City of Las Vegas

Overview

Industry

- Government

Challenge

- Lean security staff
- No visibility into insider traffic
- Limitations of existing security tools to detect threats in real time
- Wanted to adopt a proactive approach to cyber defense and threat mitigation

Results

- Complete overhaul of security platform by switching to Enterprise Immune System
- Darktrace helps take the burden off lean security team
- Gives 100% real time threat detection and visualization
- Enterprise Immune system increased confidence in security stack capabilities

Business Background

The City of Las Vegas serves as the legislative body that governs Las Vegas, Nevada. While their network covers 3,000 users, the City of Las Vegas oversees private and sensitive data of both the 600,000 residents and over 42 million tourists per year.

"Darktrace's unique Enterprise Immune System detects zero-day threats and suspicious insider behaviors, without having to define the activity in advance"

Michael Sherwood, CIO of City of Las Vegas

Challenge

In today's quickly-evolving threat landscape, it is more critical than ever for city governments to secure their infrastructure against potential attacks, especially in a busy tourist location like Las Vegas. Increasingly sophisticated attackers may target city government's data and systems, with the potential to seriously damage the city's administration.

With a limited security team, the City of Las Vegas felt that its existing security stack was insufficient to protect against the wide range of potential cyber attacks. The security team was using a SIEM tool but felt it had several limitations. The tool only looked at logs and provided no visibility into the internal traffic. The City of Las Vegas wanted a new solution that would give total visibility into the network, as well as take some of the burden off the lean security team. Given that the City of Las Vegas sees millions of tourists per year, the city government was concerned about cyber attacks that could jeopardize sensitive information. In particular, fast-moving attacks like ransomware and DDos were of concern; attacks which would have devastating impacts on the privacy and sensitive data of the city's administration.

Solution

In an effort to enhance its existing security, to meet long-term security challenges and prepare for the rapidly-evolving threat landscape, the City of Las Vegas team deployed Darktrace's Enterprise Immune System technology, based on unsupervised machine learning and new developments in Bayesian mathematics developed by specialists from the University of Cambridge. Established with the insight of government intelligence officers, Darktrace is a self-learning cyber defense technology that begins to understand a 'pattern of life' for a network as soon as it is installed. With the probabilistic understanding of abnormality, potential cyber attacks are detected as they develop, before they cause damage.

In just the first day of the Proof of Value deployment, the City of Las Vegas immediately discovered the value of the Enterprise Immune System as part of its overall cyber defense platform. The Threat Visualizer gave the company total understanding of insider traffic, including even the smallest deviations from normal operations in its network- and they could be followed in real time on the 3D graphical interface.

A few weeks later, this visualization and detection technique was put to the test when an intrusion was spotted on the network. Within minutes, Darktrace notified the security team at City of Las Vegas and the threat was immediately investigated. The Enterprise Immune System's innovative ability to detect abnormal behavior as soon as it occurs allows the City of Las Vegas to optimize its capacity for threat mitigation.

The understanding of normality for every individual user, device, and network enables the Enterprise Immune System to grow with the company, adapting to changes, and detecting potential threats, even in times of transition.

Benefits

Thanks to the Enterprise Immune System's ability to learn a unique sense of 'self' within the organization, City of Las Vegas has unprecedented awareness of its entire network. Darktrace determines the threat level of each anomaly, and filters out false positives by notifying the security team of only the most important threats via the Threat Visualizer. This means that the City of Las Vegas can stay ahead of new forms of threats and focus on legitimate attacks.

"The reality of cyber security today is that border defenses are not enough to keep fast-moving attacks out" commented Michael Sherwood, CIO of City of Las Vegas. "Using machine learning, Darktrace's unique Enterprise Immune System detects zero-day threats and suspicious insider behaviors, without having to define the activity in advance."

By basing its security on the newest advances in unsupervised machine learning, City of Las Vegas has increased its confidence that sensitive information is protected and secure. The company also found that by using the Threat Visualizer, it can proactively research issues within the network, like slow connections or network misconfigurations. By relying on the 'immune system' technology, the security team has more time to bring weaker areas of the network into sharper focus, spend their time on the most pressing threats, and feel reassured that they are armed with the best tools in case of an attack. City of Las Vegas has established itself as a leader in its industry, as the Enterprise Immune System allows it to remain proactive in the face of even the most advanced forms of cyber-threat.

Contact Us

US: +1 (917) 363 0822
Europe: +44 (0) 1223 350 653

Email: info@darktrace.com

www.darktrace.com