Effektiver Einsatz von KI-Methoden in der Abwehr von Cyber-Angriffen durch UEBA und Automatisierung

Erläuterung der Problemstellung, die mit der Idee gelöst werden soll:

vernetzte informationstechnische Infrastruktur. Ohne diese Infrastruktur ist die Kommunikation einzelner Teilprozesse untereinander massgeblich gestört, was zur Beeinträchtigung oder zum Ausfall einzelner Teilprozesse, zu kritischen Verzögerungen oder zum kompletten Systemversagen führen kann. Die Störung dieser IT-Infrastruktur ist daher, aller Voraussicht nach, das primäre Ziel eines Angreifers im Vorfeld einer zukünftigen Konfrontation auf nationaler Ebene und der Schutz dieser kritischen IT-Infrastruktur wird zur zentralen Aufgabe, die es zu lösen gilt:

- Bei genauerer Betrachtung erstreckt sich diese Aufgabe über viele getrennte Segmente, die historisch nur wenig miteinander zu tun hatten. Das bekannteste Beispiel ist die klassische Trennung zwischen "Server" und "Netzwerk". Eine Lösung für das Gesamtproblem muss also diese historischen Silos überspannen, um wirksam zu sein.
- Angriffe auf hohem Niveau nutzen immer gezielt Schwächen der Infrastruktur aus und basieren immer auf "unbekannten" Schadcode. Das bedeutet, dass die Angriffe nicht anhand statischer "Fingerabdrücke" oder Muster erkannt werden können.
- Es ist davon auszugehen, dass fortgeschrittene Angreifer KI-Methoden verwenden, um Schwachstellen in der Infrastruktur des Opfers aufzudecken. Die Nutzung von KI in der Aufklärungsphase wird passiv wie auch aktiv eingesetzt werden.
- Ein Angreifer wird alles versuchen, möglichst lange unentdeckt zu bleiben.
- Die Angriffe werden mit der Identität eines bekannten und autorisierten Benutzer verübt werden
- Angriffe werden versuchen, sich im "Rauschen" der Kommunikation zu verstecken, um damit statische Schwellwerte zu umgehen und die Erkennung durch "false positives" zu erschweren

Erschwerend kommt hinzu: All diese Faktoren wirken in einem hochdynamischen Umfeld, in dem jeder Teilbereich unabhängig von den jeweils anderen agiert.

All dies führt dazu, dass die durchschnittliche Zeit, in der Schadcode in einem Netzwerk aktiv ist, bevor er enttarnt wird, derzeit bei 146 Tagen liegt. In dieser Zeit hat ein Angreifer die Möglichkeit, Prozesse zu stören, Information zu sammeln und seinen Zugriff weiter auszubauen. Nach dieser Zeit ist die Gefahr erkannt, allerdings gibt es in der klassischen IT keine Umsetzung einer OODA-Schleife. Nach der Erkennung startet eine weitere, oft chaotische Phase, in der mit oft ungeeigneten Mitteln und ohne einheitliche Prozesse versucht wird, die Risiken einzuschätzen und den Schaden zu begrenzen.

Die Umsetzung und Beschleunigung einer geschlossenen OODA-Loop im Bereich IT Sicherheit ist der Kern des gelösten Problems.

Beschreibung der Idee und wie sie das Problem lösen soll:

Im Folgenden verwenden wir folgende Begriffe:

KI-Methoden: Verschiedene statistische und andere mathematische Modelle, Algorithmen und Methoden die zur Analyse und Klassifizierung von Daten genutzt werden. Wichtig im Kontext dieser Betrachtung ist, dass die verwendeten KI-Methoden dynamisch im Kontext der jeweiligen Fragestellung helfen, Ereignisse ganzheitlich zu bewerten. Welche konkrete Methode gewählt wird, hängt von der jeweiligen Fragestellung ab. Identität: Ein "Benutzer" oder "Gerät", das im Netzwerk und/ oder Anwendungskontext autorisiert und bekannt ist. Benutzer: Ein Mensch, der mit verschiedenen Geräten und Anwendungen Teil von einem oder mehreren Geschäftsprozessen ist. Ein Benutzer (Mensch) hat in der Regel eine oder mehrere "Identitäten", unter denen er Zugang z.B. zu Räumen, Anwendungen und/oder Geräten hat.

Grundidee:

Unabhängig von der Art und Weise der Ausführung hat ein Angriff auf eine IT-Infrastruktur immer ein festes Ziel:

- Gewinnung/ Exfiltration von Information (Aufklärung/ Spionage)
- Störung (Angriff/ Sabotage)

Um eins dieser Ziele zu erreichen, muss ein Angreifer physischen oder virtuellen Zugang zur Infrastruktur erlangen und eine Identität im Kontext der Infrastruktur annehmen. Als diese Identität hat der Angreifer dann den Zugang zu verschiedenen Ressourcen und eine Vertrauensstellung innerhalb der Infrastruktur, die für das eigentliche Ziel genutzt werden kann. Es scheint zwingend logisch, dass eine derart missbrauchte Identität im Rahmen ihrer "Übernahme" durch den Angreifer plötzlich und subtil ihre Absichten und damit auch ihr Verhalten verändert. Im ersten Schritt geht es darum, mit KI-Methoden diese subtilen Veränderungen im Verhalten von Identitäten zu erkennen, das Risiko im IT-Kontext zu bewerten und zeitnah anzuzeigen. Für diese Aufgabe haben sich verschiedene technische Ansätze bewährt, die unter dem Begriff "UEBA" oder "User/ Entity Behaviour Analytics" bekannt sind. Mit diesem Werkzeug wird im Rahmen einer OODA-Betrachtung der Schritt "Observe" und teilweise auch das "Orient" abgedeckt. Teilweise deshalb, weil die bekannten Security-Werkzeuge die Risikobewertung nicht oder nur teilweise im Kontext des Geschäftsprozesses betrachten. Es fehlt also eine übergeordnete Instanz, die die durch UEBA gewonnene Information dynamisch und flexibel mit denen aus anderen Systemen verknüpft und zusammenfasst, um ein ganzheitliches Lagebild und eine Entscheidung (Decide) zu ermöglichen. Hierfür bietet sich eine integrative Platform für die Korrelation beliebiger Maschinendaten an. Ziel dieser Platform ist es, ohne umständliche Implementierung das Wissen und die Information verschiedener, bestehender Systeme aus verschiedenen Silos zusammen auszuwerten. Zum Abschluss der OODA-Schleife fehlt noch eine flexible Komponente, mit der eine getroffene Entscheidung konsequent und (teil-) automatisiert in den verschiedenen beteiligten Systemen ausgeführt wird. Für diese Aufgabe haben sich Workflow-Engines bewährt, allen voran das Werkzeug "Node-Red".

Für die konkrete technische Umsetzung sind die benötigten Komponenten entweder als kommerzielles Produkt oder Open Source Lösung frei am Markt erhältlich. Ein konkreter Vorschlag für die Implementierung ist:

- Aruba IntroSpect als UEBA zur Anomalie-Erkennung von Identitäten

- Splunk als optimales, integratives Frontend/ GUI und zur Korrelation vom Externen Daten/ Geräten/ Lösungen.
- Node Red als Workflow-Engine zur Ausführung/Abarbeitung von Incidents/ Anomalien
- OpenDXL als Kommunikations-Schicht zur losen Kopplung der einzelnen Komponenten und flexiblen Anbindung von bestehenden Systemen

Das Ziel wird durch Lösungs-Know-How und der intelligenten Verknüpfung der einzelnen Komponenten, im Rahmen des Gesamtkontexts, erreicht.

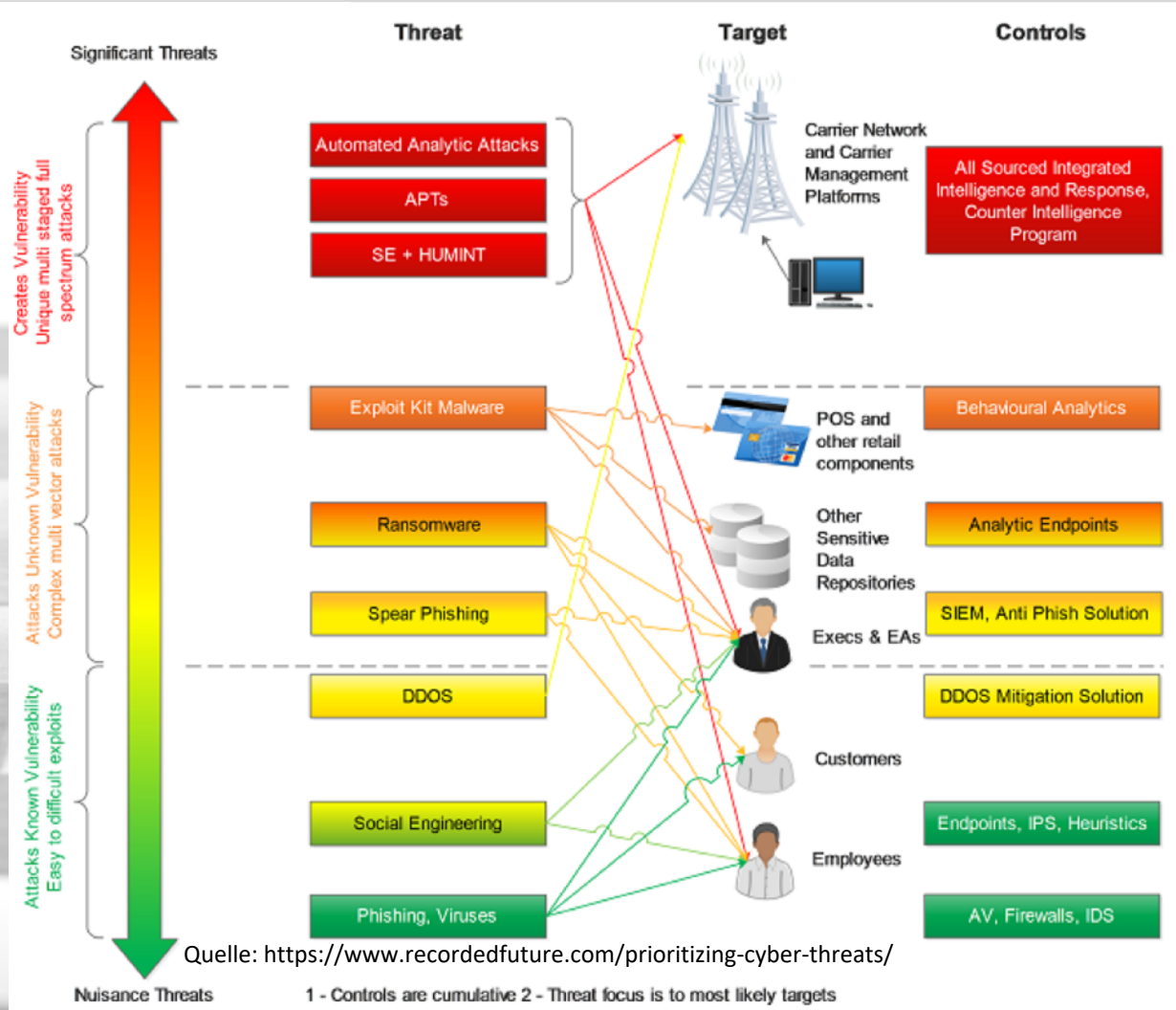
Im Rahmen der Implementierung müssen verschiedene Systeme vornehmlich Log-Daten liefern, die, je nach Informationsgehalt, in IntroSpect und/ oder Splunk gesammelt und/ oder bewertet werden. Dazu kann ein bestehendes Monitoring System eingebunden werden, um die Basisdaten von Geräten zu erfassen. Die Anbindung der Zentralen Stellen zur Benutzerauthentifizierung (z.B. AD) müssen ebenfalls angebunden werden. In kritischen Netzwerksegmenten müssen Sensoren installiert werden, die es ermöglichen, Auffälligkeiten im Netzwerk-Verkehr zu erkennen. Die Log-Information aus geschäftskritischen Anwendungen müssen mit eingebunden werden. Auch hier dient das der Erkennung von Anomalien und der Bewertung von Risiken. Wie eingangs erwähnt wird eine effektive Lösung alle Bereiche der IT Infrastruktur überspannen und demnach alle berühren, die Teile der Prozesse mit Hilfe von IT Infrastruktur abbilden. Zusammenfassend muss jeder, der relevante Maschinendaten erzeugt bereit sein, diese der Lösung zur Verfügung zu stellen. Dazu kann es notwendig sein, Transportagenten auf lokalen Rechnern oder Sensoren in Netzwerksegmenten zu installieren. Das Ziel der Lösung ist es, den Abschnitt "Act" der OODA-Schleife möglichst automatisiert ablaufen zu lassen. Dementsprechend muss jeder, der als Teil einer "Act" Ausführung im Ablauf mit eingebunden ist entweder bereit sein, Schnittstellen zum OpenDXL-Bus zu implementieren und/ oder eine Schnittstelle zu einem lokalen Abwicklungs-System (Melde-/ Ticketsystem) zur Verfügung zu stellen. Im Rahmen der Umsetzung müssen sogenannte "Playbooks" oder Abläufe für die "Act" und "Decide" Phasen erstellt werden. Diese erfordern die fachliche Zusammenarbeit von Security-, System-, Netzwerk- und Anwendungsspezialisten. Im Vorfeld der Umsetzung sind etwaige Vorgaben des Beauftragten für Datenschutz zu beachten, insbesondere hinsichtlich der Anonymisierung, Pseudonymisierung und Aufbewahrung von Daten.

Die Kernsysteme, die für die "OO" Funktion der Lösung benötigt werden sind Splunk, UEBA, AD, Netzwerk-Information (Traffic, DHCP, DNS) sowie alle Log-Daten, die an Perimeter-Grenzen erzeugt werden (Firewall, IDS/IPS, VPN). Besteht ein SIEM System wie z.B. ArcSight oder QRadar, dann kann auch dieses als hochwertiger Sensor mit eingebunden werden. OpenDXL ist an dieser Stelle optional, kann allerdings helfen externe Systeme anzubinden. Die Lösung kann ausgehend von der Anomalie-Erkennung/UEBA stufenweise erweitert werden und bestehende Systeme können durch das flexible Bus-System OpenDXL und die verwendeten offenen Standards in der Regel sehr einfach in die Lösungsmatrix eingearbeitet werden. Für die Umsetzung des "DA" ist die Implementierung des Node Red, OpenDXL und die Definition der Playbooks die Voraussetzung. Eine Automatisierung der Prozesse in der "Act"-Phase ist angeraten, um die operative Last von den Security Analysten im Betrieb zu senken.

Effektiver Einsatz von KI-Methoden in der Abwehr von Cyber-Angriffen durch **UEBA** und **Automatisierung**

SECADM
SECURE FOR SURE

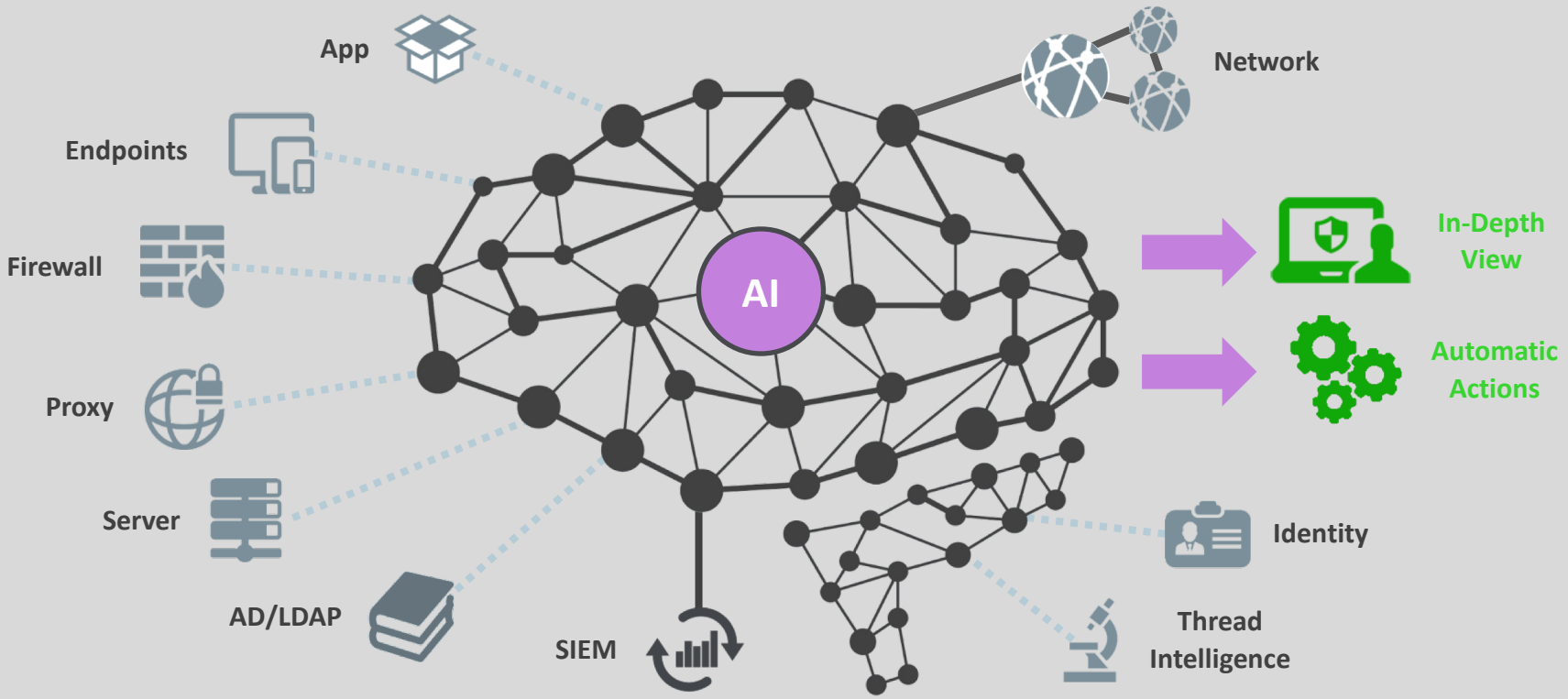
Strategie bei Bedrohungen HEUTE



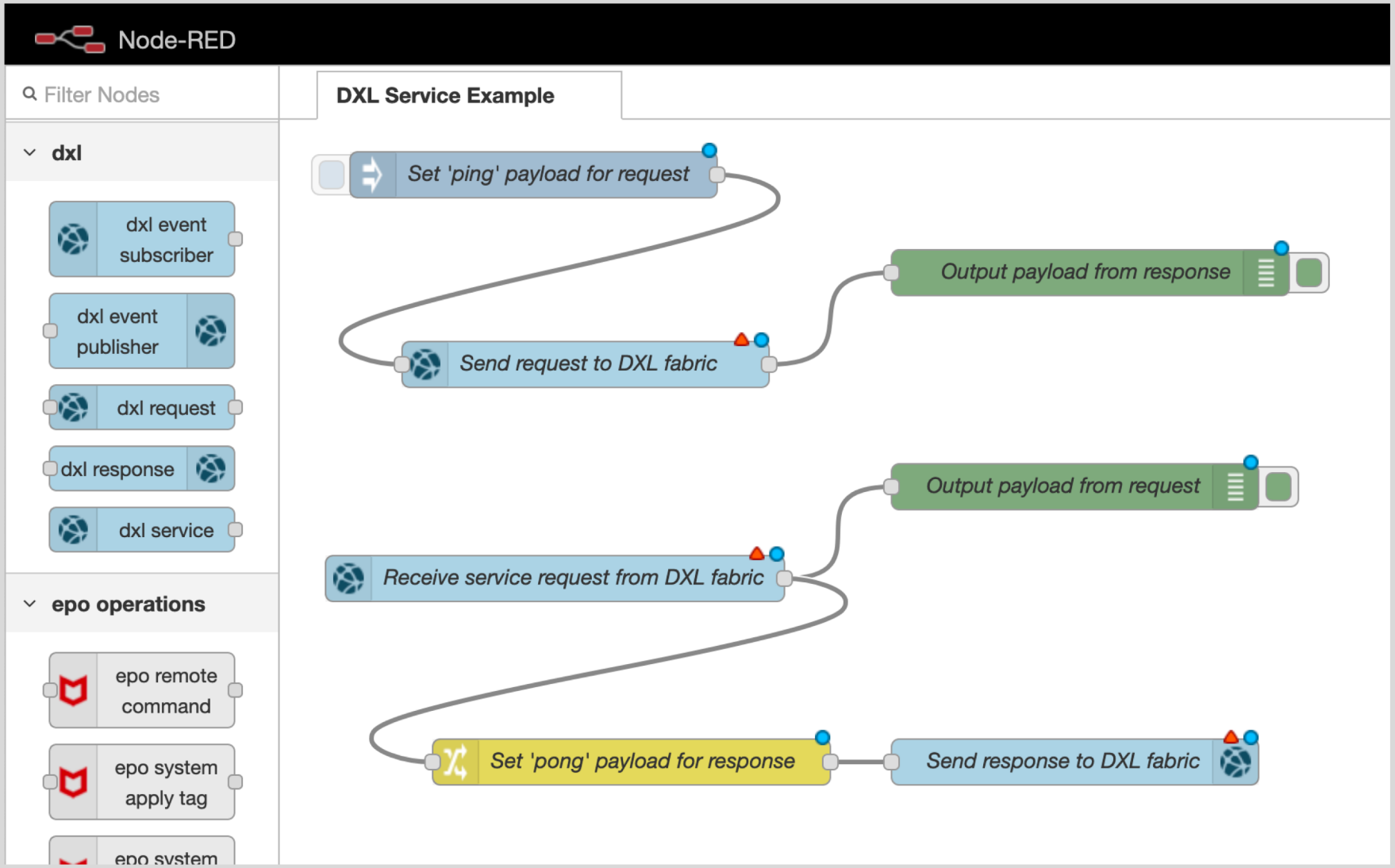
Quelle: https://www.recordedfuture.com/prioritizing-cyber-threats/

Strategie der ZUKUNFT ?

User and Entity Behavior Analytics



Workflow Automatisierung



Strategiewechsel

GO!

SECADM
SECURE FOR SURE

Vielen Dank!

Hptm d.R.

Jan.Heinbuecher@secadm.de

Cyber-
Reservisten Arbeitsgemeinschaft München