

## City of Las Vegas



### Überblick

#### Industrie

- Regierung

#### Problemstellung

- Knappes Sicherheitspersonal
- Keine Einsicht in den internen Netzwerkverkehr
- Unfähigkeit existierender Sicherheits-Tools, Bedrohungen in Echtzeit zu erkennen
- Bedürfnis nach einem proaktiven Ansatz zur Abwehr von Cyberbedrohungen

#### Ergebnisse

- Komplette Überholung der Sicherheitsplattform durch Umstellung auf das Enterprise Immune System
- Darktrace hilft, das knappe Sicherheitsteam zu entlasten
- Verleiht 100% Echtzeitvisualisierung in IT- und OT-Netzwerken
- Enterprise Immune System erhöht das Vertrauen in andere Sicherheitsmaßnahmen
- Reagiert autonom auf neu auftretende Bedrohungen und ergreift angemessene Abwehrmaßnahmen

### Hintergrund

City of Las Vegas dient als gesetzgebende Körperschaft, die Las Vegas, Nevada regiert. Während das Netzwerk 3.000 Nutzer umfasst, überwacht City of Las Vegas private und sensible Daten von 600.000 Einwohnern und über 42 Millionen Touristen pro Jahr.

“

Das einzigartige Enterprise Immune System von Darktrace erkennt Zero-Day-Bedrohungen und verdächtige Insider-Verhaltensweisen, ohne die Aktivität im Voraus definieren zu müssen.

Michael Sherwood, CIO der City of Las Vegas

”

### Herausforderung

In der sich rasant ändernden Bedrohungslandschaft von heute ist es wichtiger denn je, dass die Stadtverwaltungen ihre Infrastruktur vor potenziellen Angriffen schützen, insbesondere in einer Touristenregion wie Las Vegas. Angesichts der Tatsache, dass City of Las Vegas jährlich Millionen von Touristen anzieht, war die Stadtverwaltung besonders besorgt über Cyberangriffe, die sensible Informationen gefährden könnten.

Mit einem begrenzten Sicherheitsteam war City of Las Vegas der Ansicht, dass ihr bestehender Sicherheitsstack nicht ausreicht, um sich vor der großen Bandbreite möglicher Cyberangriffe zu schützen. Das Sicherheitsteam verwendete ein SIEM-Tool, das einige Einschränkungen zeigte. Das Tool untersuchte nur Log-Daten und gewährte keinen Einblick in den internen Netzwerkverkehr. Folglich war es nicht in der Lage, nie zuvor gesehene Bedrohungen sowohl in Unternehmens- als auch in SCADA-Umgebungen zu erkennen.

City of Las Vegas benötigte eine neue Lösung, die eine vollständige Transparenz des Netzwerks bietet und das kleine Sicherheitsteam entlastet. Vor allem schnelllebige Angriffe wie Ransomware, die verheerende Auswirkungen auf die Privatsphäre und sensible Daten der Stadtverwaltung haben würden, waren besorgniserregend.

## Lösung

Um die bestehende Sicherheit zu verbessern und sich auf die sich schnell entwickelnde Bedrohungslandschaft vorzubereiten, implementierte City of Las Vegas das Enterprise Immune System von Darktrace im gesamten Unternehmen und das Industrial Immune System von Darktrace in den Wasserrückgewinnungsanlagen. Basierend auf unbeaufsichtigtem maschinellem Lernen und KI-Algorithmen ist Darktrace eine selbstlernende Cyberverteidigungstechnologie, die beginnt, ein „Lebensmuster“ für ein Netzwerk zu erstellen, sobald es installiert ist. Mit dem probabilistischen Verständnis von Abnormalität werden potenzielle Cyber-Angriffe erkannt, während sie stattfinden und bevor sie Schaden anrichten.

Bereits am ersten Tag des Proof of Value-Einsatzes erkannte City of Las Vegas sofort den Wert des Enterprise Immune Systems als Teil ihrer gesamten Cybersicherheitstechnologie. Der Threat Visualizer vermittelte dem Unternehmen ein umfassendes Verständnis des internen Netzwerkverkehrs, einschließlich der kleinsten Abweichungen vom normalen Betrieb im Netzwerk. Darüber hinaus konnten diese in Echtzeit auf der 3D-Grafikoberfläche verfolgt werden.

Einige Wochen später wurde diese Selbstlern- und Erkennungstechnik auf die Probe gestellt, als ein Einbruch im Netzwerk entdeckt wurde. Innerhalb von Minuten informierte Darktrace das Sicherheitsteam City of Las Vegas und die Bedrohung wurde sofort untersucht. Die Fähigkeit des Enterprise Immune Systems, abnormales Verhalten direkt zu erkennen und auf ernsthafte Bedrohungen autonom zu reagieren, ermöglicht es City of Las Vegas, ihre Abwehr von Bedrohungen zu optimieren.

Das Verständnis von Normalität für jeden einzelnen Benutzer, jedes einzelne Gerät sowie jedes Netzwerk ermöglicht es dem Enterprise Immune System, mit dem Unternehmen zu wachsen, sich an Veränderungen anzupassen und potenzielle Bedrohungen selbst in Zeiten des Umbruchs zu erkennen.

“

Darktrace Antigena ist die einzige automatisierte Cyberverteidigungstechnologie auf dem Markt, die in der Lage ist, die entscheidenden Schlachten für uns zu schlagen.

”

**Michael Sherwood, CIO der City of Las Vegas**

## Vorteile

Dank der Fähigkeit des Enterprise Immune Systems, ein einzigartiges Verständnis von sich selbst innerhalb der Organisation zu erlernen, hat City of Las Vegas ein beispielloses Bewusstsein für das gesamte Netzwerk. Darktrace bestimmt die Bedrohungsstufe jeder Anomalie und filtert Fehlalarme heraus, indem es das Sicherheitsteam über den Threat Visualizer nur über die wichtigsten Bedrohungen informiert. Das bedeutet, dass City of Las Vegas neuen Bedrohungen immer einen Schritt voraus sein und sich auf tatsächliche Angriffe konzentrieren kann.

„Die Realität der Cybersicherheit heute ist, dass Schutzsysteme am Perimeter nicht ausreichen, um sich gegen schnell bewegende Angriffe zu verteidigen“, kommentierte Michael Sherwood, CIO der City of Las Vegas. „Dank des maschinellen Lernens erkennt das einzigartige Enterprise Immune System von Darktrace Zero-Day-Bedrohungen und verdächtige Insider-Verhaltensweisen, ohne die Aktivität im Voraus definieren zu müssen.“

Durch die Nutzung der Immune System -Technologie hat das Sicherheitsteam mehr Zeit, um schwächere Bereiche des Netzwerks stärker in den Fokus zu rücken, die dringlichsten Bedrohungen zu priorisieren und beruhigt zu sein, dass sie mit den besten Werkzeugen ausgestattet sind.

Das Unternehmen fand außerdem heraus, dass es mit dem Threat Visualizer proaktiv Probleme im Netzwerk untersuchen kann, wie langsame Verbindungen oder Netzwerkfehlfunktionen. Nachdem sie das „Lebensmuster“ des Netzwerks verstanden hatte, konnte Darktrace Antigena wie ein digitaler Antikörper agieren und automatisch angemessene Maßnahmen gegen gezielte Cyber-Bedrohungen ergreifen.

City of Las Vegas hat sich in ihrer Branche als führend etabliert, da die Enterprise Immune System-Plattform es ermöglicht, auch bei den fortschrittlichsten Cyber-Bedrohungen proaktiv zu sein. Es lernt und entwickelt sich, ähnlich wie ein Mensch.

## 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)