



Pentera Credential Exposure

Test for Cyber Identity Risks from Stolen or Leaked Credentials

Harden Your Credential And Identity Attack Surface

Automate the discovery and testing of compromised identities against your internal and external attack surfaces. Know the real-world impact of leaked credentials and prioritize remediation to eliminate identity threat exposure.

Key Product Pillars



Continuous Feeds

Receive real-time leaked credential data from threat intelligence feeds and see how adversaries could potentially use these credentials against your infrastructure and applications.



All Attack Surfaces

Test across all attack surfaces – internal, external, and cloud – to identify exploitable active credentials.



Multi-Format Testing

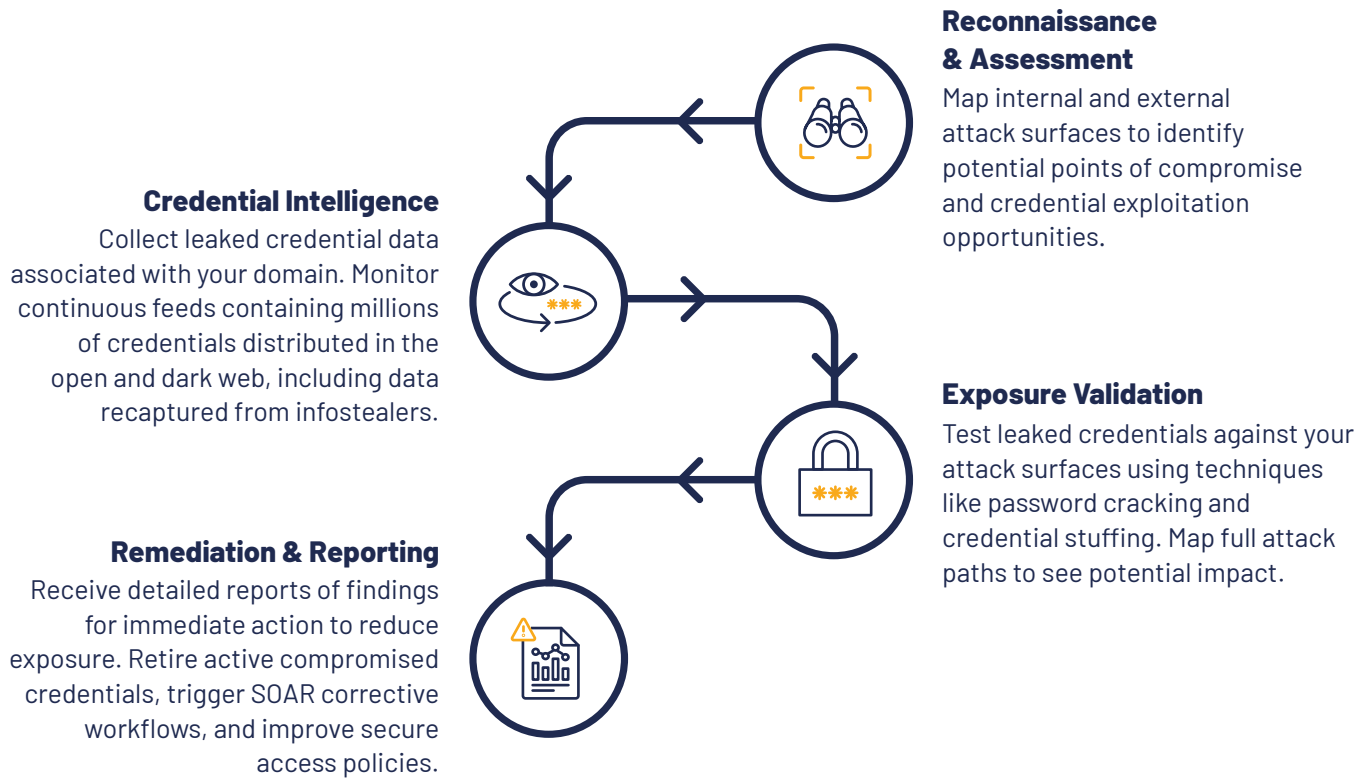
Validate leaked credentials in multiple formats, whether they are hashed, appear in clear text, in both full or partial user and login sets.



Targeted Remediation

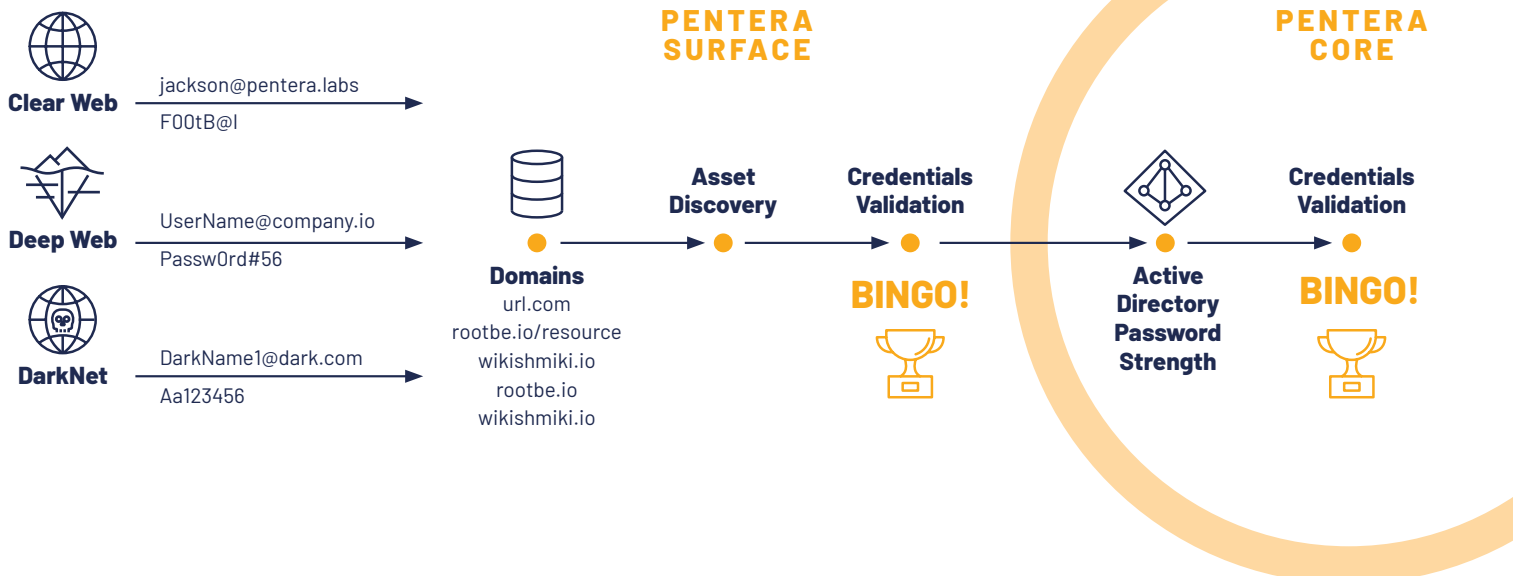
Retire compromised credentials, update password security policies, and trigger SOAR corrective action workflows.

How it works

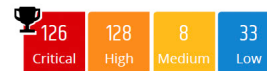


Threat Intelligence

(Based on leaked credentials data sources)



295 Achievements



Pentera accomplished 295 achievements in total. Every achievement represents a discrete successful action performed by Pentera.

(Listing 20 of 20 items).

Severity Details

9.8

Severity

(14) Validated leaked credentials

Attackers have their ways of obtaining or purchasing leaked credentials on the dark net. Leaked credentials can allow attackers to log onto hosts and gather information about users, and have the potential to allow attackers to take over hosts and escalate attacks.

dylan	administrator	nathan
oliver	asher	logan
william	levi	nextcloud
lucas	noah	james
ryan	henry	

8.1

Severity

(6) Validated leaked cleartext password

Adversaries may gather credentials that can be used during targeting. Account credentials gathered by adversaries may be those directly associated with the target victim organization or attempt to take advantage of the tendency for users to use the same passwords across personal and business accounts.

8.1

Severity

(19) Obtained user's cleartext password

An attacker might capture user's cleartext password and use it to login into hosts or services, which may lead to sensitive data theft or manipulation, and possibly to a complete take-over of the hosts or services.

7.6

Severity

(1) Replicated DC's credentials DB using DRSUAPI (DCSync)

An attacker with high privileges on the domain controller (DC) can impersonate a DC entity and replicate all the credentials without executing remote code.

7.5

Severity

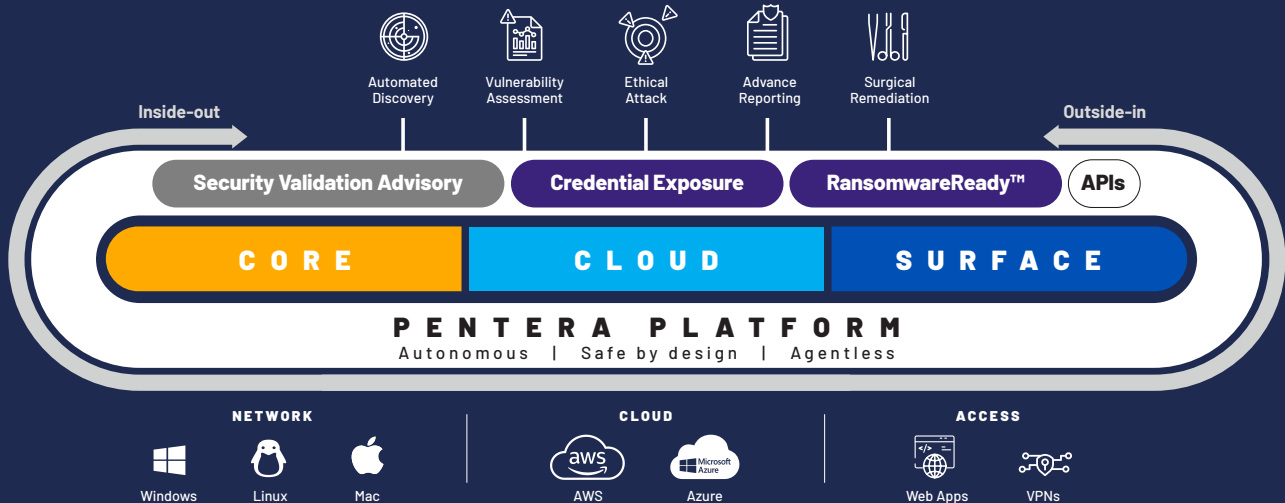
(86) Cracked user hash using GPU

An attacker might capture user password hashes during his attack, then try and crack them using various hash cracking tools. The purpose will be to gather as many user credentials as possible to escalate his attack, take-over hosts in the network and possibly learn the password policy of the organization.

Benefits

- + Reduce cyber risk exposure**
 Beat adversaries in identifying and remediating leaked and stolen credential exposures.
- + Reduce manual testing work**
 Eliminate the manual process of matching threat intelligence with active credentials.
- + Prioritize credential exposure based on true impact**
 Focus on the 1% of leaked credentials that are proven to be exploitable.

All your attack surfaces, **tested continuously** with the Pentera Platform



About Pentera

Pentera is the category leader for Automated Security Validation™, allowing every organization to test with ease the integrity of all cybersecurity layers, unfolding true, current security exposures at any moment, at any scale. Thousands of security professionals and service providers around the world use Pentera to guide remediation and close security gaps before they are exploited.