



Vulnerability scanning for products of any size

The screenshot shows the Deepengine dashboard with a sidebar on the left containing navigation items: Dashboard, Issues, Targets, Scans, Schedules, and Reporting. The main content area is titled 'Dashboard / Overview' and includes a search bar, a notification bell, and two buttons: 'Scan new target' and 'Resolve issues'. The 'Open issues' section shows a total of 72 affected targets, broken down by severity: 2 Critical, 12 High, 36 Medium, and 104 Low. An 'Action needed' indicator is present. The 'Monthly summary' section displays metrics for issues found (199, down 20), scans performed (12, up 10), targets affected (147, N/A), and issues resolved (143, down 14). The 'Active scans' section lists three scans: 'Monthly In progress', 'Weekly Scheduled', and 'Daily Complete'. The 'Recent issues' table lists three vulnerabilities: OpenSSH X11 Forwarding Security Bypass (9.8, Linux, Production), Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (7.5, SSH, D(HE)ater, Server), and ICMP Timestamp Reply Information Disclosure (2.1, Firewall).

Deepengine

Dashboard / Overview

Search: Type in a keyword

Buttons: Scan new target, Resolve issues

Open issues Action needed
Affected targets: 72

Severity	Count
Critical	2
High	12
Medium	36
Low	104

Monthly summary

Metric	Value	Change
Issues found	199	↓ 20
Scans performed	12	↑ 10
Targets affected	147	N/A
Issues resolved	143	↓ 14

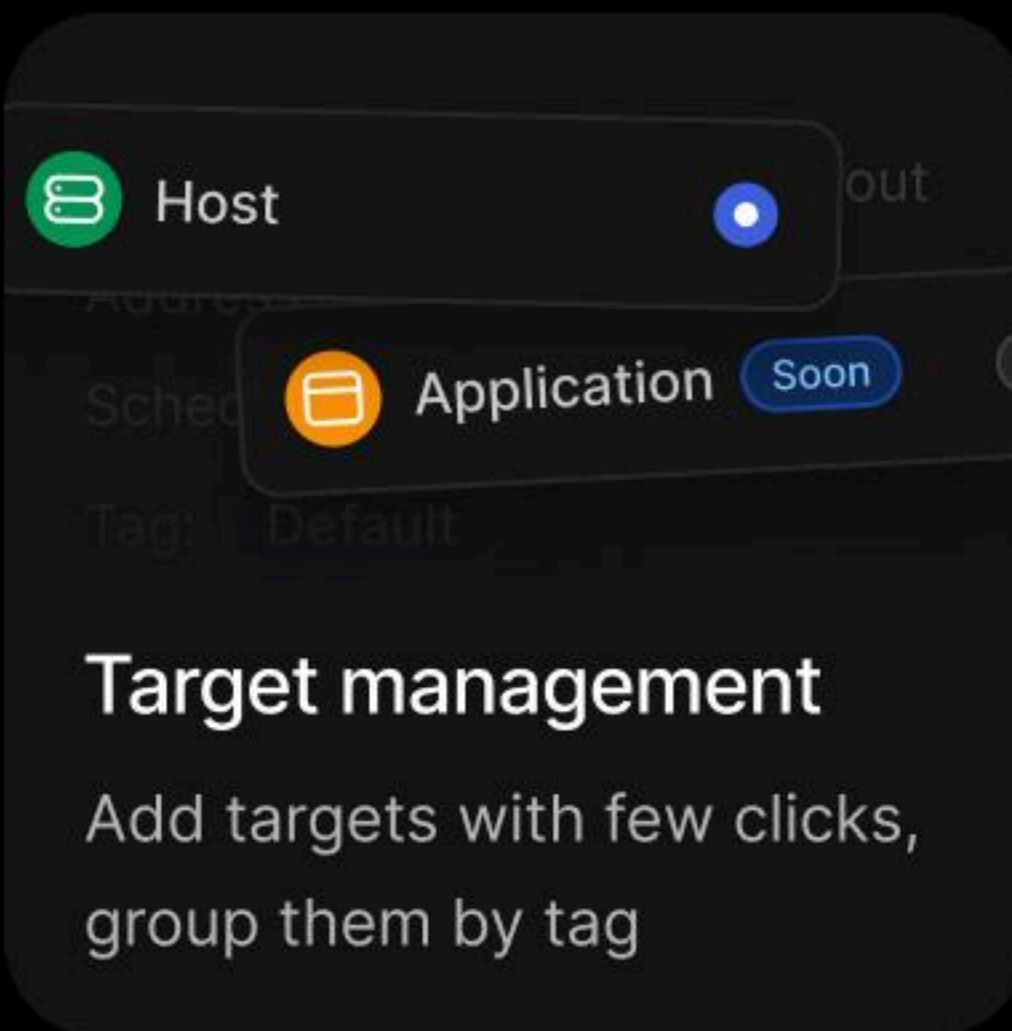
Active scans

Name	Last updated
Monthly In progress	
Weekly Scheduled	
Daily Complete	

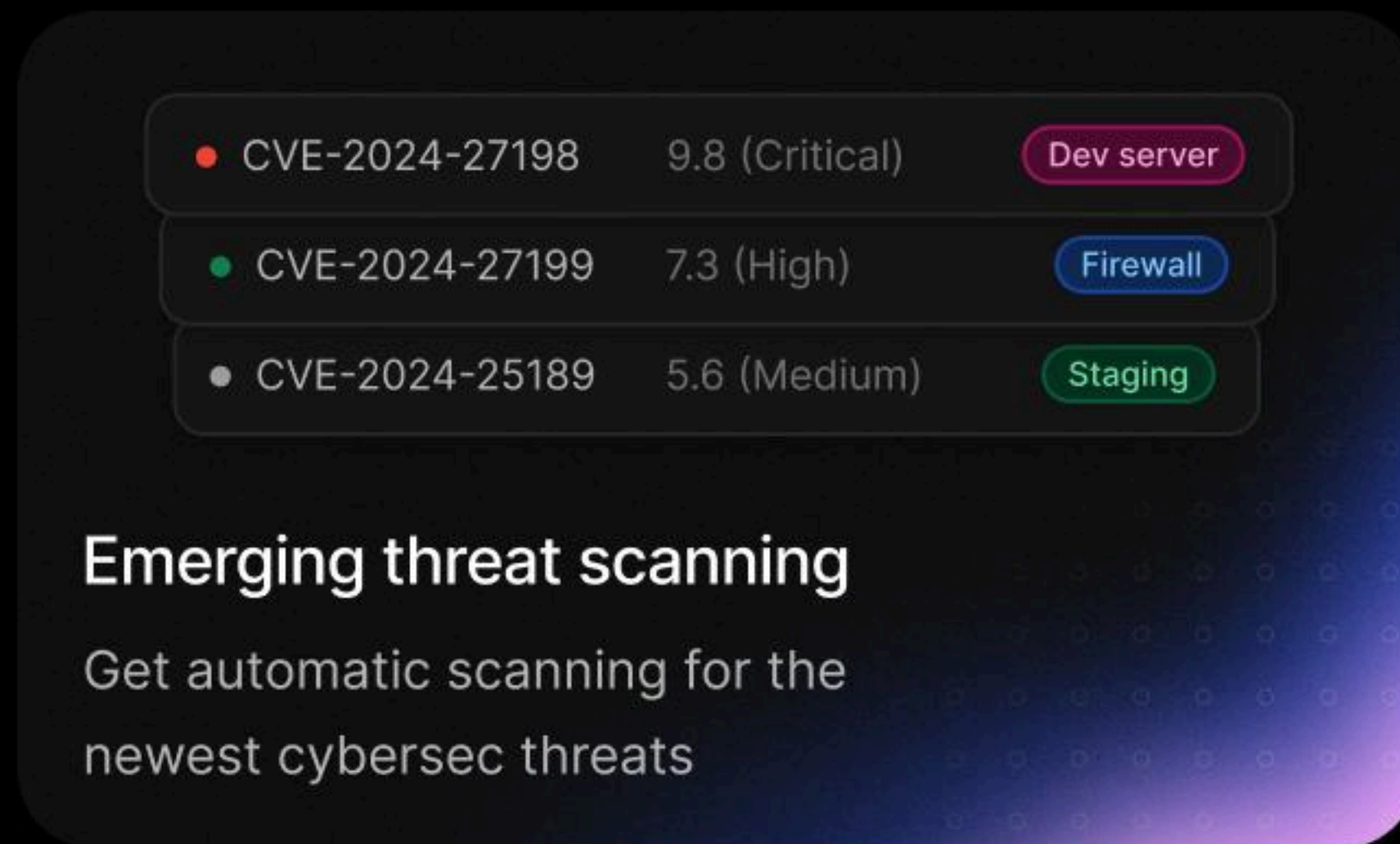
Recent issues See all >

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

Meet your command centre for threat intelligence



Target management
Add targets with few clicks, group them by tag

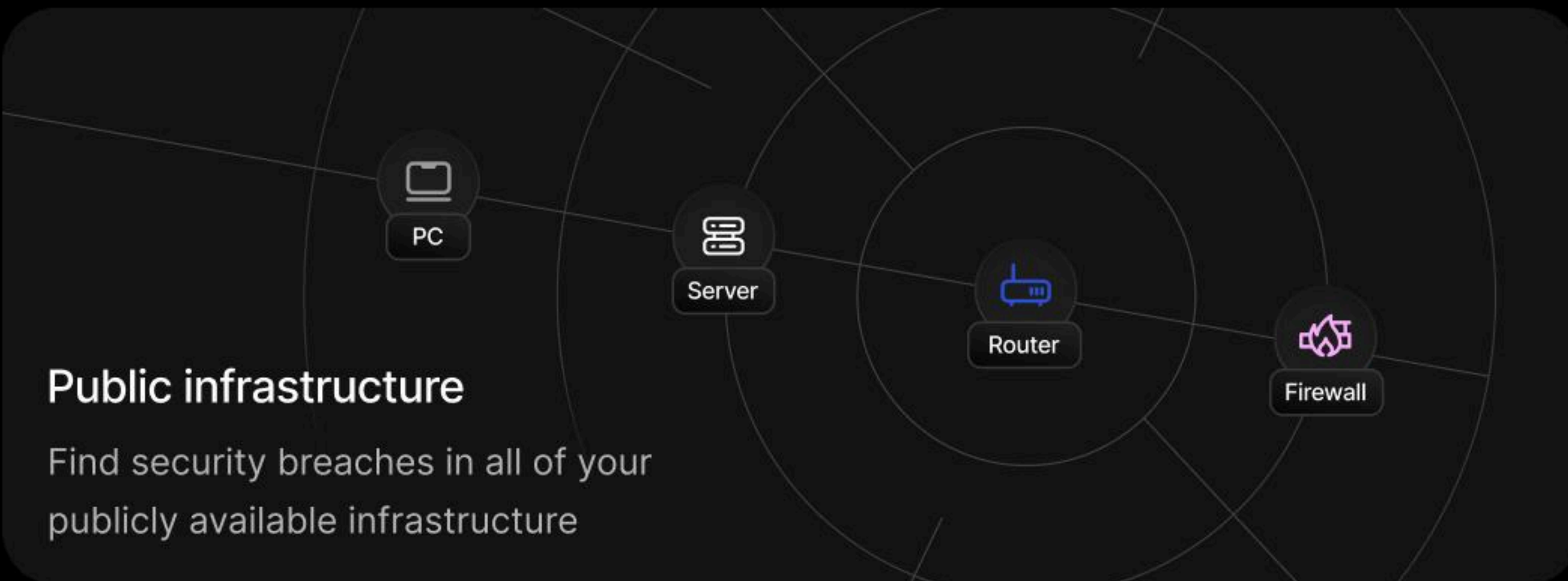


CVE-2024-27198	9.8 (Critical)	Dev server
CVE-2024-27199	7.3 (High)	Firewall
CVE-2024-25189	5.6 (Medium)	Staging

Emerging threat scanning
Get automatic scanning for the newest cybersec threats



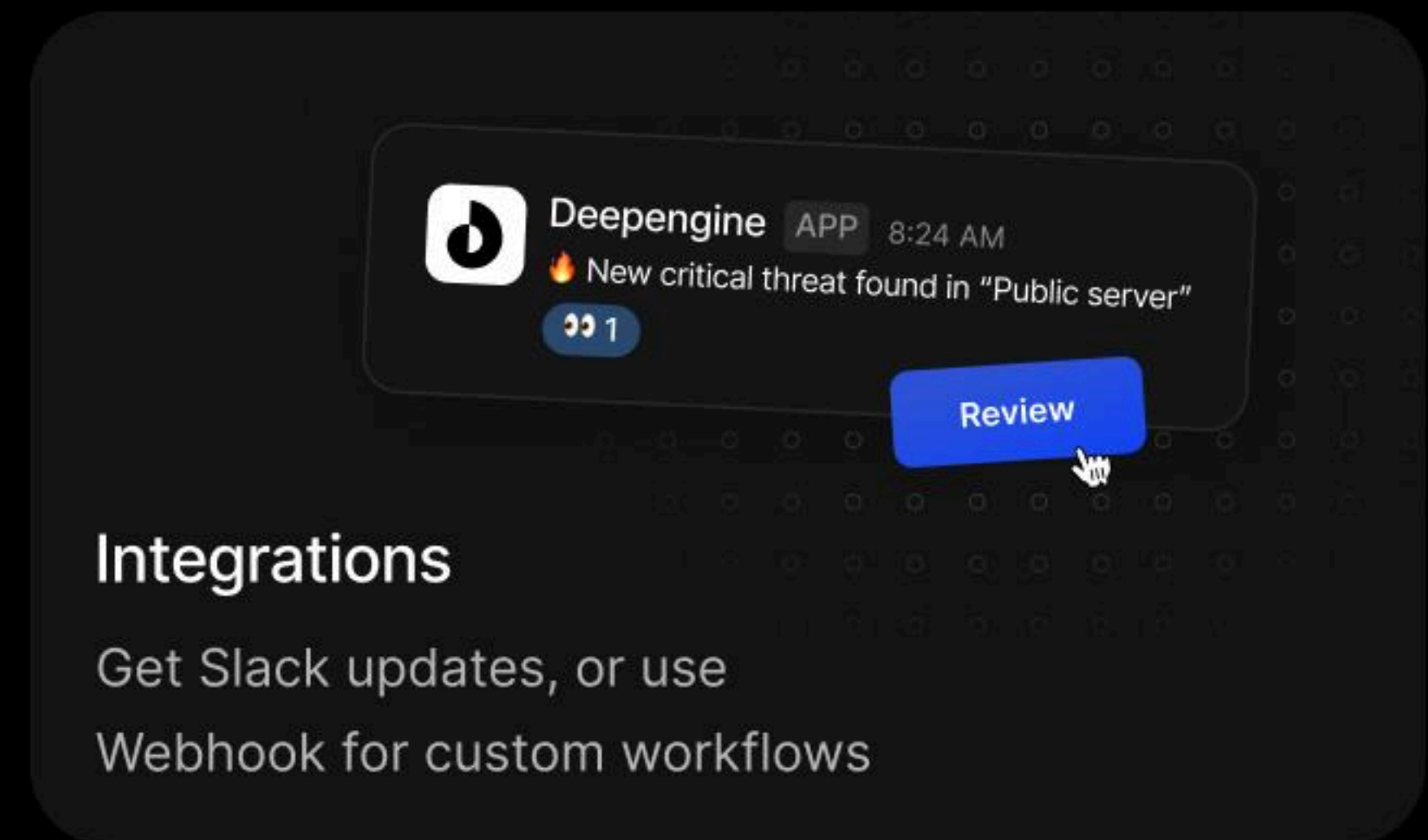
Reporting & compliance
Generate reports for each scan, act on issues, and use for compliance



Public infrastructure
Find security breaches in all of your publicly available infrastructure



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



Integrations
Get Slack updates, or use Webhook for custom workflows



Put your threat scanning on autopilot

The dashboard is divided into three columns: 'Open', 'Resolved', and 'Ignored'. Under 'Open', there are four items: 'Unpatched VPN' (Critical), 'Exposed AWS...' (Medium), 'Public CDN leak' (Low), and 'Expired cert...' (Critical). Under 'Resolved', there are two items: 'MongoDB un...' (High) and 'Swagger API...' (Medium). Under 'Ignored', there are two items: 'Weak...' and 'Firew...'. A mouse cursor is hovering over the 'Public CDN leak' item.

Detect up to 150K potential threats

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

Today

The 'Today' section shows three items: 'Routers' (Scheduled), 'Gateways' (In progress), and 'IoT' (Completed). Below these items, there is a 'Findings' section with four colored circles containing the numbers 1, 6, 7, and 4+.

Tomorrow

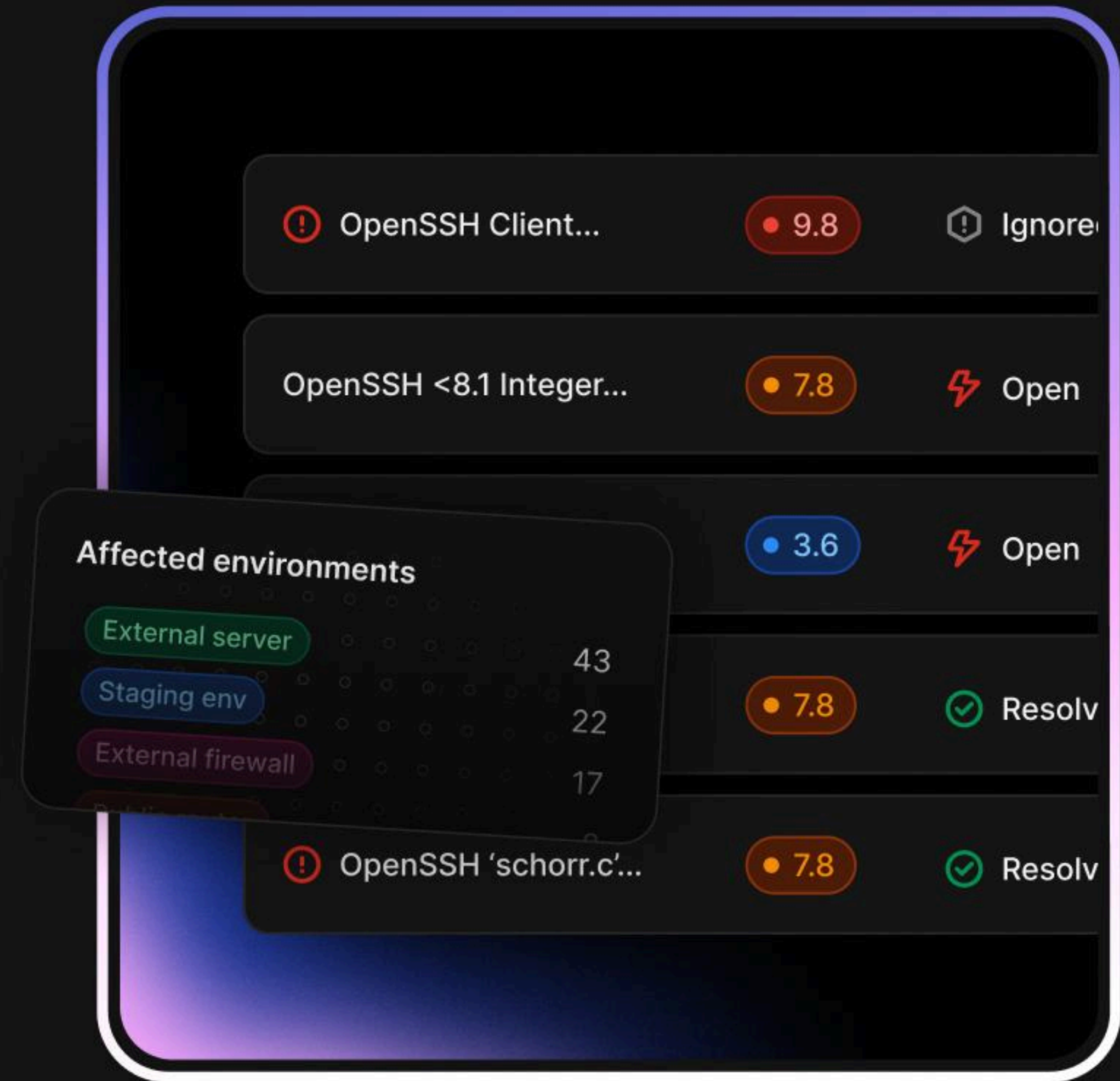
The 'Tomorrow' section shows one item: 'Routers' (Scheduled). Below this item, there is a 'Duration' section with the text '~4 hr'.

Consistent threat reconnaissance

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

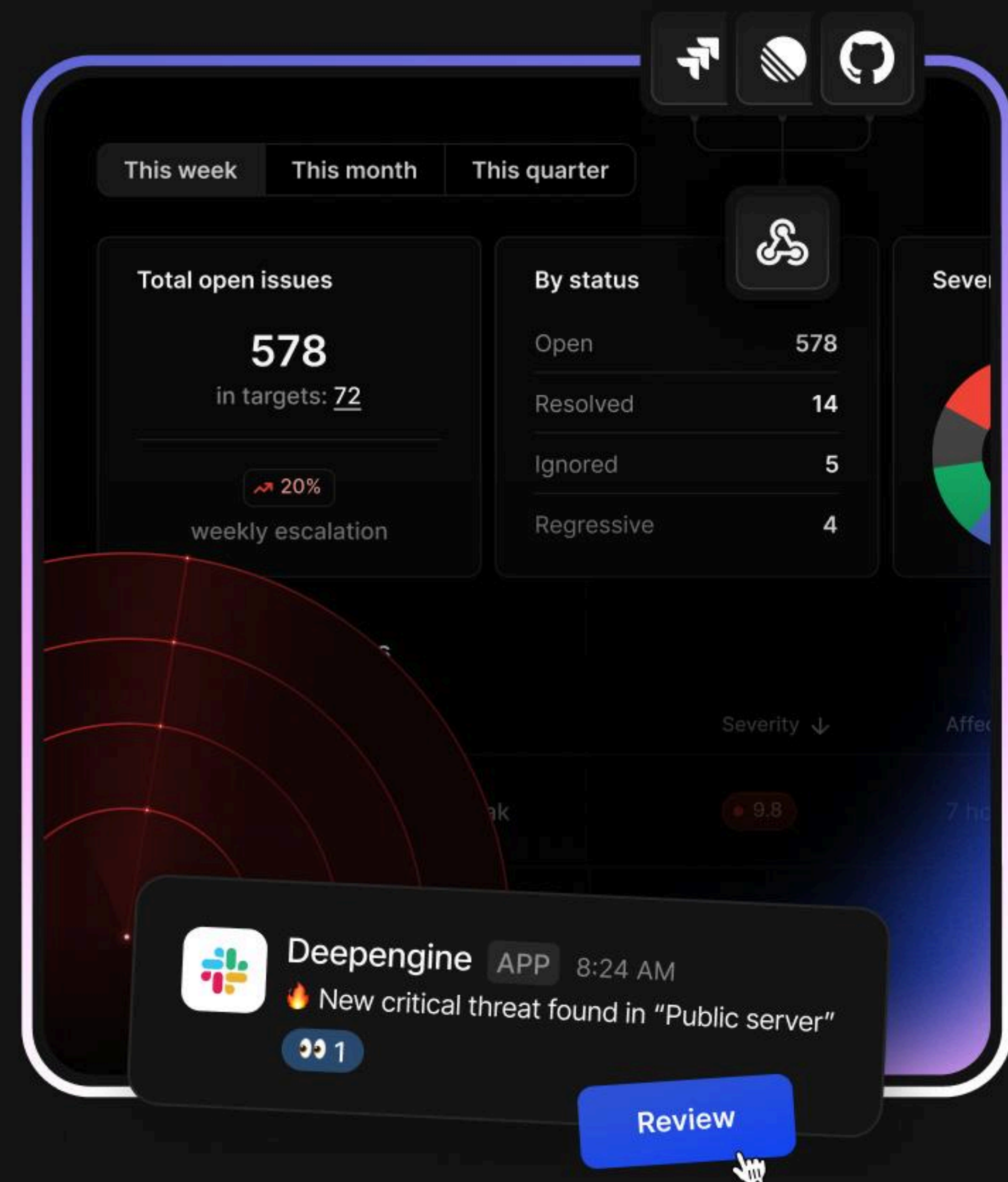
Broad visibility over security gaps

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.



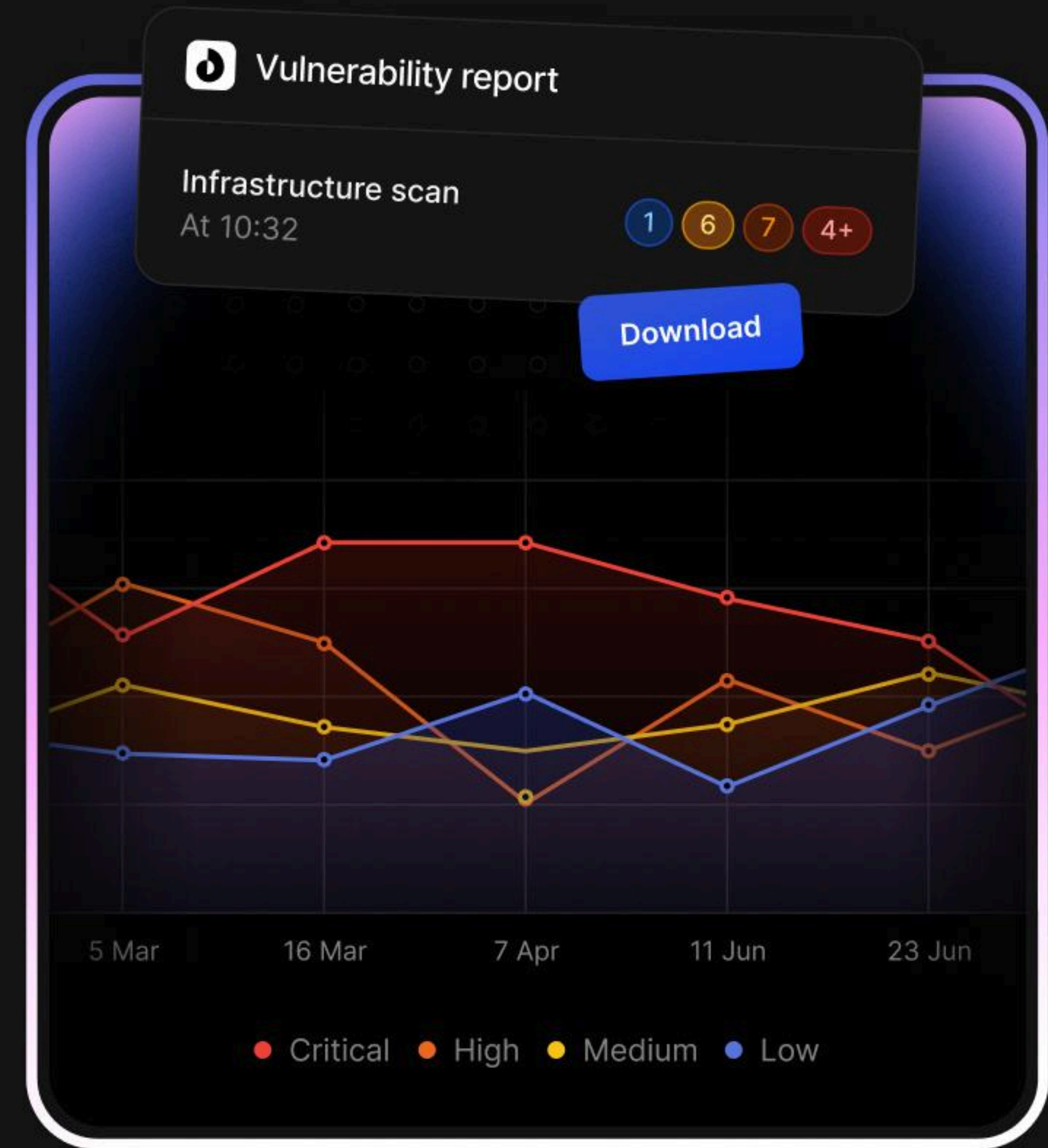
Speed up detection and response

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



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>