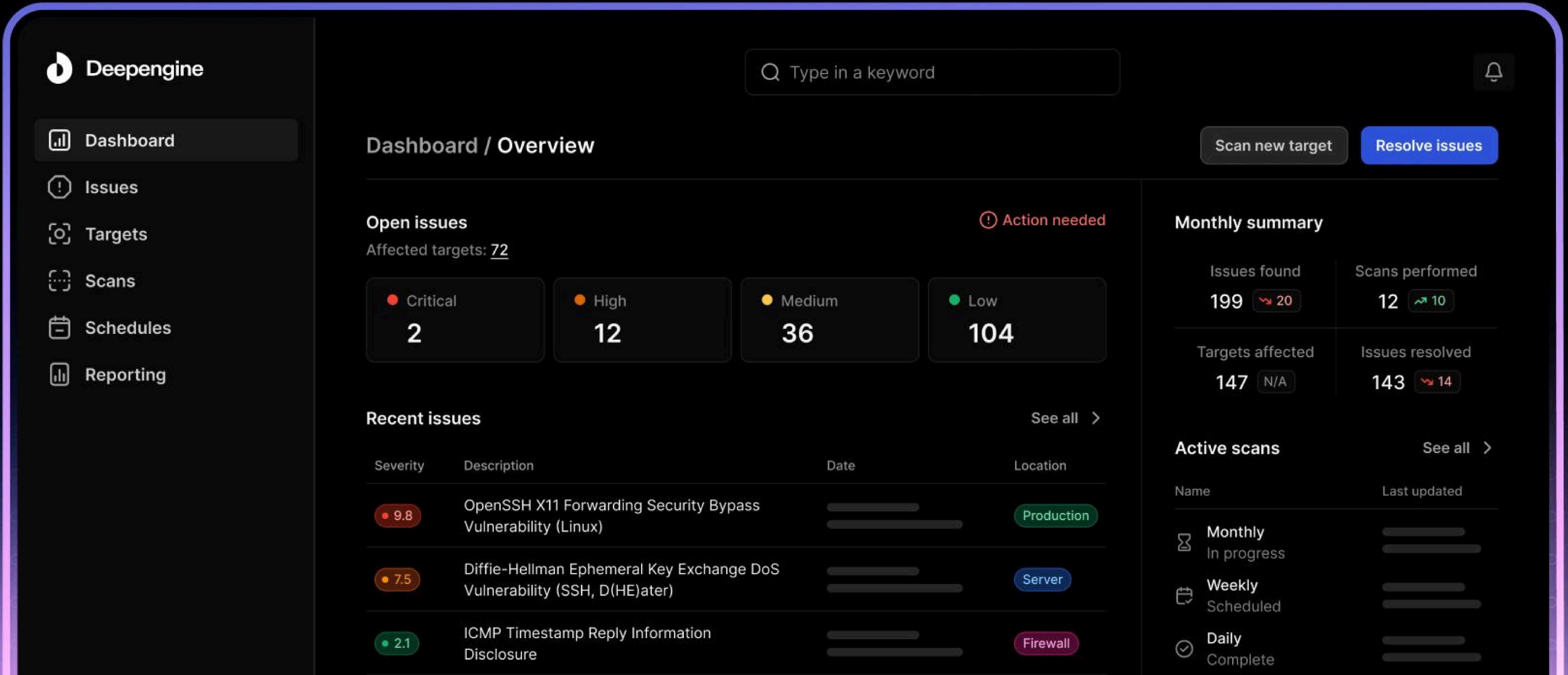
Vulnerability scanning for products of any size



Dashboard / Overview

Open issues

Affected targets: 72

Action needed

Critical	High	Medium	Low
2	12	36	104

Recent issues See all

Severity	Description	Date	Location
9.8	OpenSSH X11 Forwarding Security Bypass Vulnerability (Linux)		Production
7.5	Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSH, D(HE)ater)		Server
2.1	ICMP Timestamp Reply Information Disclosure		Firewall

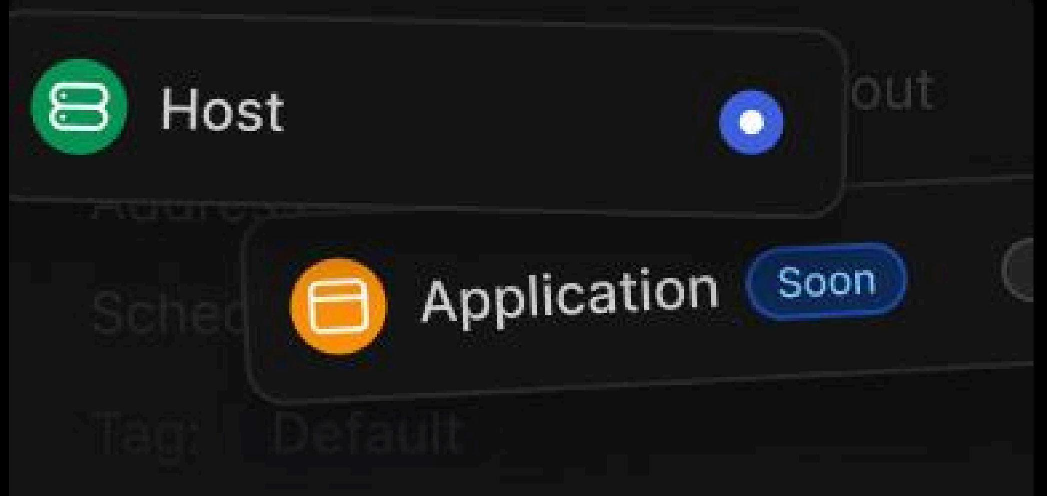
Monthly summary

Issues found	Scans performed
199 ↘ 20	12 ↗ 10
Targets affected	**Issues resolved**
147 N/A	143 ↘ 14

Active scans See all

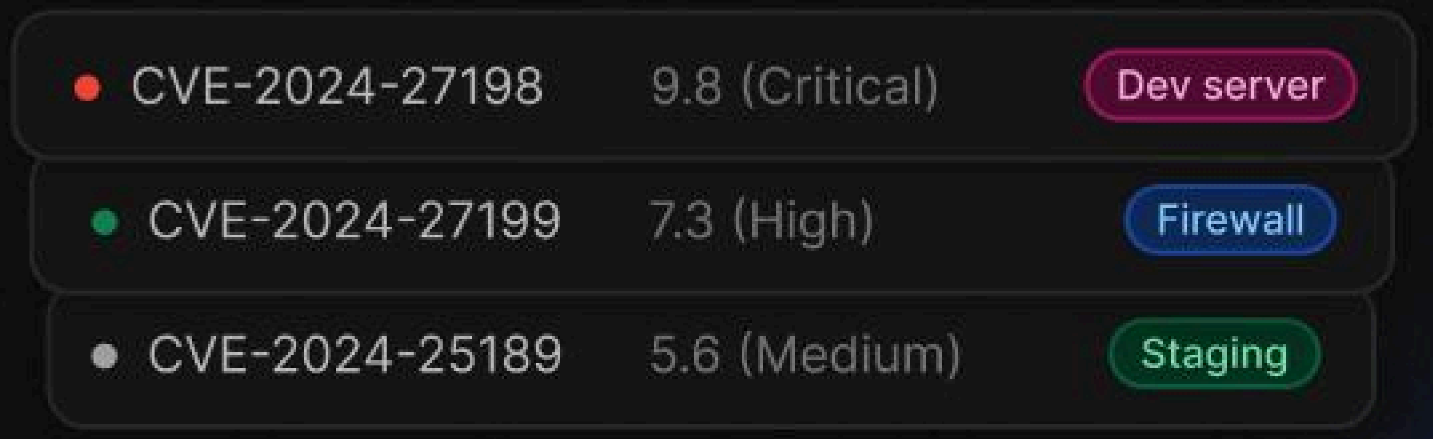
Name	Last updated
Monthly In progress	
Weekly Scheduled	
Daily Complete	

Meet your command centre for threat intelligence



Target management

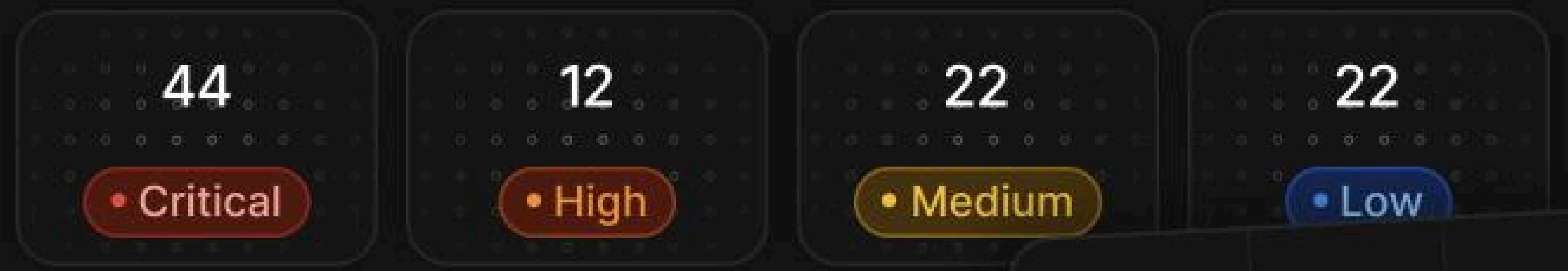
Add targets with few clicks, group them by tag



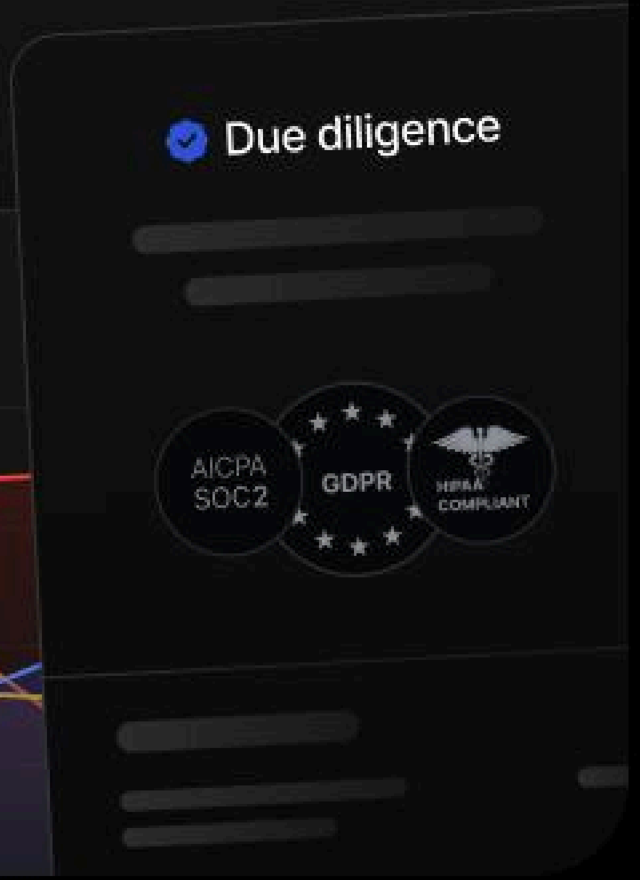
● CVE-2024-27198	9.8 (Critical)	Dev server
● CVE-2024-27199	7.3 (High)	Firewall
● CVE-2024-25189	5.6 (Medium)	Staging

Emerging threat scanning

Get automatic scanning for the newest cybersec threats



44	12	22	22
• Critical	• High	• Medium	• Low



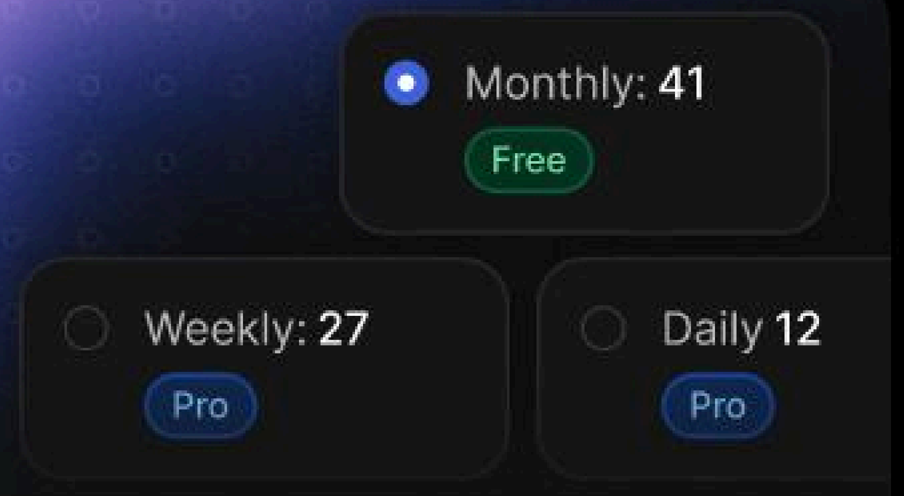
Reporting & compliance

Generate reports for each scan, act on issues, and use for compliance

PC
Server
Router
Firewall

Public infrastructure

Find security breaches in all of your publicly available infrastructure



● Monthly: 41 Free

○ Weekly: 27 Pro

○ Daily 12 Pro

Flexible schedules

Scan consistently on a daily, weekly, or monthly basis.

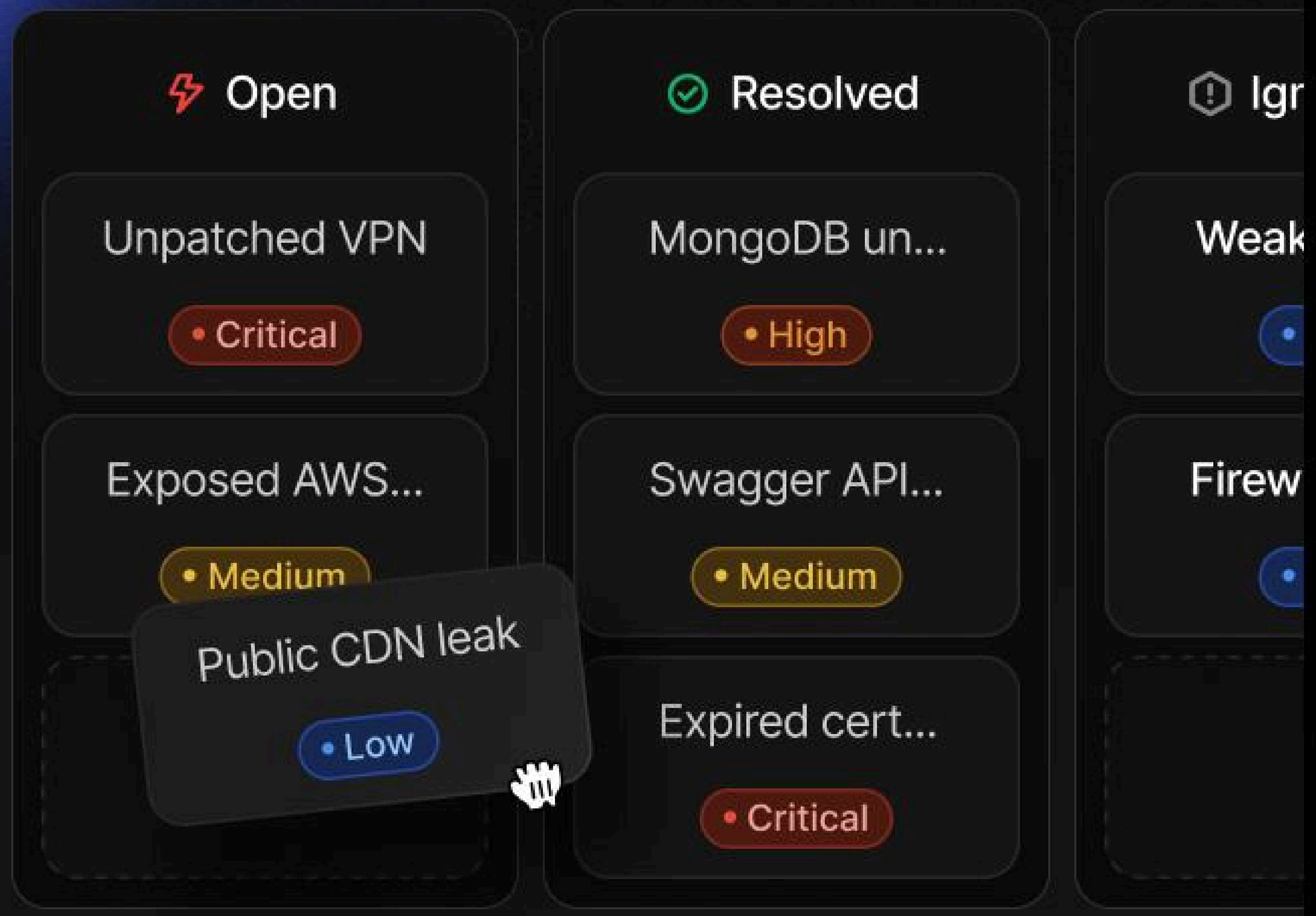
Deepengine APP 8:24 AM

🔥 New critical threat found in "Public server"

👀 1

Integrations

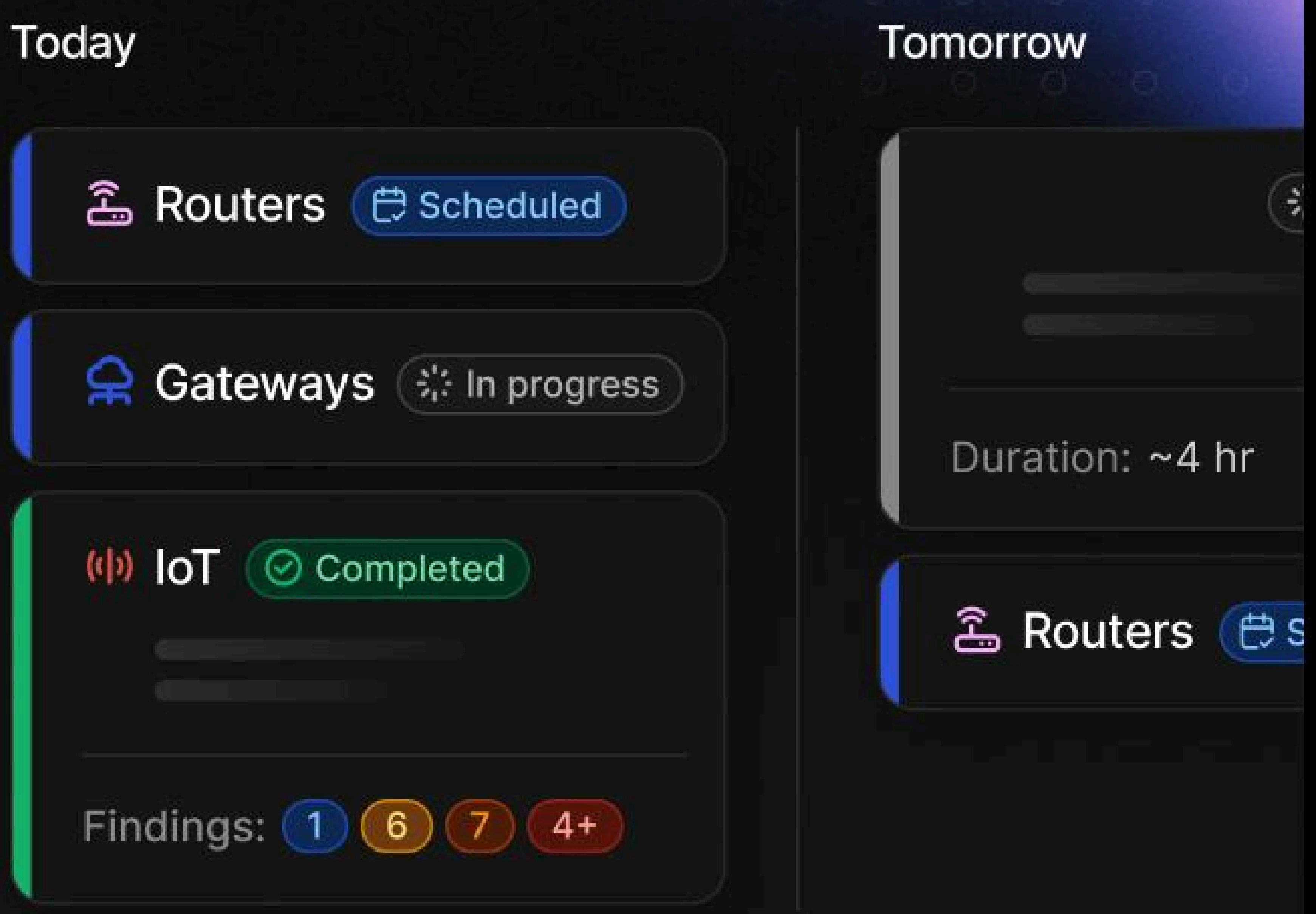
Get Slack updates, or use Webhook for custom workflows



Detect up to 150K potential treats

Detect misconfigurations, outdated patches, injections, data breaches, and more.

Put your threat scanning on autopilot

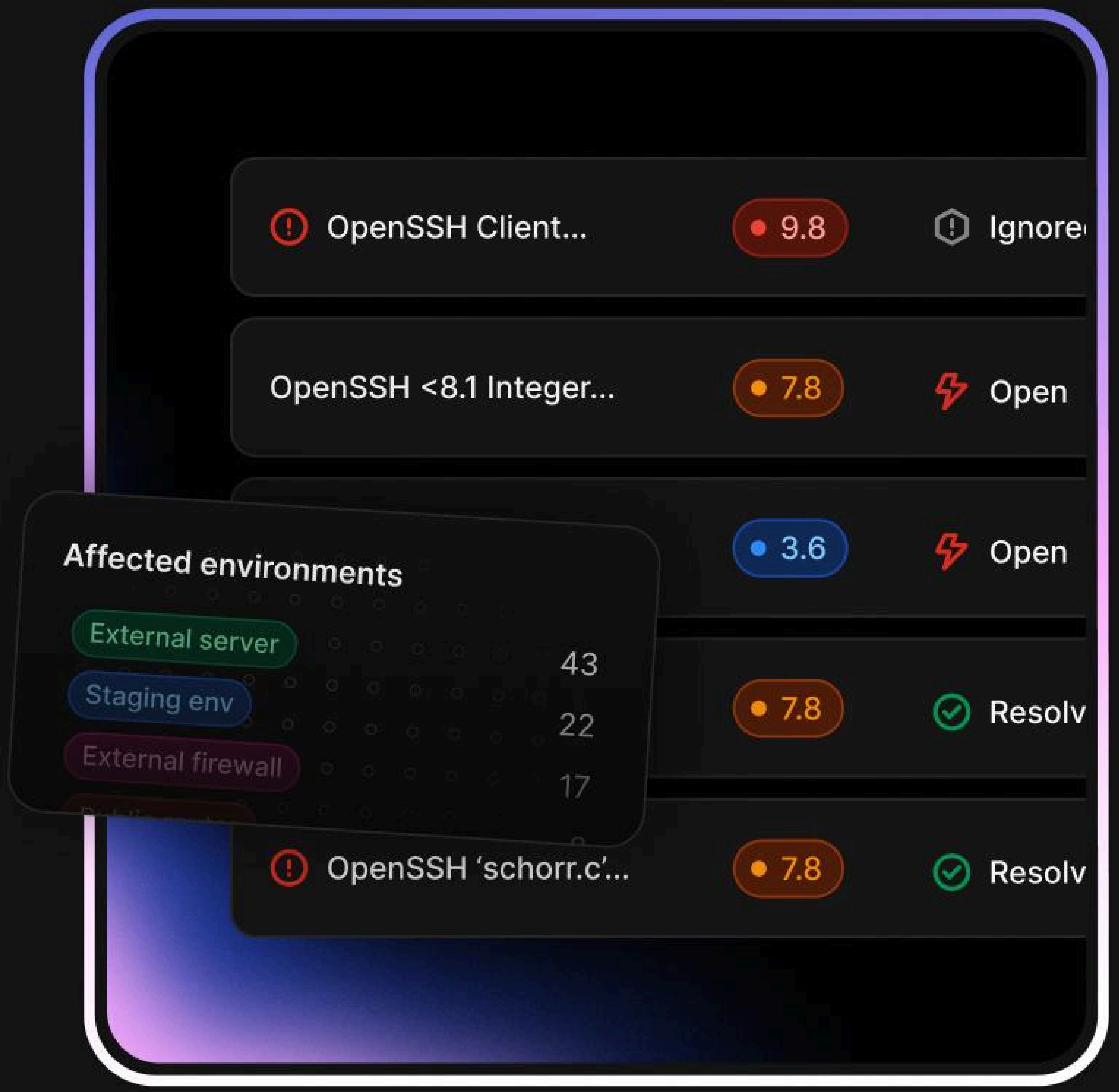


Consistent threat reconnaissance

Daily, weekly, and monthly schedules help you close security gaps on a consistent basis.

Broad visibility over security gaps

Easily scan your external infrastructure for over 150,000 threats with scheduled or on-demand scans. Additionally, automatically scan targets for emerging threats right when they appear in public.

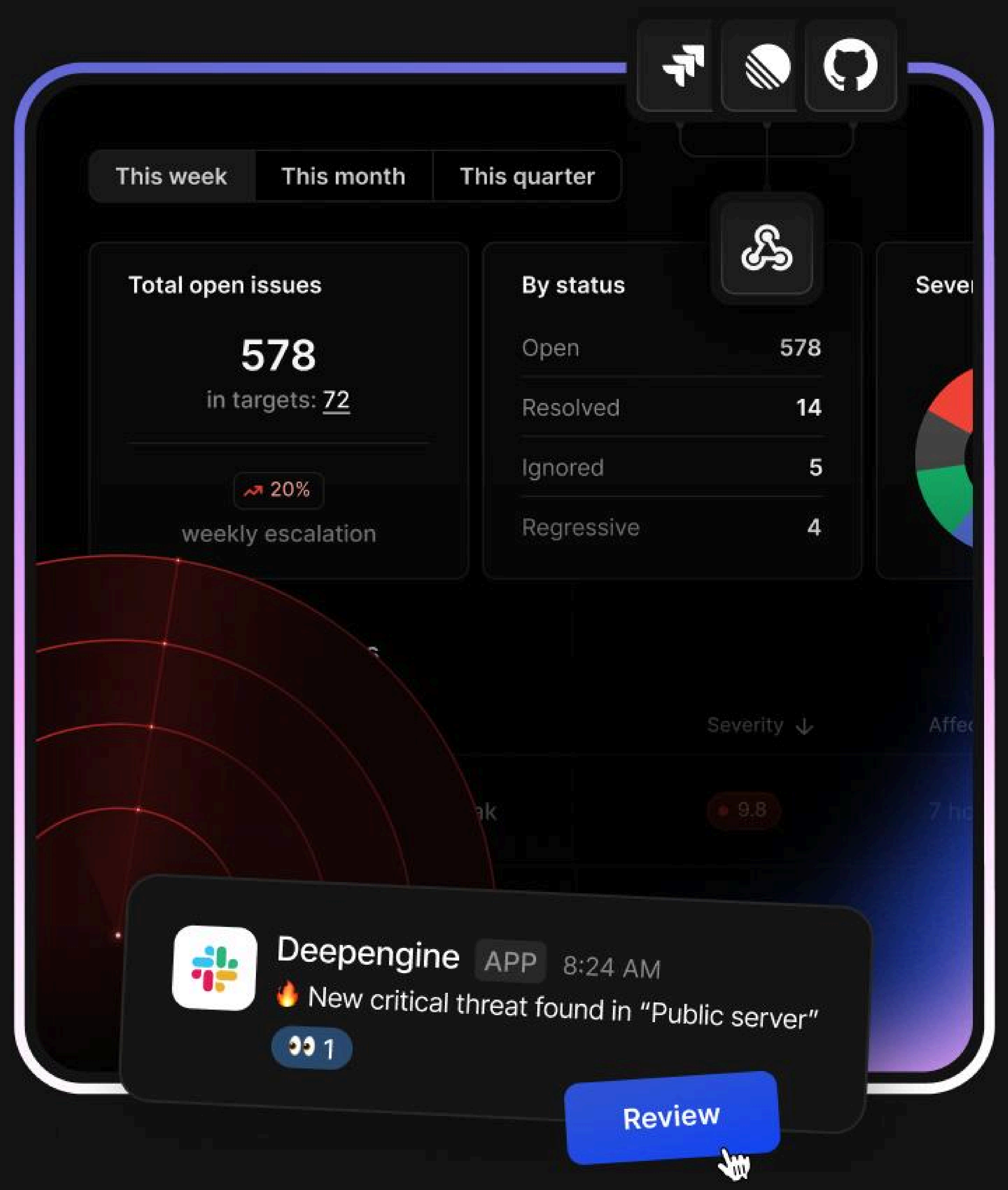


OpenSSH Client... ● 9.8 Ignore
OpenSSH <8.1 Integer... ● 7.8 Open
● 3.6 Open
● 7.8 Resolv
OpenSSH 'schorr.c'... ● 7.8 Resolv

Affected environments
External server 43
Staging env 22
External firewall 17

Speed up detection and response

Accelerate your threat response by connecting Deepengine to your ticketing systems via Webhooks or integrate with Slack to act on findings ASAP.



Total open issues

578

in targets: 72

↗ 20% weekly escalation

By status

Open	578
Resolved	14
Ignored	5
Regressive	4

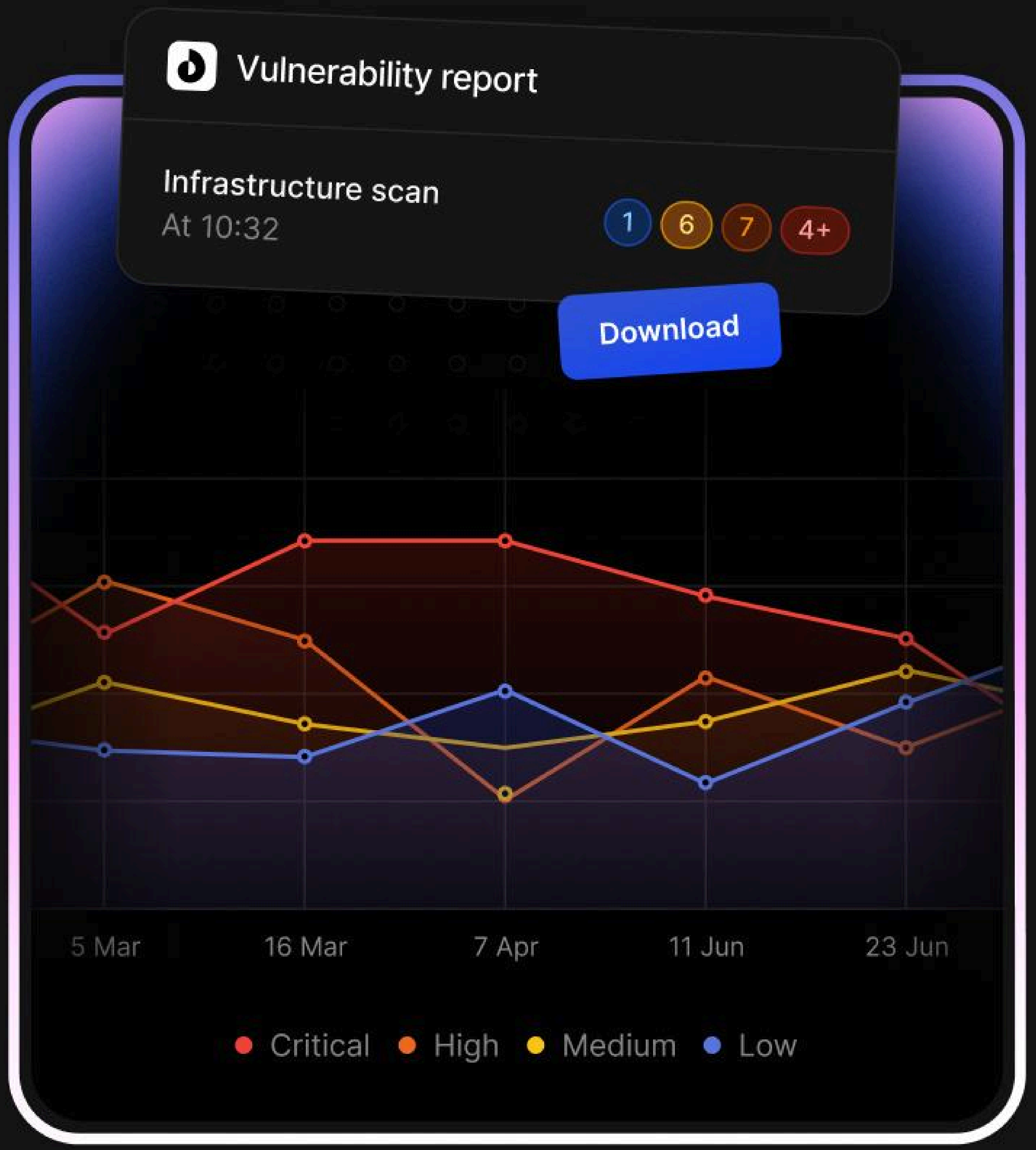
Deepengine APP 8:24 AM

🔥 New critical threat found in "Public server"

👀 1

Document findings and comply easier

Get structured reports capturing insights from every scan. Let your team evaluate your threat landscape or use as a handoff for due diligence.



Thank you!

To learn more, visit:

https://deepengine.io