Automatisierte Sicherheit mit Wazuh und Event-Driven Ansible

In einer Zeit, in der Cyberangriffe immer ausgefeilter und die Anforderungen an die IT-Sicherheit immer komplexer werden, ist eine effiziente und automatisierte Reaktion auf Sicherheitsvorfälle von entscheidender Bedeutung.
Zeitnah auf Herausforderungen zu reagieren, ist eine grundlegende Aufgabe des IT-Betriebs. Dafür stehen heute zahlreiche Monitoring- und Tracing-Lösungen zur Verfügung. Wiederkehrende Aufgaben zu automatisieren, bildet eine weitere Grundlage des Betriebs: Maßnahmen sollten schnell und sicher durchgeführt werden – mit möglichst wenigen Fehlermöglichkeiten. Für diesen Zweck gibt es verschiedene Lösungen auf dem Markt. Doch was wäre der nächste Schritt? Die beiden Aspekte miteinander zu verbinden, um mithilfe vorgefertigter automatisierter Lösungen schnell auf potenzielle Fehler reagieren zu können. Für diesen Ansatz haben wir eine Demonstration vorbereitet.
Unser Vortrag beleuchtet die Integration von Wazuh, einer leistungsstarken Open-Source-Sicherheitsplattform, und Event-Driven Ansible, einem Framework zur automatisierten Ereignisbehandlung.
Wir zeigen, mit welcher Logik bestimmte Anomalien im Betrieb erkannt werden können, wie die Monitoring-Plattform Reaktionen auslöst und wie diese Reaktionen durch mächtige Automatisierungsfunktionen und Zusatzfeatures wiederholt ohne Verzögerung und Mehraufwand umgesetzt werden können. Zudem erläutern wir, warum wir genau diese Lösungen ausgewählt haben und wie sie miteinander verknüpft sind.
Die Teilnehmer*innen erhalten zunächst eine Einführung in die grundlegenden Funktionen von Wazuh, darunter Sicherheitsüberwachung, Schwachstellenscans und Compliance-Berichte. Anschließend werden die hier relevanten Aspekte von Ansible erklärt und das Konzept von Event-Driven Ansible vorgestellt. Daraufhin zeigen wir, wie Event-Driven Ansible genutzt werden kann, um Ereignisse zu erkennen und sofortige, automatisierte Gegenmaßnahmen einzuleiten – von der Isolierung kompromittierter Systeme bis hin zur Schwachstellenbehebung.
Durch praxisnahe Anwendungsfälle und eine Live-Demonstration wird das Potenzial dieser Kombination greifbar gemacht. Mit einigen kleinen, aber typischen und unter Konferenzbedingungen reproduzierbaren Beispielen möchten wir die Möglichkeiten und das Potenzial dieser Ansätze kurz veranschaulichen. Wir demonstrieren beispielsweise, wie ein ungewöhnlicher Login von Wazuh erkannt wird und das betroffene System automatisch durch Ansible isoliert werden kann. Abschließend diskutieren wir, wie diese Tools weiterentwickelt werden können, um zukünftigen Herausforderungen gerecht zu werden.
Der Vortrag richtet sich an DevOps- und Sicherheitsverantwortliche, die ihre Prozesse automatisieren und ihre Reaktionszeiten minimieren möchten. Besondere Vorkenntnisse sind zwar von Vorteil, aber nicht zwingend erforderlich. Ziel ist es, ein Konzept vorzustellen, das noch relativ neu ist und für das es bisher wenig Fachliteratur gibt. Das Thema dürfte alle interessieren, die sich mit Fragen der Sicherheit und Stabilität beschäftigen. Unser Ziel ist es, den Vortrag so zu gestalten, dass er auch ohne besondere Vorkenntnisse und ohne Fachjargon verständlich ist.