Whitepaper

Deception Technology

als unverzichtbare Komponente des zukunftsfähigen SOC

Kurzfassung

Angesichts immer raffinierterer Angriffsmethoden, zunehmender Kosten und Risiken rund um Datensicherheit und einer sich stetig verschärfenden Bedrohungslage wächst auch die Nachfrage nach „SOCs der nächsten Generation“. Was ist darunter konkret zu verstehen?

Grundsätzlich handelt es sich um einen Sammelbegriff, der eine Vielzahl von Anwendungsfällen abdeckt: von einfacher Log-Aggregration und statischer Bedrohungserkennung bis hin zu proaktiven Erkennungsmodellen mit geringer Fehlalarmquote und umfassenden Analytikfunktionen, die aus Daten Informationen gewinnen, und hochgradig automatisierten Reaktionsmechanismen.

Das Prinzip der Deception-Technologie basiert auf dem Grundgedanken, Erkenntnisse über die Absichten und Taktiken des Angreifers zu gewinnen. Viele entscheidende Funktionen eines SOC der nächsten Generation sind daher in ihrem Leistungsumfang inbegriffen.

In diesem Whitepaper werden eine Reihe effektiver und praxiserprobter Maßnahmen vorgestellt, wie Sie Deception-Technologie zur Optimierung vorhandener Monitoring-Funktionen einsetzen, damit Ihre Organisation Bedrohungen künftig schneller, präziser und zuverlässiger abwehren kann.

Das Prinzip der Deception-Technologie basiert auf dem Grundgedanken, Erkenntnisse über die Absichten und Taktiken des Angreifers zu gewinnen. Viele entscheidende Funktionen eines SOC der nächsten Generation sind daher in ihrem Leistungsumfang inbegriffen.

Kernpunkte

- Die effektive Erkennung und Bekämpfung komplexer Bedrohungen setzt voraus, dass Security Operations Centers nach der Prämisse des Misstrauens als Grundannahme handeln und immer davon ausgehen, dass bereits eine Sicherheitsverletzung vorliegt.
- Durch proaktive Abwehrmaßnahmen wie Deception-Technologie und Threat Hunting drehen Sicherheitsbeauftragte den Spieß um, drängen Angreifer in die Defensive und verlagern die finanzielle und kognitive Belastung vom intendierten Opfer auf den Täter.
- False Positives und unzuverlässige Daten sind ein Störfaktor, der die Effizienz herkömmlicher SOCs empfindlich beeinträchtigt. Deception-Technologie zeichnet sich im Vergleich zu sämtlichen Alternativen durch eine niedrigere Fehlalarmquote aus, da jede Interaktion mit einer Decoy-Ressource per se verdächtig ist.
- Sicherheitsteams profitieren von einer niedrigen Fehlalarmquote, die die automatische Orchestrierung von Maßnahmen zur Vorfallbekämpfung ohne menschliches Eingreifen ermöglicht.
- Bei Interaktionen mit Decoy-Ressourcen handelt es sich immer um böswillige bzw. anomale Aktivitäten. Die Analyse der dabei erfassten Daten liefert aussagekräftige Erkenntnisse zu akuten Bedrohungen, die eine schnelle Reaktion auf Sicherheitsvorfälle ermöglichen.
- Der Begriff „Deception“ (dt.: Täuschung) bezeichnet kein Einzelprodukt oder -tool. Vielmehr beschreibt er einen konsequenten strategischen Ansatz zur proaktiven Bedrohungsabwehr mit entsprechenden Schulungen und Prozessen, die risikobasiert und in Verbindung mit betriebswirtschaftlichen Prioritäten definiert werden müssen.

Jedes SOC der nächsten Generation braucht eine Deception-Plattform — und zwar aus 6 HAUPTGRÜNDEN, die in diesem Whitepaper erläutert werden

1 **Misstrauen als Grundannahme**
Die Zeiten, in denen eine eindeutige Unterscheidung zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerkbereichen möglich war, sind ein für allemal vorbei. Angesichts der massiven Skalierung von Unternehmensnetzwerken und der zunehmenden Raffinesse der Angreifer, deren Fähigkeiten denen eines durchschnittlichen Sicherheitsteams oft weit überlegen sind, setzt sich zunehmend die Grundannahme durch, dass überall potenzielle Bedrohungen bzw. Kompromittierungen zu vermuten sind.

Diese Grundannahme entbindet Sicherheitsbeauftragte von der nahezu unlösbaren Aufgabe, jede einzelne Schwachstelle zu beheben zu versuchen. Stattdessen können sie sich nun darauf konzentrieren, eine Baseline zu ermitteln und das System auf laufende Kompromittierungen zu überwachen. Mithilfe einer guten Baseline und zuverlässiger Telemetriedaten können auch die raffiniertesten Angreifer aufgespürt werden, die sich im Netzwerk eingenistet haben.

In Deception-Technologie ist die Prämisse des Misstrauens von vornherein eingebaut. Decoys werden auf Endgeräten, im Active Directory und im Netzwerk so platziert, dass Bedrohungsakteure im Zuge eines laufenden Angriffs mit ihnen interagieren und dadurch aus der Deckung gelockt werden.

2 **Proaktive Abwehr**
Im Rahmen einer aktiven Abwehrstrategie sorgt Deception-Technologie dafür, dass das Netzwerk zum feindlichen Gebiet wird, in dem Angreifer möglichst keine Chance haben, unerkannt zu bleiben. Dieser dynamische und agile Ansatz bietet wesentliche Vorteile gegenüber statischem Security-Monitoring, indem er Organisationen auch vor neuen Angriffstaktiken schützt und verhindert, dass Angreifer sich monate- oder gar jahrelang im Netzwerk einnisten.

Deception-Technologie basiert jedoch nicht auf statischen Anwendungsfällen. Eine Deception-basierte Abwehrstrategie richtet sich nicht in erster Linie gegen die von den Angreifern eingesetzten Tools, Exploits oder Vernebelungstaktiken, sondern gegen die menschlichen Intentionen hinter dem Angriff. Daher entwickeln sie sich dynamisch mit den Angriffsmethoden weiter und verlieren nicht im Laufe der Zeit ihre Wirksamkeit. Zukunftsfähige SOCs können neuartige Bedrohungen agil und proaktiv bekämpfen, ohne erst abwarten zu müssen, welche Formen sie annehmen. Deception-Tools helfen ebenso beim proaktiven Aufspüren und Enttarnen von Angreifern wie bei der Ermittlung des Ausmaßes laufender Sicherheitsvorfälle.

3 **Geringe Anzahl von False Positives**
Fehlalarme sind ein ständiges Ärgernis bei herkömmlichen SOCs. Das Risiko zu häufiger Alarmmeldungen muss laufend neu bewertet und sorgfältig gegen die Gefahr abgewogen werden, dass ein akuter Vorfall unerkannt bleibt. Je niedriger also die Fehlalarmquote, desto produktiver arbeitet das Sicherheitsteam, das sich nun voll und ganz auf die Bekämpfung echter Bedrohungen konzentrieren kann.

Deception-Technologie zeichnet sich aufgrund ihres Funktionsprinzips durch eine sehr geringe Fehlalarmquote aus. Denn kein User hat einen legitimen Grund, mit Systemen, Anmeldedaten oder Dateien zu interagieren, die als Decoys angelegt wurden. Entsprechend ist jede Interaktion mit einem Decoy verdächtig und macht immer eine Untersuchung oder sogar eine orchestrierte Reaktion erforderlich. Alarmmeldungen werden also nur dann ausgelöst, wenn wirklich dringender Handlungsbedarf besteht.

4 Datenanalyse und Bedrohungsinformationen
Gängige Analyse-Tools funktionieren zumeist nach dem Prinzip, möglichst große Datenmengen zu erfassen und auszuwerten. Um aussagekräftige Erkenntnisse zum Sicherheitsstatus einer IT-Umgebung zu gewinnen, kommt es jedoch eher auf die Qualität als auf die Quantität der Daten an. Deception-Systeme bieten in dieser Hinsicht den großen Vorteil, dass sie per se nur anomalen bzw. schädlichen Traffic registrieren. Die dabei erfassten Daten liefern wertvolle und präzise Informationen zu akuten Bedrohungen.

Anstatt statische Bedrohungsinformationen aus externen Quellen zu verarbeiten (die weder spezifisch noch aktuell sind), können SOCs anhand dieser Daten eigene Bedrohungsinformationen und Kompromittierungsindikatoren erstellen. Diese sind für das Unternehmen relevanter und können künftige Abwehrmaßnahmen effektiver unterstützen.

5 Orchestrierte Reaktionen
Mit orchestrierten Reaktionsmechanismen können Bedrohungen behoben werden, bevor sie die Produktivität oder Betriebsabläufe beeinträchtigen. Dazu müssen jedoch Auslöser definiert werden, die so zuverlässig sind, dass keine Validierung durch einen Sicherheitsexperten erforderlich ist. Andernfalls besteht das Risiko, dass es durch Fehlalarme zu unnötigen Betriebsunterbrechungen kommt.

Aufgrund der geringen Anzahl von False Positives sowie der im Funktionsumfang inbegriffenen Orchestrierungs- und Integrationsoptionen unterstützen Deception-Plattformen eine kontinuierliche Reaktionsstrategie zur Erkennung kompromittierter IT-Ressourcen und User innerhalb des Netzwerks. Bedrohungen werden automatisch und ohne menschliches Eingreifen untersucht und isoliert bzw. behoben.

6 Insider-Bedrohungen
Sicherheitsteams sind in erster Linie auf die Bekämpfung externer Angreifer fokussiert — die Gefahr, die von Insidern mit legitimem Zugriff auf vertrauliche Daten und IT-Ressourcen ausgeht, wird dabei häufig unterschätzt. Diese Bedrohungsakteure sind mit den vorhandenen Sicherheitsmechanismen bestens vertraut und können ihre schädlichen Aktivitäten als harmlose Vorgänge tarnen.

Deception-Tools schlagen Alarm, wenn Insider gezielt Informationen über stark exponierte Fach- oder Führungskräfte abrufen, außerhalb ihres eigentlichen Aufgabenbereichs auf Systeme zugreifen oder unbefugt Daten kopieren und öffnen. Da Deception-Technologien für normale User nicht sichtbar sind und nur ein kleiner Kreis vertrauenswürdiger Mitarbeiter über die Platzierung von Decoys informiert wird, stehen die Chancen gut, dass die betreffenden Personen ahnungslos in die gestellten Fallen tappen. Auch Fälle von Gelegenheitsbetrug oder unangebrachter Neugier der Mitarbeiter werden dadurch aufgedeckt bzw. verhindert.

Kompromittierte User erkennen

Schutz vor lateraler Ausbreitung

Proaktive Abwehr von Ransomware

Deception-Technologie ist eine unverzichtbare Komponente zukunftsfähiger SOCs. Sicherheitsbeauftragten stehen damit radikal neuartige Möglichkeiten bereit, den Spieß umzudrehen und Angreifer mit einer proaktiven Abwehrstrategie in die Defensive zu drängen.

Zscaler Deception wird weltweit von Organisationen mit hochgradig ausgereiften Sicherheitskonzepten zur Optimierung und Ergänzung herkömmlicher Funktionen Bedrohungserkennung und -bekämpfung eingesetzt. Neu eingerichtete Sicherheitsteams, die unsere Deception-Technologie als effektive Einstiegslösung zur Abwehr gezielter Bedrohungen einsetzen, profitieren ebenfalls von ihren Vorteilen in Bezug auf Zuverlässigkeit, Produktivität und Automatisierungsgrad.

zscaler™ | Experience your world, secured.™

Über Zscaler
Zscaler (NASDAQ: ZS) beschleunigt die digitale Transformation, damit Kunden agiler, effizienter, stabiler und sicherer arbeiten können. Zscaler Zero Trust Exchange schützt Tausende Kunden mittels sicherer Verbindungen zwischen Usern, Geräten und Anwendungen an jedem beliebigen Standort vor Cyberangriffen und Datenverlust. Die SSE-basierte Zero Trust Exchange ist auf über 150 Rechenzentren der ganzen Welt verteilt und die weltweit größte Inline-Cloud-Sicherheitsplattform. Informieren Sie sich auf **zscaler.de** oder folgen Sie uns auf Twitter unter **@zscaler**.

+1 408 533 0288 Zscaler, Inc. (Hauptsitz) • 120 Holger Way • San Jose, CA 95134, USA zscaler.de