Modernisieren Sie Ihr SOC mit einem KI-basierten virtuellen Security-Analysten

Künstliche Intelligenz (KI) kann viel schneller als ein Mensch Muster in riesigen Datenmengen identifizieren, Trends erkennen und Bedrohungen klassifizieren. Mit einem KI-basierten SOC-Analysten (Virtual Security Operations Center), der mit Deep Learning wie tiefen neuronalen Netzen arbeitet, lassen sich wachsende Kompetenzlücken schließen und Sicherheitsvorfälle schneller erkennen und angehen.

74 % der Security-Experten sagen, der Mangel an Cyber-Security-Fachkräften macht sich im Unternehmen bemerkbar.[1]

Ein virtueller SOC-Analyst, der auf einem tiefen neuronalen Netz basiert, kann Kompetenzlücken abmildern, indem er einfachere Aufgaben übernimmt und Analysten bei schwierigeren Fragen unterstützt.

Ein gut funktionierendes KI-System muss bestimmte Eigenschaften haben.

Ein KI-gesteuerter virtueller Security-Analyst muss selbstlernend sein.

Bei häufig verwendeten **Algorithmen für maschinelles Lernen** bringt ein virtueller Security-Analyst, der auf Deep Learning basiert und autonom ohne vorheriges Training eingesetzt werden kann, eine große Entlastung für personell begrenzte SOC-Teams – weil man sich darauf verlassen kann, dass sich die KI an die sich weiterentwickelnde Cyber-Bedrohungslandschaft anpasst.

Maschinelles Lernen		Deep Learning
Überwacht	Trainingsmodell	Selbstständig
Vom Anbieter kontrollierte Domain	KI-Hosting	Überall, einschließlich On-Premises beim Kunden
Erfordert cloudbasierte Updates	KI-Reife (laufendes Training)	Selbstlernend, optionale Ergänzung durch Global Learning
Wochen	On-Prem-Training	Vortrainiert: ab dem 1. Tag einsetzbar

Die KI sollte umfassend mit den Mitarbeitern, Prozessen und Technologien eines Unternehmens zusammenarbeiten.

Eine solche Zusammenarbeit verbessert die Skalierbarkeit von Teams, automatisiert grundlegende Aufgaben und schafft eine Security, die mit komplexen Bedrohungen Schritt halten kann.

Die Maschinengeschwindigkeit der KI sollte das Erkennen, Untersuchen und Abwehren von Bedrohungen verkürzen.

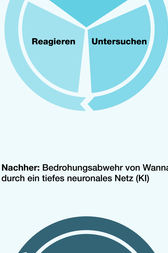
Ein SOC erhält durchschnittlich **10 000 Warnungen pro Tag**, verfügt aber nur über die Mitarbeiter und Ressourcen, um einem Bruchteil davon nachzugehen.[2] Zwei Drittel der Security-Analysten untersuchen weniger als 30 Warnungen pro Tag[3] – die Hälfte davon sind wahrscheinlich Fehlalarme.[4]

Ein KI-basierter virtueller Security-Analyst kann den Prozess der Erkennung und korrekten Klassifizierung potenzieller Angriffe deutlich verkürzen. Er kann auch die nötigen Untersuchungsschritte ausführen, um die Quelle der Bedrohung und die betroffenen Rechner zu identifizieren, sowie geeignete Abhilfemaßnahmen ergreifen.

Das bedeutet eine erhebliche Entlastung des Security-Teams und senkt die Kosten, die durch Sicherheitsvorfälle verursacht werden.

Beispiel-Ablauf bei der Bedrohungsabwehr

Vorher: Herkömmliche Bedrohungsabwehr von WannaCry nur mit SecOps-Analysten

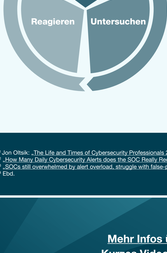


Identifizieren (mind. 1 Std.)
- Angenommen, dass es sich bei 100–1000 im SOC-Dashboard ausgewählten Alerts um Ransomware handelt oder um direkte Meldungen von betroffenen Benutzern

Untersuchen (mind. 4 Std.)
- Bei Security-Produkten anmelden
- Logs/Alarme prüfen
- Ransomware mithilfe integrierter und externer Tools bestätigen
- Extern recherchieren
- Bei Security-Produkten anmelden, um nach seitlicher Bewegung von WannaCry zu suchen
- Abwehrplan erstellen

Reagieren (mind. 2 Std.)
- Gerät(e) und Netzwerk-Segment in Quarantäne setzen
- Gerät(e) bereinigen/Backup wiederherstellen
- Patches anwenden
- Ticket schließen

Nachher: Bedrohungsabwehr von WannaCry mit SecOps-Analysten, gestützt durch ein tiefes neuronales Netz (KI)



Identifizieren (< 1 Sek.)
- KI: Ransomware in weniger als einer Sekunde bestätigt
- KI: lernt neue Ransomware-Merkmale selbstständig

Untersuchen (< 5 Min.)
- KI: liefert WannaCry-Kill-Chain mit kontextbezogener Bedrohungsforschung
- KI: identifiziert Ursprung der WannaCry-Infektion („Patient Null") und seitliche Bewegung
- SecOps: Abwehrplan erstellen

Reagieren (< 30 Min.)
- Security-Kontrollen mit integrierter KI:
  – Gerät(e) und Netzwerk-Segment in Quarantäne setzen
- SecOps-Nachbereitung:
  – Gerät(e) bereinigen/Backup wiederherstellen
  – Patches anwenden
- Ticket schließen

[1] Jon Oltsik, „The Life and Times of Cybersecurity Professionals 2018", ESG & ISSA, April 2019.
[2] „How Many Daily Cybersecurity Alerts does the SOC Really Receive?", Bricata, 2. Oktober 2019.
[3] „SOCs still overwhelmed by alert overload, struggle with false-positives", Help Net Security, 29. August 2019.
[4] Ebd.

Mehr Infos über FortiAI
Kurzes Video über FortiAI