CounterCraft

Datasheet

CounterCraft
The Platform™

CounterCraft

The Platform™

Aktiver Schutz für kritische Geschäftssysteme, Prozesse und Daten

Trotz hoher Investitionen in Cybersicherheit sind gezielte Cyber-Angriffe weiterhin erfolgreich.

Traditionelle Sicherheitssysteme können die Flut an Malware und bösartigen E-Mails, die Ihr Unternehmen angreifen, nicht abwehren: geübte Angreifer finden weiter einen Weg. Sie werden häufig nicht entdeckt und können so lange weitermachen, bis sie ihre Ziele erreicht haben. Sie sind unsichtbar und können ihr Unwesen treiben, ohne eine Threat Intelligence-Spur zu hinterlassen.

- CISOs stehen unter Druck, die Sicherheitsressourcen zu priorisieren.
- Die Heads von SOCs stehen vor sich ständig weiterentwickelnden und immer feindseligeren Bedrohungen und haben nur begrenzte Ressourcen zur Verfügung.
- Threat Intelligence Manager leiden unter Intel Feeds, die keinen Kontext bieten und geringe Handlungsfähigkeit zur Folge haben.

Weniger Glück für den Angreifer – Mehr Sicherheit für Sie

Verantwortliche für Sicherheits- und Risikomanagement sind berechtigterweise frustriert vom Ungleichgewicht zwischen Angriff und Verteidigung. Verteidiger müssen zu 100 % richtig liegen, während Angreifer nur ein einziges Mal das Glück haben müssen, eine Sicherheitslücke in einem ansonsten perfekt geschützten System zu finden.

Ist es an der Zeit, einen anderen Ansatz zu wählen?

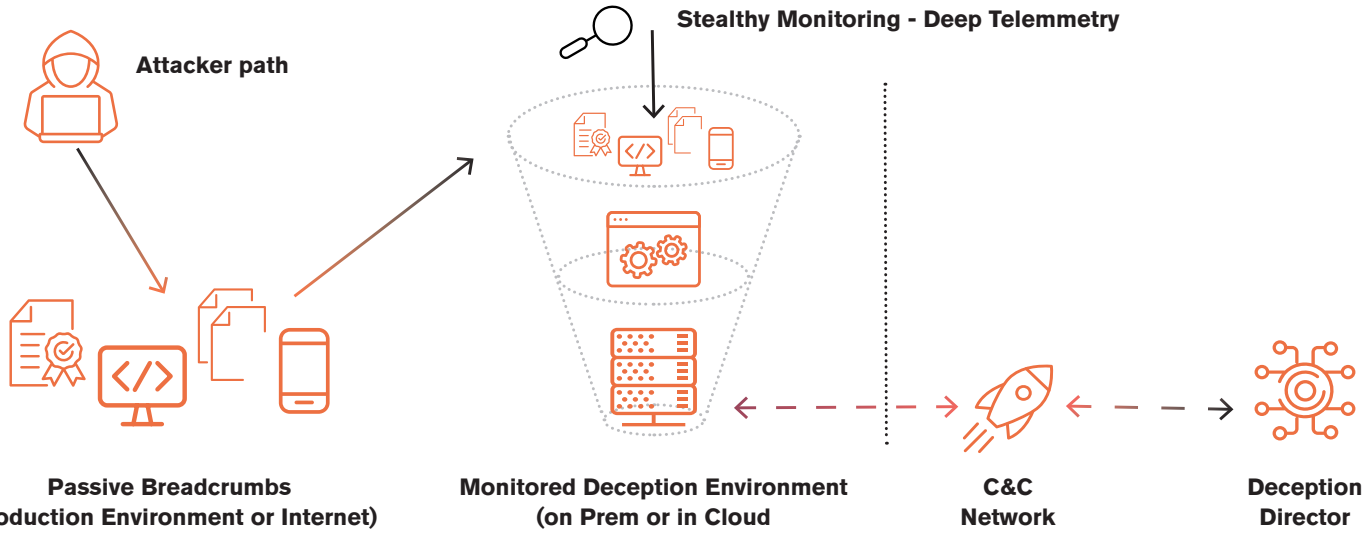
1. **Feindliche Aktivitäten früh entdecken:** Warnungen vor feindlichen Aktivitäten sind qualitativ hochwertig und werden früher als in jedem anderen System erzeugt: Entdeckung vor Beginn und während des Angriffs. Angreifer werden gezwungen, sich während der „Vorbereitungsphase“ (Planung und Reconnaissance) des Angriffs oder während des internen Lateral Movement zu erkennen zu geben.

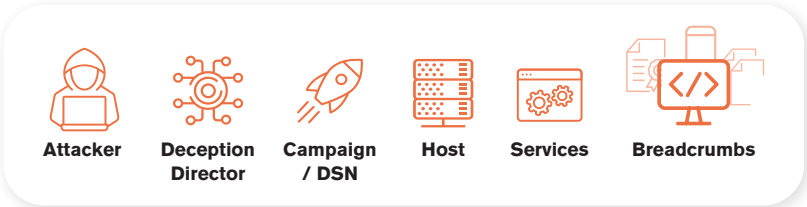
2. **Angereicherte Bedrohungsdaten sammeln:** Es werden Echtzeit-Bedrohungsdaten von den feindlichen Aktivitäten gesammelt. Die Daten werden automatisch mit TTP-, MITRE ATT&CK- und IOC-Kontextdaten angereichert. Diese Daten werden in den Threat Intel-Workflow integriert. Den Abonnenten werden wirkungsvolle Threat Intel-Feeds geliefert – gezielt und rechtzeitig.

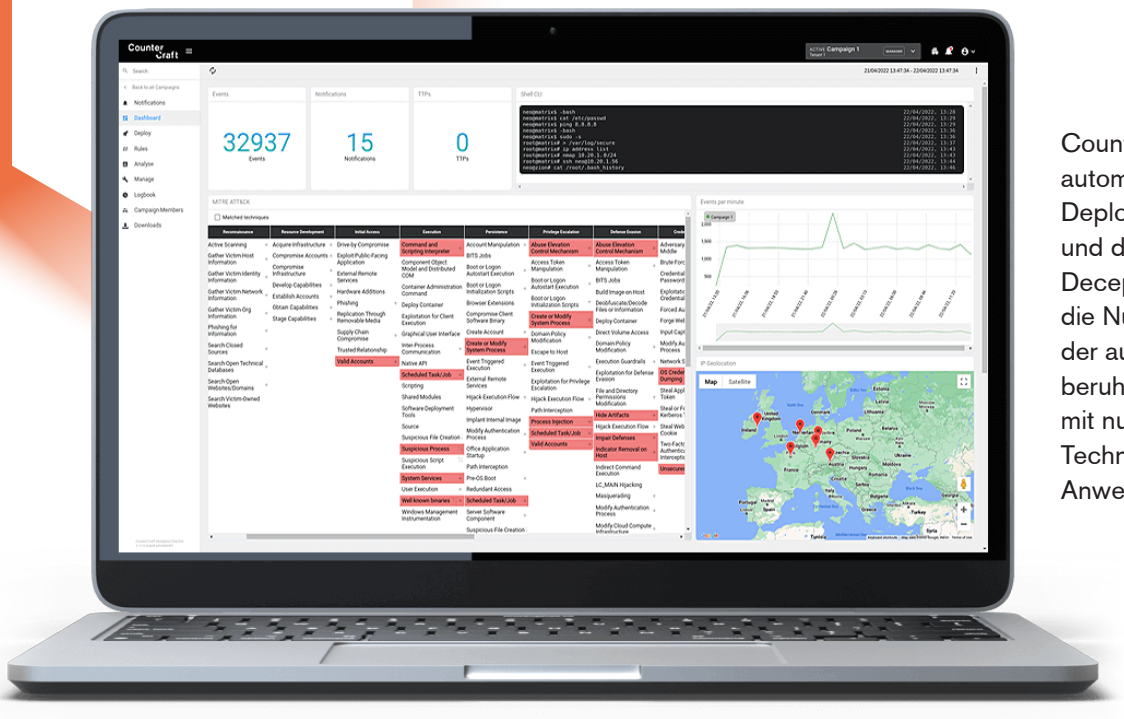
3. **Angreifer verwalten:** Integration in Intelligence- und Incident Response-Workflows. Andere Geschäftssysteme werden sofort neu konfiguriert, um dem Angriff standzuhalten. Es wird direkt und in Echtzeit mit dem Angreifer interagiert, um den Angriff zu verwalten, hinauszuzögern und abzuwenden, damit mehr Intelligence-Daten vom Angreifer gewonnen werden können.

So funktioniert es

Die Technologie der Distributed Deception errichtet eine künstliche Umgebung, die Angreifer dazu bringt, mit falschen Informationen und gefälschten digitalen Assets zu interagieren, anstatt echte Betriebssysteme und Daten anzugreifen. Während Angreifer einen Weg durch das Netzwerk suchen, gewinnen Sie detaillierte Informationen über ihre Taktiken, Techniken und Prozeduren (TTPs).







CounterCraft **The Platform**™ automatisiert das Design, das Deployment, die Überwachung und die Instandhaltung von Deception-Umgebungen. Durch die Nutzung eines Ansatzes, der auf Deception-Kampagnen beruht, können Sie ganz einfach mit nur einem Klick die Deception-Technologie für spezifische Anwendungsfälle einsetzen.

Geschäftsvorteile

Früh erkennen

↓

Mehr Zeit, um auf den Angriff zu reagieren

↓

Verbesserte Cyber-Resilienz

Threat Intel sammeln

↓

Aktionen und Entscheidungen priorisieren

↓

Reduzierte Kosten

Angreifer verwalten

↓

Sicherheitssysteme in Echtzeit anpassen

↓

Vermeidung von Störungen durch Angriffe

Ein einzigartiger Ansatz für aktive Verteidigung:

Größte Abdeckung – Funktioniert innerhalb und außerhalb der traditionellen Unternehmensgrenze. Vollständig Cloud-integriert. Leichtes Einrichten von Pufferzonen für gefährdete Cloud-Assets.

Reibungslos – Host-basiert mit Integration in die Cloud-Infrastruktur – muss nicht an die interne Netzwerk-Ausstattung angeschlossen werden.

Hochautomatisiert – Hochautomatisierte Deployment- und Management-Prozesse sorgen für reduzierte Ressourcennutzung.

Einsatzbereit – Vorinstallierter Katalog mit Anwendungsfällen für führende Deception. Auch Laien können das System ohne Weiteres verwenden.

Flexibilität bezüglich Anwendungsfällen – Ein kampagnenbasierter Ansatz für die Deception ermöglicht das Deployment verschiedener Anwendungsfälle mit nur einem Tool.

Angreifer-Mapping – Warten Sie nicht, bis der Angreifer in Ihr Netzwerk eingedrungen ist. Seien Sie dem Angreifer einen Schritt voraus und verstehen Sie seine TTPs und strategischen Treiber.

About Us

CounterCraft is a software company that goes beyond detection and response to provide proactive cybersecurity solutions and detect attacks faster for the world's leading organizations. Their premier product, CounterCraft **The Platform™**, consistently stops red teams, spear phishing, ransomware attacks and insider threats. This distributed deception platform is a global leader in active defense, with tooling that provides real-time intelligence and the capability to manipulate adversary behavior. Their technology stops attackers in pre-breach recon phases, integrates contextualized threat intel with incident response workflows, and saves money and time by helping security teams prioritize their actions. CounterCraft The Platform is used successfully around the globe by Fortune 500 companies and government organizations, including the US Department of Defense.

Find out more. Request a demo at countercraftsec.com