

## Drax



### Überblick

#### Industrie

- Energie und Versorgung

#### Herausforderung

- Komplexe Bedrohungslandschaft
- Gezielte Cyber-Attacken bedrohen den Energiesektor
- Große Mengen an Datenvolumen mit unzureichender Transparenz
- Zu viele „False Positives“ in bestehenden Sicherheitssystemen
- Insider-Bedrohungen
- Hauptsächlich reaktive, und nicht genügend proaktive Ansätze

#### Ergebnisse

- Selbstlernendes Konzept und probabilistische Beurteilung des Risiko-Verständnisses vom Nutzer-Verhalten
- Anomalie-Erkennung
- Komplette Netzwerksichtbarkeit und ein verbessertes Verständnis der Aktivitäten
- Analysiert externe und interne Bedrohungen

### Hintergrund

Drax ist ein führendes Energieinfrastrukturunternehmen und ist für rund 7% der britischen Stromerzeugung verantwortlich. Seit der Umstellung auf Biomassegeneratoren gilt Drax als eine der zukunftsorientiertesten Organisationen in der Energie- und Versorgungsbranche.



Die Künstliche Intelligenz (KI)-Technologie von Darktrace hat sich als instrumental für die Sichtbarkeit von Geräten erwiesen, von denen wir noch nicht einmal wussten, dass sie in unserem Netzwerk sind.

**Martin Sloan, Gruppenleiter Sicherheit, Drax**



### Problemstellung

Der Energiesektor ist mit einer sich rapide entwickelnden Bedrohungslandschaft konfrontiert, in welcher immer ausgeklügeltere Angreifer erfolgreich Netzwerke infiltrieren. Bei Cyber-Bedrohungen in diesem Bereich steht viel auf dem Spiel und erfolgreiche Attacken haben erhebliche Auswirkungen auf die Sicherheit und Integrität nationaler kritischer Infrastrukturen.

Angesichts der vielfältigen Motivationen der Angreifer und des sich abzeichnenden Risikos einer internen Bedrohung wurde es für Drax immer schwieriger, neuen Angreifern zuvorzukommen und ihre Methoden vorherzusehen. Drax musste in der Lage sein, bei Bedrohungen frühzeitig einzugreifen, um ihre kritischen Daten und Systeme besser schützen zu können.

Angriffe im Energiesektor sind aufgrund der zunehmenden Integration von IT mit operativen Technologien (OT) sowohl gravierender als auch schwieriger abzuwehren. Die Integration der beiden Netzwerksystemen (IT & OT) schafft neue Angriffsvektoren, da das jeweils eine auch als Eintrittspunkt in das andere fungieren kann.

## Lösungsansatz

Drax entschied sich für einen Immune System Ansatz, um auch auf Bedrohungen zu reagieren, die nie zuvor von anderen Sicherheitslösungen identifiziert wurden. Darktraces Enterprise Immune System erlaubte es dem Unternehmen von einem selbstlernenden System zu profitieren, das keine A-priori-Kenntnisse benötigt um Angriffe zu erkennen, sondern ein anpassungsfähiges Verständnis von Normalität und Abnormalität im Netzwerk bildet.

Die Fähigkeit des Systems, sich kontinuierlich und in Echtzeit an schnell entwickelnde Informationsumgebung anzupassen war für Drax von entscheidender Bedeutung, da die Firma in der Lage sein musste in potenziell gefährlichen Situationen frühzeitig zu handeln.

Nach der erfolgreichen Implementierung des Enterprise Immune Systems im Unternehmensnetzwerk erweiterte Drax dieses, um auch das industrielle Kontrollsystem vor Angriffen zu schützen. Durch die umfassende Transparenz von IT- und OT-Umgebungen bietet Darktrace Drax die einzigartige Möglichkeit, alle Bereiche des Unternehmens- und Produktionsnetzwerkes zu analysieren und bisher unbekannte Bedrohungen zu erkennen.

“

Es hilft uns, den aufkommenden Angriffen immer einen Schritt voraus zu sein und unsere kritischen Systeme besser zu verteidigen. Wir freuen uns daher, mit der führenden, selbstlernenden Plattform von Darktrace an Cyber-Innovationen arbeiten zu können.

”

**Martin Sloan, Gruppenleiter Sicherheit, Drax**

## Vorteile

Darktrace wurde, aufgrund ihres einzigartigen probabilistischen Ansatzes und der Fähigkeit aufkommende Bedrohungen zu erkennen bevor diese erheblichen Schaden verursachen können, schnell zu einem wesentlichen Bestandteil der Cyber-Sicherheitsstrategie von Drax.

Seit dem Einsatz vom Enterprise Immune System wird das Unternehmen schnell auf potenzielle Eindringungsversuche, die andere Sicherheitskontrollen umgangen hätten, aufmerksam gemacht. Drax kann die Gesundheit ihres Unternehmensnetzwerkes daher kontinuierlich analysieren und Anomalien erkennen, die mit hoher Wahrscheinlichkeit bösartig, gefährlich oder nicht konform mit Sicherheitsrichtlinien sind.

Somit profitiert Drax von der fortschrittlichsten Cyber-Verteidigungstechnologie, um ihre kritische Infrastruktur zu beschützen. Das Enterprise Immune System schützt dazu unabhängig davon, ob Bedrohungen von innerhalb oder außerhalb der Organisation kommen.

## Kontakt

Nordamerika: +1 415 229 9100

Europa: +44 1223 394 100

Asien-Pazifik: +65 6804 5010

[info@darktrace.com](mailto:info@darktrace.com)

[darktrace.com](https://darktrace.com)