CYBERSPRINT
BREAKTHROUGH SECURITY

ATTACK SURFACE MANAGEMENT FOR

API SECURITY

An API is an Application Programming Interface. It functions as a communication bridge between applications and software, so that an information request is met with the correct response.

However, there are also things that can go wrong in this process. That can result in a compromised communication process where threat actors can interfere with the information requests.

Protecting your APIs with the proper security measures is critical, as APIs expose all your application functionalities and data, and almost all system traffic uses this technology.

OUR ATTACK SURFACE MANAGEMENT PLATFORM WILL HELP YOU TO

PREVENT INCIDENTS

Continuous insights from an outside-in perspective help identify vulnerabilities and assess risks.

IMPROVE PRODUCTIVITY

Contextual API information and proposed mitigation actions help to delegate security fixes.

UPHOLD OPERATIONS

Automated risk detection enables continuous monitoring of APIs for all related services.

PROTECT BRAND REPUTATION

Mitigate risks to provide a continuous level of service, both for customers and employees.

WHY YOU NEED API SECURITY

AUTOMATED, OUTSIDE-IN, AND CONTINUOUSLY

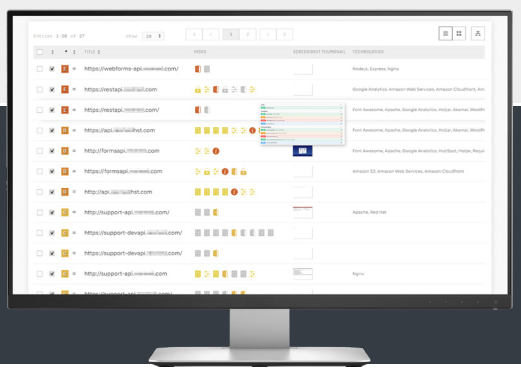
Web-based APIs are widely used for things such as programming and accessing databases. That makes it an appealing process for threat actors as well. Insufficient encryption allows them to immediately access large amounts of data because APIs don't require users to click through menus or filters. On top of that, it's easy to accidentally install an API as a lot of software automatically comes with the technology.

348%

API ATTACK TRAFFIC GROWTH
OVER H1 2021*

SECURING APIS IS A NECESSARY STEP FOR ALL FACETS OF THE ORGANISATION, AS IT

- > ensures business continuity
- > decreases risk exposure
- > prevents incidents and data leaks
- > ensures compliance to regulations
- > protects the brand reputation and the trust from customers and employees



API SECURITY AS PART OF OUR PLATFORM

The API Security solution is available as a standard feature to the Attack Surface Management platform. It builds on the mechanics of the Asset Identification & Risk Detection processes, but uses additional techniques and algorithms to look for APIs and potential risks in their configuration settings.

* SALT, STATE OF API SECURITY REPORT Q3 2021

THE ATTACK SURFACE MANAGEMENT SOLUTION FOR

API SECURITY

The Cybersprint Attack Surface Management platform helps you by identifying the APIs in your attack surface. Automatic risk assessment provides the contextual data to determine the risk level, evidence, and proposed mitigation actions per asset.

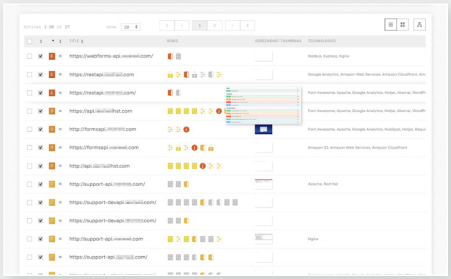
HACKER MODUS OPERANDI

STEP 1

Find an entry point:

> Identify the target's API end points and scan for weaknesses

ASM PLATFORM SOLUTIONS



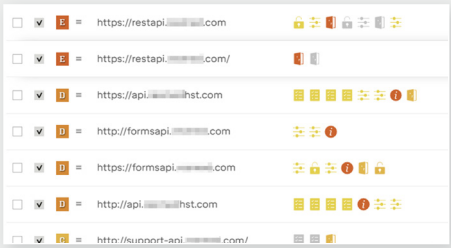
IDENTIFY

Discover and collect information on publicly exposed APIs within the attack surface

STEP 2

Exploit the API misconfiguration or vulnerability

Elevate privileges for increased access and control



ASSESS

Assess the risks related to API endpoints (configuration, authentication, or authorization)

Identify infrastructure exposed through the API's vulnerabilities

STEP 3

Gain access and visibility into back-end applications or databases

MANAGE

Obtain remediation advice and track mitigation status over time

Automatic notifications for new vulnerabilities

Integrate with CMDBs

STEP 4

Abuse the data and interfere with processes

Threaten with, or cause a data leak

REPORT

Export vulnerability and risk information to support:

> Governance and vulnerability management

> Audits and compliance

OUR ATTACK SURFACE MANAGEMENT PLATFORM WILL

DETECT & ASSESS THE APIs IN YOUR ATTACK SURFACE – AUTOMATICALLY AND MANUALLY

DETERMINE EACH ASSET'S RISK LEVEL BASED ON CONTEXTUAL INFORMATION

PREVENT MALICIOUS INTERFERENCE WITH SYSTEM PROCESSES

cybersprint.com info@cybersprint.com +31 70 22 12 892 @cybersprintnl /cybersprint