INTEL471

Trellix Case Study

TRELLIX

Industry: Technology
Sub-Industry: Cybersecurity
Location: United States

THEIR CHALLENGE

The security engineering team at Trellix have historically needed to manually cross-reference the credentials pulled from the TITAN Platform against their own active directory (AD).

The purpose of this is to verify if any valid credentials have been compromised and to mitigate any risk through early detection. The time and resources required for this process could be better utilised elsewhere if a solution could be found. Trellix faced the challenge of trying to automate this process and improve efficiency within the team.

THE SOLUTION

The Intel 471's engineering team was able to produce a unique script that the Trellix team could implement with minimal effort. This script was designed to automate this cross-referencing process between the data pulled from TITAN and the AD.

The Trellix team is now able to automate this task for immediate remediation
As a result, Trellix is alerted when new relevant credentials are available in the underground, they can automatically asses their validity and if necessary, take immediate action to reduce exposure time.

OUTCOMES

- Automated alerts of new stolen credentials in the market
- Instant validation of new data against the company active directory
- Rapid alerts in conjunction with a actionable response minimise time of exposure
- Effective threat mitigation will ultimately deter future attacks from threat actors

WHY INTEL 471?

Our experts operate across the globe, closely tracking sophisticated threat actors in the places they operate, speak their languages, and understand cultural references that expose and illuminate their underground activities. As a result, we can provide the most relevant and timely intelligence to our customers. Relevant intel refers to specific threats to your business or industry, and when CTI teams are often stretched to capacity, having the guidance on where to focus your team's finite resources is essential. The additional ability for organizations to understand and then implement necessary change is where the real value lies. We pride ourselves on helping organizations operationalize their intel so they are better protected against possible threats. As your organization and their CTI requirements grow, so too can our solution. Even for the most mature CTI teams, our intelligence will far exceed their most ambitious requirements.

> "Intel 471 has been a valued partner of the Trellix Threat Intelligence Group for several years. Our mission is to provide our customers with a broad spectrum of cyber threat information and the Intel 471 capability suite provides a unique perspective in key areas of the globe. The Trellix and Intel 471 team follows a disciplined all source approach to give our customers the most accurate risk picture globally."

sales@intel471.com intel471.com