# Addressing Threat Correlation Challenges with Website Contacts API and Other Domain Research Tools

Posted on December 9, 2019

A threat defense system that runs separately from operation systems and applications is comparable to a bank with security guards who do not possess any firearms, metal detectors, or radio equipment. Anyone can get assess in that this establishment's security is fragile, and there's a good chance that robbers can get whatever they want. Sure, the guards can try to protect the bank with hand-to-hand combat, but that's no match for the robbers' guns.

Ridiculous as it may sound, most organizations' cybersecurity infrastructure works in the same way — with blind spots between their threat intelligence gathering and response tools. As a result, cybercriminals can quickly launch attacks on digital infrastructure. No matter how well an organization designs its threat defense, if there is no efficient correlation, it won't be as effective.

In this post, we examined some of the most common threat correlation challenges and how Domain Research Monitoring tools, such as a Website Contacts API and Domain Reputation API, can help organizations face them.

## Challenges in Threat Correlation

We can't blame the lack of threat defense correlation entirely on the security operations team or a company's managed/endpoint detection and response (MDR/EDR) service provider. The current state of technology development has been creating more cybersecurity gaps.

In particular, recent research findings identified these challenges that amplify the absence of threat correlation in security infrastructure:

### Increasing Number of Attack Vectors

Around 30% of organizations now use new cloud-based hosts and applications as well as employing consultants that provide attackers with more avenues to penetrate their networks. Other

research supports this, as it found that almost a third of organizations consider moving to the cloud a high investment priority. They also hope to use more cloud-based systems and applications and engage in business process outsourcing (BPO) by 2022.

The adoption of software-as-a-service (SaaS) applications is also bound to take up a significant chunk of planned organizational investments. In fact, the SaaS market is projected to reach a revenue of US $623 billion by 2023. This rising market poses yet another threat to the overall cybersecurity posture of organizations. How can they verify the authenticity and reputability of a SaaS provider?

A website contacts API can help address this challenge. By automating website classification and verification, security teams can focus on defending potential attack vectors. With more than 283 million well-parsed contact details obtained from over 152 million domain records, Website Contacts API can help security teams perform background checks on SaaS platform providers and other partners and suppliers faster.

Users can check the contact information provided by their partners and suppliers with data returned by Website Contacts API to find out if they are who they say they are. In addition, the API returns the website owner's social network profiles and email address, making background checks a lot easier to perform.

## More Time Spent on Cure Rather Than on Prevention

Also, according to the previously cited ESG research, 36% of cybersecurity teams spend the majority of their time fixing emergency issues and less time improving their security processes. As a result, organizations' cybersecurity remains stuck even as their infrastructure progresses.

One way to get out of the rut is for organizations to conduct background checks on every possible attack vector. If they have a new human resource (HR) cloud software provider, they can check them out first. If they are planning to switch to a different payroll system, they need to make sure the provider has not suffered from security breaches before.

Background checks minimize the risk of getting attacked and help prevent fraud. Website Contacts API and Domain Reputation API are just some of the tools that make this process easier as they help check if a site or domain is associated with suspicious activities. More specifically, domain Reputation API gives out reputation scores that allow users to instantly know if a site is safe to access or not.

Security teams are, therefore, able to detect threats before they can infiltrate systems and their network, effectively avoiding costly damages in the form of brand damage and breach settlement.

## Manual Threat Detection Instead of Automation

The same ESG research also found that 26% of organizations still rely on manual processes when it comes to threat detection and response. This fact is surprising, especially amid the advent of automation, machine learning (ML), and artificial intelligence (AI). These organizations may find it even more difficult, if not impossible, to keep up with their competitors, industry, and cybercriminals.

Security information and event management (SIEM); and security orchestration, automation, and response (SOAR) platforms are just some of the emerging technologies that organizations can explore to get ahead.

These platforms can be fed threat intelligence data feeds that can be used to identify IP addresses, domains, site URLs, and email addresses connected to publicly reported attack indicators of compromise (IoCs). These can then be proactively blocked to improve organizations' security posture.

The development of new technologies and solutions has significantly widened the attack surface. However, this doesn't mean that organizations should shy away from adopting anything new just because they may increase the risks that come with cyber attacks.

Effective correlation using data obtained from their network, cloud-based platforms, IoT devices, and threat intelligence can help in that regard. That way, when a threat is detected in one area, it is immediately communicated to others so they can check for the same threat.

Detecting attacks at the reconnaissance stage is pivotal, and luckily, some tools help organizations do so. Website Contacts API and Domain Reputation API are just some of these tools that can help them nip cyber attacks in the bud.