SOCRadar®

WHITE PAPER

What is attack surface management?
Absolute beginner guide

Attack surface management (ASM) is the process of discovering, listing, classifying, analyzing, prioritizing, and monitoring information that can be collected on the internet to inform your organization about sensitive data by searching external digital assets.

A useful ASM follows your entire digital footprint over the Internet, discovering and collecting the information that relates to your company. But that could be either too much information or not useful information. That's why instead of sharing this information with your company, it gets analyzed and classified first. After this step, the information is prioritized based on its sensitivity. Finally, monitoring is the last step.

In short, attacks surface is everything that attackers can and will discover as they research the threat landscape for vulnerable organizations.

SOCRadar AttackMapper informs the company when a vulnerability is published regarding the assets of company that is visible on the external network and their applications.

SOCRadar provides the following modules as a service;

- Digital footprint discovery
- Domain/IP monitoring
- SSL certificate monitoring
- DNS monitoring
- Vulnerability detection
- Critical port detection
- JavaScript monitoring
- Critical data leak detection

Why is ASM important?

To manage this dynamic attack interface, organizations must ensure that they have the right security controls to reduce the number of vulnerabilities in the attack surface that attackers can exploit. This can be done by using cybersecurity tools to minimize the places where organizations are vulnerable to cyber-attacks. However, it is not impossible to put into perspective the enormous scale of an organization's target area; it simply requires looking at it in a new way. Attack surfaces can be further reduced by proactively mapping the digital footprint, monitoring online channels for attack indicators, quickly defusing identified threats, and protecting customers, employees, and networks. To keep your organization safe, it is important to understand the way your infrastructure is exposed and vulnerable to attacks, and then prioritize activities that help reduce it. Once you understand what a cyber-attack is and what it involves, as well as how extensive your own is, security experts can begin to narrow down the types of attacks your infrastructure is exposed to.

ASM combines advanced Internet data intelligence and analysis to speed up investigations, understand the attack surface, and take action against digital threats. Continuous security monitoring is a level of attack area management concerning trusted digital assets of third parties.

ASM tools provide insight and visibility into these assets to discover and monitor everything related to your organization on the Internet to bring the enormous scale of your attack surface into focus.

This real-time visibility is critical to the risk of violating the attack surface, which is dynamic and highly complex as it is a key component of any organization's security strategy.

For this reason, it is important to monitor the attack surface to detect and manage assets that attackers target across the Internet, mobile, and cloud environments. You can further reduce the attack surface by proactively mapping your digital footprint, monitoring online channels for attack indicators, quickly mitigating identified threats, and protecting your customers, employees, and networks. Intelligent threat interface management can also help transform your IT security team from a crisis manager to a true security analyst whose insights protect your bottom line. By increasing the visibility of digital attack areas and reducing your business exposure, you can find and monitor all assets released by the Internet.

Organizations can proactively intervene in defense by continuously managing and reducing the attack surface to make it harder and harder for attackers to succeed. They can improve their security position by using ASM; reduce risks by improving attack surfaces by using credible and authentic deception in the cloud.

You may already have a perimeter around your network to protect the entire system, but a controlled attack surface helps you avoid some of the most common cybersecurity risks facing organizations today. Segmentation of the network makes sense because segmentation helps reduce the area of attack by increasing the number of barriers that attackers encounter when trying to travel through a network. By defining the scope of the software, you can identify and stop potential problems at the edge of the networks before they ever reach the attack surfaces. Another key to reducing the impact of emerging endpoint attacks is to make events more visible at the endpoints.

Good attack surface management products monitor all systems around the clock for newly discovered new security vulnerabilities. Real-time visibility is critical to detecting the impact of an attack on the attack surface of a range of networks, software, protocols, and services that run online in an enterprise. Given the number and complexity of network and software protocols and services in an online business, it can be difficult to identify which parts of your attacks are the source of breaches and intrusions. The identification of injury risks, which is dynamic and highly complex, is characterized by several complex areas to be explored, such as network infrastructure, network security, data security, and network management.

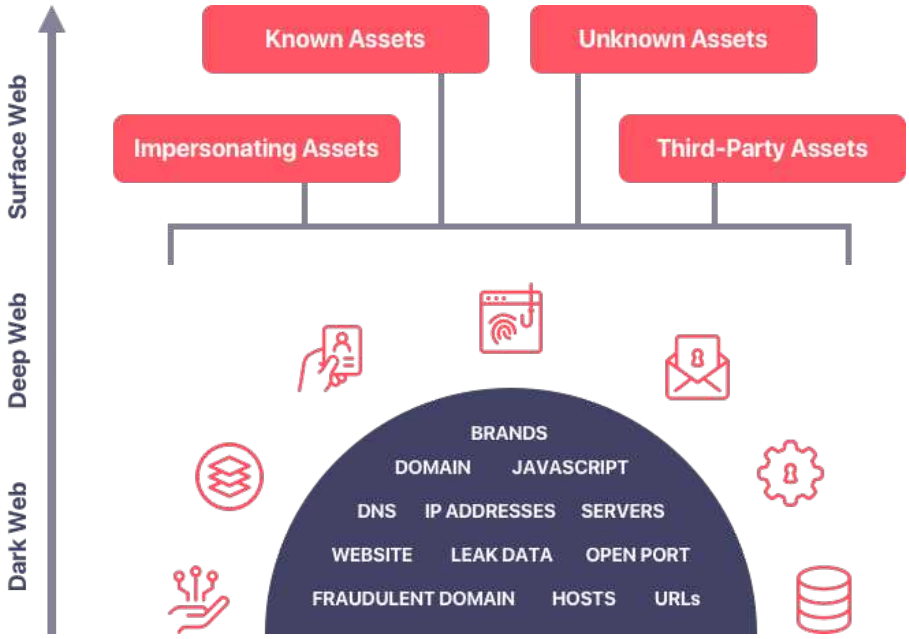
For today's organizations, manage the attack surface per se minimizes the chances that opponents can exploit vulnerabilities and helps prevent data breaches.

What is the attack surface?

The attack interface is the point or vector through which an attacker enters the environment and is merely a list of all possible ways in which the attacker can enter a device or network and extract data. In other words, the attack interfaces can be described as a collection of different points where unauthorized users could infiltrate an IT environment. There are several points from which attackers could attempt to penetrate the environment, such as access to the network, access from a remote location, or access via a network connection.

The attack surface describes the various points at which an attacker can get into the system and access the data. Simply put, the attack surface consists of the network environment of the organization that the attacker can exploit to conduct a successful attack, including protocols, interfaces, software, and services deployed. It is the resource that is exposed to the enterprise.

In modern companies, attack surface is massive and hyper-dimensional, and given the complexity of today's digital landscape, we understand the challenges associated with attack surface management better.



Attack surface can be categorized into the 4 groups.

All attack surfaces can belong to at least one of these 4 groups.

Attack surface refers to any asset such as domain infrastructure, web site services, cloud technologies, etc. that is open to the Internet and can be exploited by the attacker. It can be described as the network interface of an organization, its network infrastructure, and resources. In summary, the attack surface includes:

Impersonating Assets

Malicious infrastructures such as fake domains, malicious social media accounts seem like belonging to companies but created by attackers.

Unknown Assets

Unknown assets are like domains that have been opened and not closed for marketing purposes forgotten by the security team or some sensitive data that the development team forgot in repositories constitute unknown entities.

Known Assets

Known assets are the assets that are registered and managed by companies such as website, server, etc.

3rd Party Assets

The attack surface does not end up only targeting companies own assets and companies. 3rd party JavaScripts on the websites used by the companies or hosting servers used to locate their assets are part of the attack surface in the ecosystems of the companies where data is exchanged.

How to manage the attack surface in 4 steps?

1. Digital footprint discovery

To manage the attack surface, it is necessary to first identify all assets open to the Internet. The Discovery phase is important because companies have many assets that they do not know or forget, as well as assets they know and manage.

For instance, some promotional pages that have been opened for marketing purposes may have forgotten to shut down or may not have been notified to the security team. Any assets that are forgotten or not configured for security pose could be harmful to companies. Because attackers always prefer to attack companies over unmanaged assets.

Also, some exposed PII (personally identifiable information) data and assets used by attackers to imitate the company, such as websites, sm accounts, can be detected in the first step of the attack surface management.

Third-party applications or vendors that are connected to the company's assets also appear at the discovery stage, and in this case, it expands your attack surface as it is included in the company ecosystem.

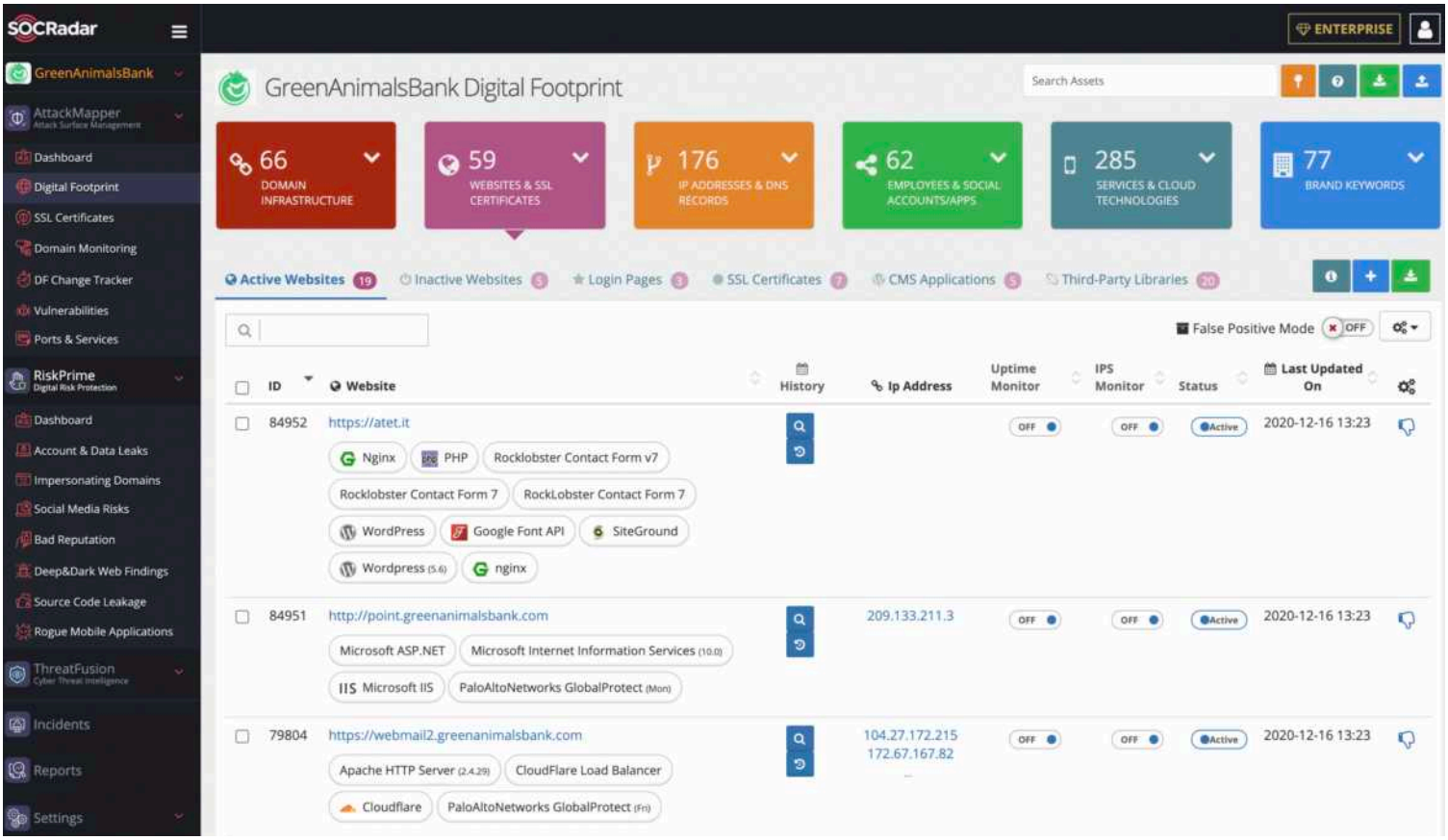
The discovery process ranges from simple scanning of provisioned IP addresses and subnets to more comprehensive OSINT (open-source intelligence) and dark web browsing.

Some security solutions request data inventory from the organization to monitor and manage the attack surface or make some positioning within the company.

SOCRadar takes only the domain address as input for the attack surface discovery of organizations. It explores the entire asset inventory over the surface web, deep web, and dark web with OSINT methodology without touching and damaging any assets of the companies thanks to advanced search methodologies.

Learn more →

2. Asset inventory and classification



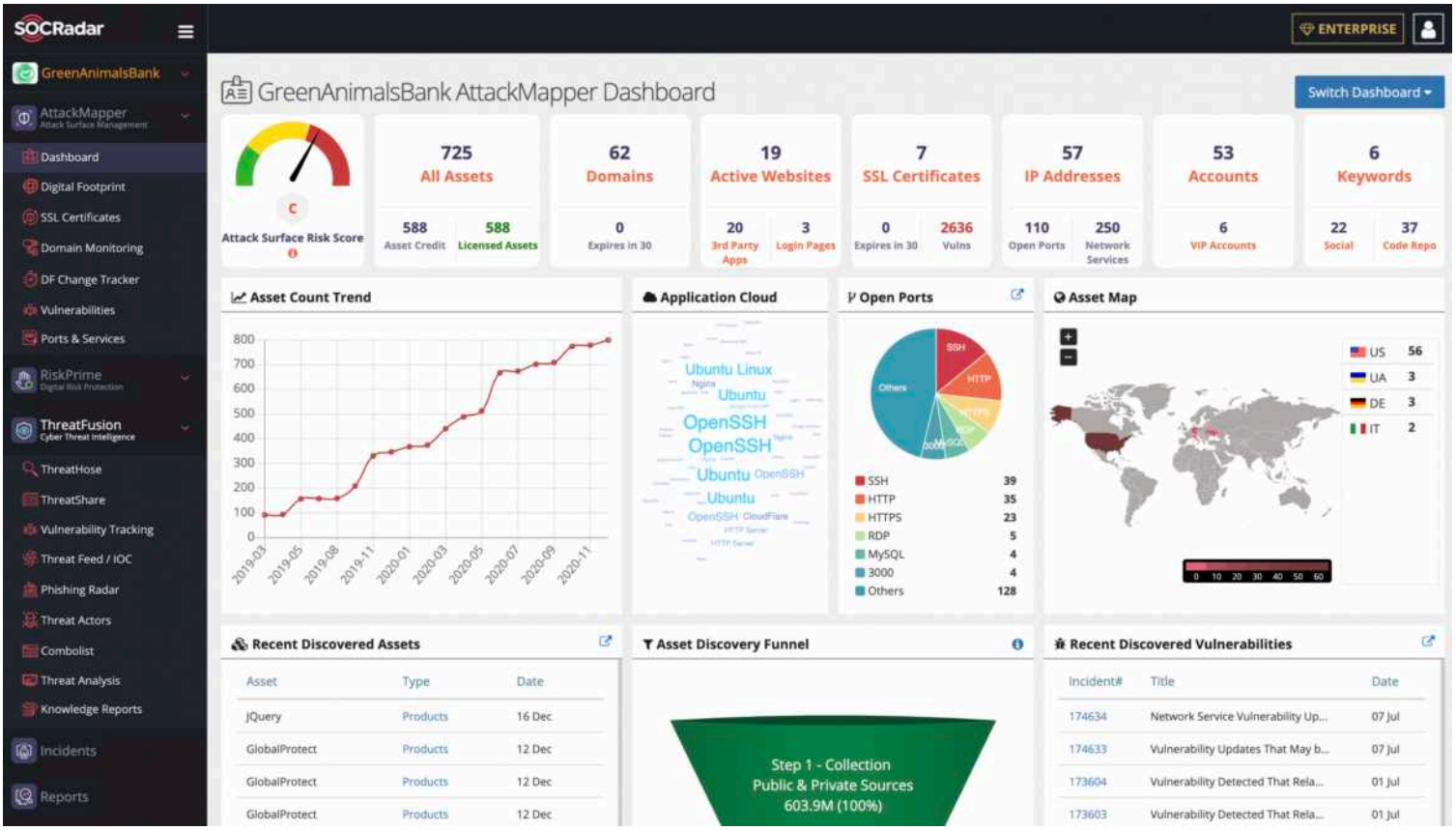
After the assets are discovered, an inventory should be created with the correct labels according to their type, technical characteristics, business criticality, and compliance requirements.

Organizations need asset maintenance and protection that are constantly updated. However, the types of assets managed by each department are different. For example, while the network team wants to monitor changes in DNS records, the management of social media accounts may be under the marketing team. People in charge who want to be able to quickly access the assets they manage. Because of this, it is important to create a correctly classified inventory.

SOCRadar provides easy access to the asset by classifying the assets into different categories. It also has an authorization mechanism that can notify different people who are in charge of the findings that occur during the monitoring of each asset.

Learn more →

3. Continuous security monitoring



Organizations' assets are constantly being updated in the digital world, and security teams are challenging to keep track of updated assets as their inventory grows. There are also a lot of 3rd party applications running on assets and hundreds of easily exploitable security vulnerabilities are published every day on these applications. Therefore, it is imperative to ensure 24/7 monitoring of your digital assets for newly discovered vulnerabilities, and misconfigurations.

SOCRadar aims to continuously monitor the detected assets, to notify the security team about any misconceptions or configurations within the company, and to identify possible offensive activities. Thanks to the **Vulnerability Tracking Module**, applications with weaknesses can be detected within the attack surface.

Learn more →

4. Impersonating assets and incident monitoring

Continuous Security Monitoring covers known and unknown digital assets operated by your organization or authorized third parties. However, the attack surface is wider than that and includes malicious or fraudulent assets created by cybercriminals.

This includes phishing websites to abuse your trademarks or goodwill, mobile apps pretending to belong to you, or digital threats such as fake accounts on social networks.

Therefore, constant monitoring of malicious entities and events is vital to ensure holistic visibility of attack vectors against your organization.

SOCRadar builds instant phishing domain identification, internet-wide scanning, and compromised credential detection technologies by aggregating and correlating massive data points into actionable intelligence alerts.

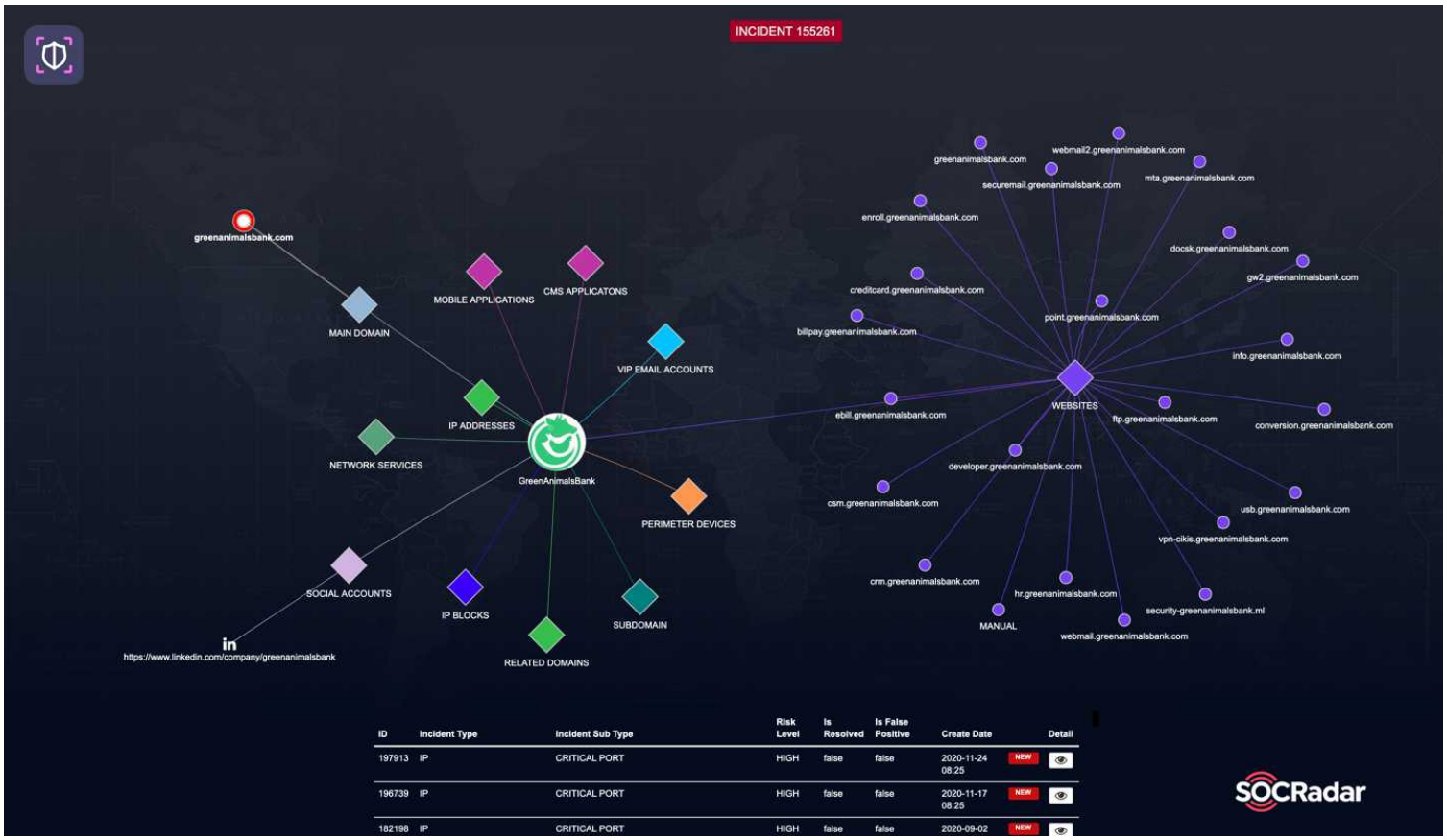
Learn more →

How can SOCRadar help you with attack surface management?

ASM helps customers gain additional visibility and context regarding the severity of unknown external-facing digital assets in an automated manner. Through SOCRadar's advanced internet-wide monitoring algorithms, AttackMapper provides security teams with direct visibility into all internet-facing technological assets in use as well as assets attributed to IP, DNS, Domain, and cryptographic infrastructure.

SOCRadar AttackMapper detects the digital footprint of companies using only the main domain address information and can automatically extract the asset inventory by classifying it.

It regularly monitors your organization's assets and detects changes related to them. By monitoring the assets that make up the attack surface, it enables us to follow the attacker and prevent possible attacks. Also, it can provide information to security teams about missing security configurations that occur within the company, critical open ports, expired SSL certificates/domains, etc.



SOCRadar informs the company when a vulnerability is published regarding the assets of the company that is visible on the external network and their applications. SOCRadar provides the following modules as a service;

- Digital footprint discovery
- Domain/IP monitoring
- SSL certificate monitoring
- DNS monitoring
- Vulnerability detection
- Critical port detection
- JavaScript Monitoring
- Critical data leak detection

See what attackers see.

Stay focused on managing your attack surface to limit the opportunities for cybercriminals.

SOCRadar®

Gartner peerinsights™ 4.9 OUT OF 5 STARS IN 14 REVIEWS AS OF 11/2020

4000 Legato Road, Suite 1100
Fairfax, VA 22033 USA

+1 (571) 249-4598

info@socradar.io

www.socradar.io

SOCRadar delivers intelligent digital risk protection platform against sophisticated cyber attacks for organizations of any size. Its portfolio of digital assets and perimeter monitoring platforms hardened with targeted threat intelligence – all automated and supported by a global team of qualified intelligence analysts – provides unparalleled visibility, management, and protection of digital risks. Prioritized, up-to-date, and relevant cyber threat insights empower customers to take action starting from the reconnaissance stage of the cyberattack life cycle.