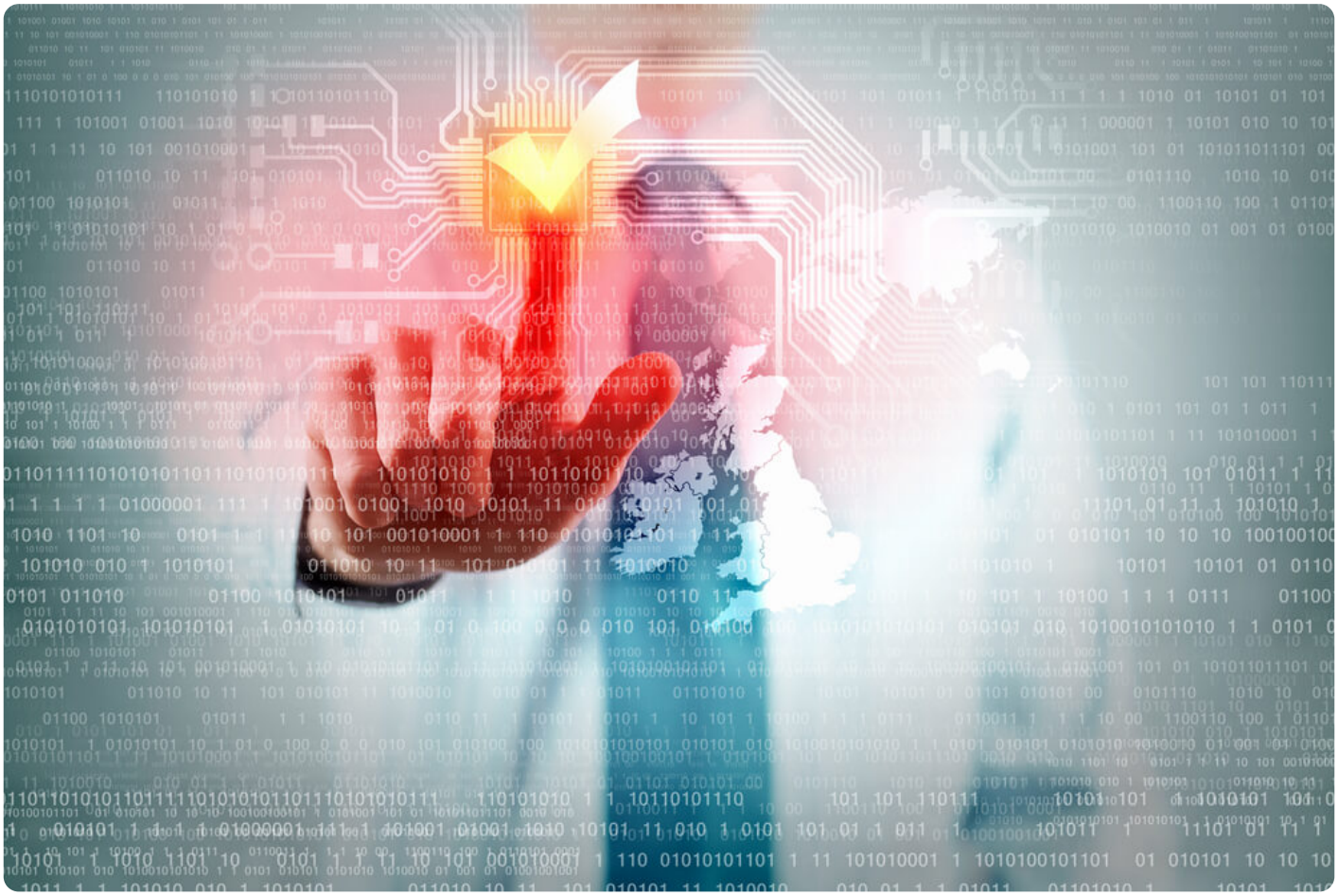
Domain Data: A Common Denominator in Threat Detection Techniques

Posted on November 27, 2019



Today’s cyber warfare is much like an arms race. Cybercriminals continuously improve their strategies trying to keep their schemes uncovered. In parallel, it’s only natural that companies make their security protocols better to respond to or anticipate new and more sophisticated attack patterns.

Doing so, however, is not within the reach of every organization. CISOs who lack the resources to implement initiatives in-house find it more practical and cost-effective to outsource their security requirements.

The concept of outsourcing presents several options as external providers assemble their respective stacks of technological solutions to match various companies’ needs. This post discusses what those options are and how domain data serves as a vital threat intelligence source regardless of the system or provider adopted.

Managed Detection and Response (MDR) Services

MDR services focus on threat detection. As such, providers bring in a team of professional cybersecurity analysts and technological tools and procedures to continuously monitor and provide recommendations to protect their clients’ assets. Their tools are typically positioned at Internet gateways to monitor endpoint activities. Their techniques vary, but they all rely on advanced security analytics fueled by accurate threat intelligence.

As part of this, domain data constitutes a rich source of intelligence to help identify intruders and attack vectors. As such, accessing a variety of domain and IP feeds allow MDR teams to dig deeper and uncover actionable information to detect and prevent threats from becoming full-blown attacks.

Managed Security Services

Managed security service providers (MSSPs), on the other hand, regularly provide companies with essential cybersecurity monitoring and management and regulatory compliance reports, something that MDR teams don't do. Unlike MDR teams, MSSPs are not primarily concerned about threat and intrusion detection. Also, while MDR teams work solely with event logs, MSSPs use different logs and security data.

Domain data can be integrated into an MSSP's solutions and tools to enhance risk assessment, intrusion detection, and vulnerability scanning while continuously performing daily IT security functions.

Security Information and Event Management (SIEM) Software

SIEM solutions provide real-time analysis of security logs and event data and compare them with threat intelligence feeds to detect security-related activities.

Domain data can enrich SIEM analytics by showing inconsistencies in the domain records of entities seeking to interact with the company and their claims. For instance, an MSSP can look at the domain owner's details and compare them with an email sender's claims. Domains flagged for inaccuracies can then be treated as crucial leads to cases that warrant further investigation.

Unified Threat Management (UTM) Appliances

UTM appliances can better protect a network with the integration of multiple security functions and features that include firewalls, anti-malware solutions, and intrusion detection tools. These simplify

security monitoring and management by responding from a single point of defense instead of using different technological tools that serve different functions.

UTM manufacturers can use the information on billions of domains to identify potential phishers, malware authors, cybersquatters, and other threat actors.

Security Operations Centers (SOCs)

A SOC is the center of a company's cybersecurity monitoring, threat detection, and incident response operations. Its scale varies according to how big a company's network is or how much resource is allotted to it. Large enterprises are expected to have a large SOC that performs extensive functions while small and medium-sized businesses (SMBs) may have a basic facility. Regardless of size, however, a SOC depends on real-time sources of data to identify and respond to security incidents and prevent access to potential attack vectors.

A SOC can add domain data to its resources to identify the personalities behind phishing or data breach attempts. Because WHOIS records reveal who owns a domain name, along with his contact information, it is a vital source of threat intelligence that's needed to secure a company's network continuously.

A Common Source of Intelligence for Different Providers

The traditional prevention-only model of securing an organization's IT network has, unfortunately, become inadequate in the face of the growing incidence and virulence of today's cyberattacks.

As such, third-party security providers with varying threat detection, incident response, andsecurity monitoring offerings have surfaced. MDR service providers focus on threat detection,MSSPs concentrate on their clients' day-to-day security needs, and SIEM and UTM vendorsprovide multiple security functions with a single tool.

Regardless of their differences, though, they share a common source of information — domain data. Domain intelligence feeds containing information on billions of domains enrich their threat intelligence thus improving threat monitoring, detection, and mitigation efforts.

The specter of cyber attacks launched against a company remains a constant threat, and businesses can’t afford to lower their guard or risk financial losses or reputational damage. Several attractive options can help — both in-house and outsourced — to bolster an organization's security posture, but their common denominator is data.

In fact, no matter how threats or ways to combat them evolve, domain data will remain a constant ally in pinpointing and neutralizing cyber attacks. Contact us to find out more about our offerings and let us know how we can help.