SIM2K
Adapting Technology to Your Business Needs

CYLANCE™

Cylance® Case Study: Government

INDUSTRY

Government

ENVIRONMENT

Highly secure and advanced, but still vulnerable to attack

CHALLENGES

Reduce the amount of malware introduced to networks from infected endpoints

Prevent the exploitation of assets and protect personal, government and critical classified information

Safeguard computers and improve detection rates without impacting continuity or taking excessive measures to lock down systems

SOLUTIONS

Deploy CylancePROTECT® on all endpoints and remove previously deployed product from all systems as needed to better protect against cyberattacks

Improve the efficacy of DHS EINSTEIN

Retain Cylance® Consulting to handle alerts generated by user actions and identify if agency security was previously breached

Multiple Agencies

Cylance has deep experience working with government agencies to remediate and repair damage following high profile threats, and deploy effective, preventive measures to stop future attacks.

The Situation

Government agencies are the high profile targets that cybercriminals dream of infiltrating. No single entity offers the attacker more praise from the hacker community and more sense of self-pride than successfully breaching a government system or endpoint.

Nation states and organized criminal organizations employ elite hacker teams that can attack an agency around the clock with advanced persistent threats and malware.

Guarding against these attacks can be a costly and resource-intensive endeavor, but the cost of a successful breach can be far worse, effecting critical infrastructue, public trust, and in some cases, even resulting in the loss of human life.

The Process

Cylance deploys and monitors its award-winning product that was built using artifical intelligence and machine learning, CylancePROTECT, on all systems. CylancePROTECT identifies and blocks malware that has gone undetected by traditional antivirus solutions.

CylancePROTECT immediately quarantines malware and potentially unwanted programs already present on agency systems.

CylancePROTECT typically uncovers multiple varients of CryptoLocker and other ransomware as well as advanced threats designed to steal credentials and other personally identifiable information.

SIM2K®
Technology Consultants

6330 E. 75th St., Suite 336
Indianapolis, Indiana 46250

317.251.7920
800.746.4356
www.sim2k.com
sales@sim2k.com

Cylance also can perform a full Compromise Assessment on all servers, desktops and laptops across all global hosts. Combining both its artificial intelligence technology and compact process, Cylance is able to extract insightful data from all hosts in just a matter of days using a lightweight endpoint agent that reports meta data back to Cylance. With the data outside the agency's environment, Cylance incident analysts aggregate and analyze it for idiosyncrasies and abnormalities.

At this point, Cylance can quickly identify the initial source of a targeted breach and immediately take the steps necessary to ensure the breach is secured, and does not occur again.

Not only does Cylance replace traditional endpoint antivirus and anti-malware products, it also precludes the need for other detection, forensic recording and host intrusion prevention technologies. It does this while reducing the need for experienced threat response teams to investigate, deconstruct and remediate attacks.

The Results

Using indicators that are gathered during data collection, Cylance's cybersecurity experts are able to dig into specific systems looking for precisely the threats that have not been found by the company's existing antivirus solutions.

Our solutions are based on a sophisticated approach to detecting and stopping previously "unknowable" malware, like those used in advanced persistent threat campaigns. The Cylance solution not only blocks zero-day malware in near real time, but also provides additional context around threats as demanded by top government agency Incident Response teams. When an agency's security posture can effectively shift to PREVENTION instead of RESPONSE, the benefits are clear.

CylancePROTECT can be easily deployed using the most common software deployment solutions. A user-friendly web management console takes the pain out of managing large deployments and is accessible from anywhere with an Internet connection. CylancePROTECT can easily integrate into SIEM consoles for reporting.

Agencies get a product that prevents existing and future threats from ever executing and a support team consisting of the most experienced experts in the cybersecurity industry.

Free Consultation

Want to see how CylancePROTECT and Cylance Consulting will empower your organization in the fight against cyberattacks? Contact us today for a free consultation!

Cylance Privacy Commitment
Cylance is committed to protecting your organization against advanced threats, which includes privacy disclosure. We do not publish the names of our case study partners for this reason.

SIM2K®
Technology Consultants

6330 E. 75th St., Suite 336
Indianapolis, Indiana 46250

317.251.7920
800.746.4356
www.sim2k.com
sales@sim2k.com