ATTACK SURFACE INTELLIGENCE

DATA SHEET

What is Attack Surface Intelligence?

Attack Surface Intelligence (ASI) is a routine process conducted to help organizations monitor their external presence and attack surface on a frequent basis. Unlike a traditional vulnerability management program, which is intended to identify security vulnerabilities present on network systems, services, and applications, the ASI service expands upon this. The tasks conducted during this service include monitoring the public Internet for newly discovered opened/closed ports, identification of compromised email addresses, newly registered domain names similar to that of the organization, and more.

The ASI service is valuable for organizations looking to expand their information security program by actively monitoring for potential threats that could lead to a successful attack against the organization's assets and/or data. Combining this service with a mature vulnerability management solution, the overall discovery rate at which potential attack vectors become available is much less lower.

The following potential attack vectors can be quickly identified and remediated when subscribed to the ASI service:

- Compromised email address discovery
- Newly registered domain names, similar to that of the organization
- Publicly disclosed sensitive data by an employee
- Network service port changes (opened vs. closed)
- Soon-to-expire SSL certificates

THE BENEFITS OF ATTACK SURFACE INTELLIGENCE

Your organization's network staff have many daily tasks to perform, including monitoring firewall logs, responding to security incidents, implementing new network security controls and technology, and managing remediating pre-existing security vulnerabilities. Our consultants can reduce your network staff's responsibilities of managing potential threats originating from the external environment..

PEACE OF MIND

Monitoring for threats that could potentially result in a successful attack against your organization's systems and/or data is a challenging task in itself. Our routine checks against the public Internet for these threats will provide your organization with a peace of mind.

ACTIVE MONITORING & ALERTING

Combining both automated and manual tasks, your network security staff can be assured that, should we identify any data or vulnerabilities that could negatively impact your organization, we will immediately investigate the details and alert your network security staff with valuable data and recommendations.

MANAGED SECURITY

Allowing us to partner with your network staff to monitor the external presence will allow your team the ability to focus on other areas. Through this team effort, we will continuously monitor your external presence for pre-existing as well as new security threats.

Our Attack Surface Intelligence Methodology

Based on our professional experience, research, and the activities performed by modern-day attackers, Vonahi Security consultants have combined several different methods to identify potential threats that target your organization. The following tasks are performed as part of our ASI service.

IDENTIFICATION OF SERVICE AND PORT CHANGES

Based on a baseline configuration, we can identify when a newly discovered network service or port has been opened within your external presence.

UNNECESSARY INTERNET-FACING SERVICES

Occasionally, network administrators may unintentionally allow a port, service, or even a directory of a web application to be exposed to the public Internet. Services that may not be required for business operations will be reported to network security staff.

COMPROMISED EMPLOYEE EMAIL ADDRESSES

Compromised employee email addresses could pose a significant threat to your organization, as many users use the same account credentials with multiple services. Using several publicly accessible databases that report compromised email addresses, our service can quickly identify if your employees' email addresses become compromised.

REGISTRATION OF DOPPELGANGER DOMAIN

Doppelganger domains are domains which are similar to your organization and can be used for social engineering attacks. Our service will monitor the public Internet for newly-registered doppelganger domains that are not owned by your organization.

PUBLICLY DISCLOSED SENSITIVE DATA

On a rare basis, employees, including network administrators, unintentionally disclose information that may be valuable to an attacker, such as internal IP address information, log data, etc. Using our fine-tuned web crawlers, targeted against common and popular web forums and sites, we can, in many cases, identify when there may be publicly disclosed data that pertain to your organization.

What You Get

At Vonahi Security, we understand the demands and expectations for quality information security services. As part of our ASI services, your organization can expect the following:

- **Investigated & Validated Incidents**
- **Custom Alerts & Reporting**
- **Professional & Results-Driven Recommendations**
- **Experienced & Certified Security Experts**

VONAHI SECURITY

ABOUT US

Vonahi Security is a cybersecurity consulting firm that offers comprehensive information security services. Our team is comprised of security experts experienced in offensive and defensive operations, allowing us to provide quality information security services. We ensure your organization is successful with achieving its security goals and remaining one step ahead of malicious adversaries.

HELLO WORLD. MEET MODERN SECURITY.

www.vonahi.io

info@vonahi.io

1.844.VONASEC (866-2732)

@vonahisec