DARKTRACE

INDUSTRY SPOTLIGHT

Cyber Defense for Government & Defense

Few targets are as enticing for coordinated cyber-criminals as governments, and with the safety of millions hanging in the balance, no sector has more to lose from cyber-attacks. State-sponsored threat actors and sophisticated hacktivists are investing enormous resources to bypass the traditional security defenses protecting such governments — defenses which are largely programmed to spot known threats and cannot adapt to novel attacks or subtle insiders.

Innovative ransomware attacks in particular have become an increasingly common problem for cities and counties alike, with the 2018 attack on the City of Atlanta portending even more devastating attacks to come. Many of Atlanta's connected systems took months to recover following the incident, which cost the city in excess of $9.5 million as well as countless hours of lost productivity.

In addition to ransomware attacks, governments are also seriously imperiled by the threat of data theft, since they safeguard the personal information and lucrative intellectual property of their citizens. Beyond the individual consequences of identity or IP theft, governmental data leaks serve to erode confidence in institutions and therefore have lasting effects for society as a whole.

The undermining of public trust in institutions has already served as a powerful motivator for previous attacks like the notorious 2016 Democratic National Committee breach, which precipitated the resignation of the DNC's leadership and impacted that year's presidential election. Ideological and geopolitical disputes are an inescapable reality of modern politics, providing ample incentive for malicious actors to inflict the reputational harm associated with such breaches on their political adversaries.

The imperative of digital security is as urgent as the need for physical security in the Digital Age. And while governments spend billions of dollars on their armed forces, many remain vulnerable to crippling cyber-attacks that threaten to compromise state secrets and disable public services. States simply cannot afford to wait for cyber-criminals to find the vulnerabilities in their static security postures - rather, they must adopt cyber defenses that fight back in real time when those criminals inevitably strike.

> “Artificial intelligence is absolutely critical to our sector's ability to keep up with evolving threats. Human reaction time and learning can't possibly adapt as quickly as the threats are evolving.”
>
> **Daniel Bourdeau, CIO,**
> **City of Westland**

Threats By Numbers

Ransomware attacks increased by **36%** globally in 2017, while more than 100 new malware families were introduced that year.

Governments are uniquely endangered by such ever-evolving ransomware strains, since such attacks can cause city and county infrastructures to come to a screeching halt.

3 in 4 U.S. federal agencies are either "at risk" or "at high risk" from cyber-threats.

Only a quarter of these agencies were found to be able to detect attempts to access large volumes of data on their systems.

DARKTRACE

CASE STUDY

City of Las Vegas

Background

The City of Las Vegas serves as the legislative body that governs Las Vegas, Nevada. While its network covers 3,000 users, the City of Las Vegas oversees the private and sensitive data of its 650,000 residents, as well as over 42 million tourists per year.

Challenge

As one of the most visited tourist destinations in the world, the City of Las Vegas is continually faced with the challenge of securing its critical data, ensuring operational continuity in its industrial facilities, and maintaining its reputation as a trusted leader in 'smart city' innovation. With a lean security team, the City required a tool that could detect in-progress threats in both its enterprise and industrial systems, and respond autonomously to fast-moving threats like ransomware.

> Using machine learning, Darktrace detects zero-day threats and suspicious insider behaviors, without having to define the activity in advance.
>
> **Michael Sherwood, CIO,**
> **City of Las Vegas**

Solution

In an effort to meet the challenges presented by the rapidly-evolving threat landscape, the City of Las Vegas deployed Darktrace's Enterprise Immune System across its enterprise network, and Darktrace's Industrial Immune System in its water reclamation facilities.

Within weeks of the initial deployment, Darktrace was put to the test when an intrusion was spotted on the network. In minutes, Darktrace notified the security team at the City of Las Vegas and the threat was immediately investigated. Darktrace's ability to detect and respond to abnormal behavior as soon as it occurs allows the City of Las Vegas to neutralize threats before they have time to escalate into a crisis.

"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 Enterprise Immune System can detect and respond to zero-day threats, email-borne attack campaigns, and suspicious insider behaviors - without having to define the activity in advance."

Utilizing Darktrace Antigena, the City of Las Vegas is now able to autonomously contain threats at the first sign of compromise across email, cloud, and network traffic. "With Darktrace Antigena, we are deploying the most revolutionary technology I have seen in a long time," commented Sherwood. "Antigena is the only automated cyber defense technology on the market that is capable of fighting the most important battles for us."