Real-Time Protection by Integrating Website Reputation Scores into SIEM Solutions

Posted on January 11, 2020

Real-time threat detection is tantamount to up-to-date protection, which should be the only kind of cyberdefense. The key to any good defense, however, is to think and act like there is always a threat. This is true in the virtual realm, to some great extent, where we see a hacker attack every 39 seconds.

For this reason, the use of security information and event management (SIEM) solutions is gaining popularity among security operations centers (SOCs). Security teams are gearing up for when and not if they are attacked. And it’s real-time threat detection and protection that is their goal.

Following that train of thought, this post examines how correlating Web traffic logs with **website reputation scores** returned by Domain Reputation API help SIEM solutions detect and protect against threats in real time.

Not All SIEM Solutions Are Created Equal

While many organizations employ SIEM solutions to improve their security posture, around 26.1% of users believe they don’t get the full value from their implementations. More than that, only 31.9% said they got more than an 80% return on their investment.

When it comes to maximizing SIEM solution value, timing is of crucial importance. Early detection allows organizations to mitigate costly damages in terms of both costs and reputation. SIEM solutions that don’t work at the optimum level are often discarded and replaced with better systems.

Any security solution needs to be able to prevent attacks at the earliest possible time, notably through the use of a variety of domain and IP intelligence feeds, or else users may end up like our two featured data breach victims.

Case Studies: How Website Reputation Scores Can Provide Real-Time Protection

Case #1: Marriott International

Marriott International acquired Starwood Hotels and Resorts Worldwide in 2016. In September 2018, they discovered that the personal information of half a billion of its customers had been stolen due to the attackers' presence in Starwood's computer systems since 2014.

Among the information stolen were passport, contact, travel, and credit card details of 100 million customers. The breach cost Marriott hundreds of millions of dollars, prompting it to lower financial projections for 2019. Its reputation also suffered, resulting in its stock price plummeting.

Upon investigation, Marriott found that Starwood's IT systems were infected with a Remote Access Trojan (RAT). A RAT gives hackers complete access to and control over a computer and it can be unknowingly downloaded with a program (e.g., a game, an app, etc.) or as an email attachment.

The particular RAT inside the Starwood network allowed the hackers to drop Mimikatz, a penetration tool that enabled them to gather passwords stored in the affected system's memory. Once done, the network was ripe for picking.

Using Website Reputation Scores to Filter Malicious Domains and Email Addresses

Hackers may have had a harder time breaching Starwood's network if its system used **website reputation scores** to determine which sites are safe to access and which aren't. Domain Reputation API looks at hundreds of parameters and factors before returning a risk score, including the following:

- Mail server configuration
- Mail server reputation (whether or not it is blacklisted)
- Links to .exe files
- Links to .apk files

The tool also performs malware database, mail server real-time black hole, and nameserver configuration checks. Often, it could return high-risk/low scores for email addresses or site URLs that carry a RAT or other malware and prevent the compromise.

Case #2: Equifax

In 2017, Equifax disclosed that the personal information of 147.9 million of its customers was exposed starting in mid-May concerning a breach they discovered on July 29. Hackers were able to get hold of their victims' Social Security numbers, street addresses, dates of birth, and driver's license numbers.

Equifax accrued US $690 million in legal proceedings costs and lost an additional US $1.4 billion for cleanup. Its reputation also suffered.

According to a U.S. General Accounting Office report, when hackers scanned the Web for vulnerable servers, they found Equifax's online customer complaint portal and gained access to documents associated with dispute resolutions. These documents contained personally identifiable information (PII). Once inside the server, the hackers found other login credentials and servers to exploit. In total, the attackers stole data from 51 databases in over 76 days.

Correlating Website Reputation Scores with Traffic Logs

While the vulnerability that hackers found in Equifax’s portal didn’t have an available patch, a SIEM solution that correlates traffic logs with **website reputation scores** could help detect an ongoing attack.

When the Web traffic logs show that domains with high-risk/low scores are accessing a company’s website, that can trigger an alert so the incident will be addressed. The suspicious domain can be blocked automatically by setting rules, and a threat scan on the server can then be performed to see if the system has been infiltrated.

Website reputation scores gleaned from Domain Reputation API helps security teams and SIEM solution developers provide real-time protection for clients, which is vital in a world where numerous attack vectors exist. The cases of Marriott International and Equifax caused considerable damage that we can all learn from. And if there’s one lesson here, it’s real-time threat detection that can save an organization millions of dollars while protecting its reputation.