unter: https://www.checkpoint.com/products/public-cloud-security-analytics/

Folgen Sie Check Point auf:
Twitter: http://www.twitter.com/checkpointsw
Facebook: https://www.facebook.com/checkpointsoftware
Blog: http://blog.checkpoint.com
YouTube: http://www.youtube.com/user/CPGlobal
LinkedIn: https://www.linkedin.com/company/check-point-software-technologies

Über Check Point Software Technologies Ltd.
Check Point Software Technologies Ltd. (www.checkpoint.com) ist ein führender Anbieter von Cyber-Sicherheitslösungen für Unternehmen und Regierungen weltweit. Seine Lösungen schützen Kunden vor Cyber-Angriffen der 5. Generation mit einer branchenführenden Fangrate von Malware, Lösegeldforderungen und anderen gezielten Angriffen. Check Point bietet eine mehrstufige Sicherheitsarchitektur mit unserer neuen Gen V Advanced Threat Prevention, die alle Netzwerke, Clouds und mobilen Operationen eines Unternehmens vor allen bekannten Angriffen schützt, und kombiniert mit dem umfassendsten und intuitivsten Single Point of Control Management System der Branche. Check Point schützt über 100‘000 Unternehmen jeder Grösse.
Check Point Alps (Schweiz und Österreich) mit Sitz in Zürich und Wien beschäftigt rund 50 Mitarbeitende.

Pressekontakt:
Check Point Software Technologies (Switzerland) AG
Sonja Meindl
Tel: +41 44 316 64 44
E-Mail: smeindl@checkpoint.com

Jenni Kommunikation
Sylvana Zimmermann
Tel: +41 44 388 60 80
E-Mail: sylvana.zimmermann@jeko.com

