

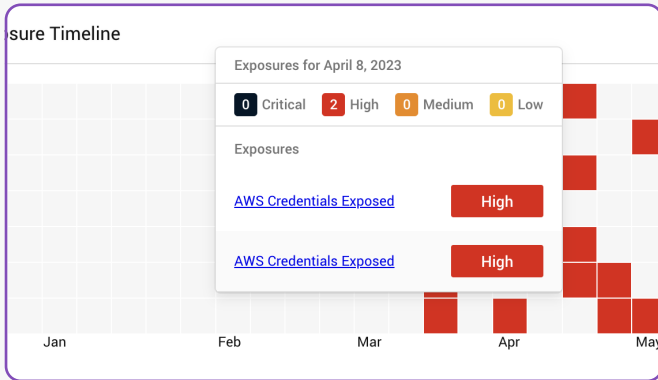


Do you know your
exposure to external
attack?



Next-Gen Vulnerability Detection

Our attack surface management platform provides high signal, real-time and continuous security monitoring of your assets. Every hour, our exposure engine analyses the entire attack surface of the organisation to uncover potential exposures.



Real-Time Exposure Detection

Continuous high-signal monitoring of all assets for security exposures means reducing the risk of a critical incident, removing opportunities for attackers to gain access and go on to execute their objectives. In dynamic modern IT environments where changes can happen on a minute to minute basis, high frequency scanning is required to detect changes.

No Time For Noise

False positives cause breaches by distracting security teams from real consequential security alerts. By validating vulnerabilities for exploitability and impact, you can focus on what matters.

Validate With PoCs

Security teams spend significant time investigating alerts to try and reproduce the issue. Supplied Proof of Concepts for each issue allow teams to immediately validate and remediate findings

Speed Where It Counts

Modern IT environments move fast. As with discovery of assets, high frequency monitoring is key to identifying exposures in highly dynamic environments.

Backed by our Innovative Security Research

Backed by industry leading penetration testers, bug hunters and security researchers, the Assetnote Continuous Security Platform is underwritten by leading security research. Assetnote customers are the first to know about some of the most damaging 0 days with clear advice for remediation or mitigation.

Name	Category	Subcategory	Asset	Port	Severity	Custom Severity
WordPress Setup Exposed	Server Security Misconfiguration	Insecure Exposure of Administrative Functionality	booking.ab.c.fr	443	Critical	Critical
JIRA Information Disclosure - Filters	Server Security Misconfiguration	Insecure Cloud Infrastructure Configuration	test.jira.abcgroup.com	443	Low	Low
Subdomain Takeover (Elastic IP)	Server Security Misconfiguration	Insecure DNS Configuration	safeg.abc.com.tr	443	High	High
Remote Command Execution (Sitecore Report.aspx)	Injection and Output Encoding	Remote Code Execution	qa-origin.test.taab.com	80	Critical	Critical
WordPress User Information Disclosure	Server Security Misconfiguration	Insecure Web Server Configuration	specjalista-s-przedlady-przeodbitkow-hankowych.ab.c.pl	443	Low	Low
JNDI Injection via Log4j (CVE-2021-4428)	Injection and Output Encoding	Remote Code Execution	reports.test.aab.com	443	Critical	Critical
Server Side Request Forgery (Microsoft)	Server Security	Use of Unpatched	autodiscover	443	Critical	Critical

Get In Touch For A Live Demo

Don't wait until your next quarterly penetration test (or worse a breach) to find out you have a security issue. Come book a live demo with us today.

<https://assetnote.io>

[@assetnote](#)

contact@assetnote.io

