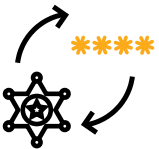


CREDENTIAL EXPOSURE MODULE



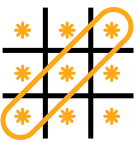
Use Pentera Credential Exposure (CE) Module to continuously monitor stolen and compromised credentials against your complete attack surface to preempt breaches.

Key Module Pillars



Continuous Feeds

Tap into several threat intelligence credential streams that correlate with your domain to assure ongoing validation against compromised credentials.



The Net Threat

Pentera correlates threat intelligence with existing privileges and security gaps, including services and the Active Directory, to identify toxic combinations of exploitable credentials and remove them.



Multi-Format Credentials

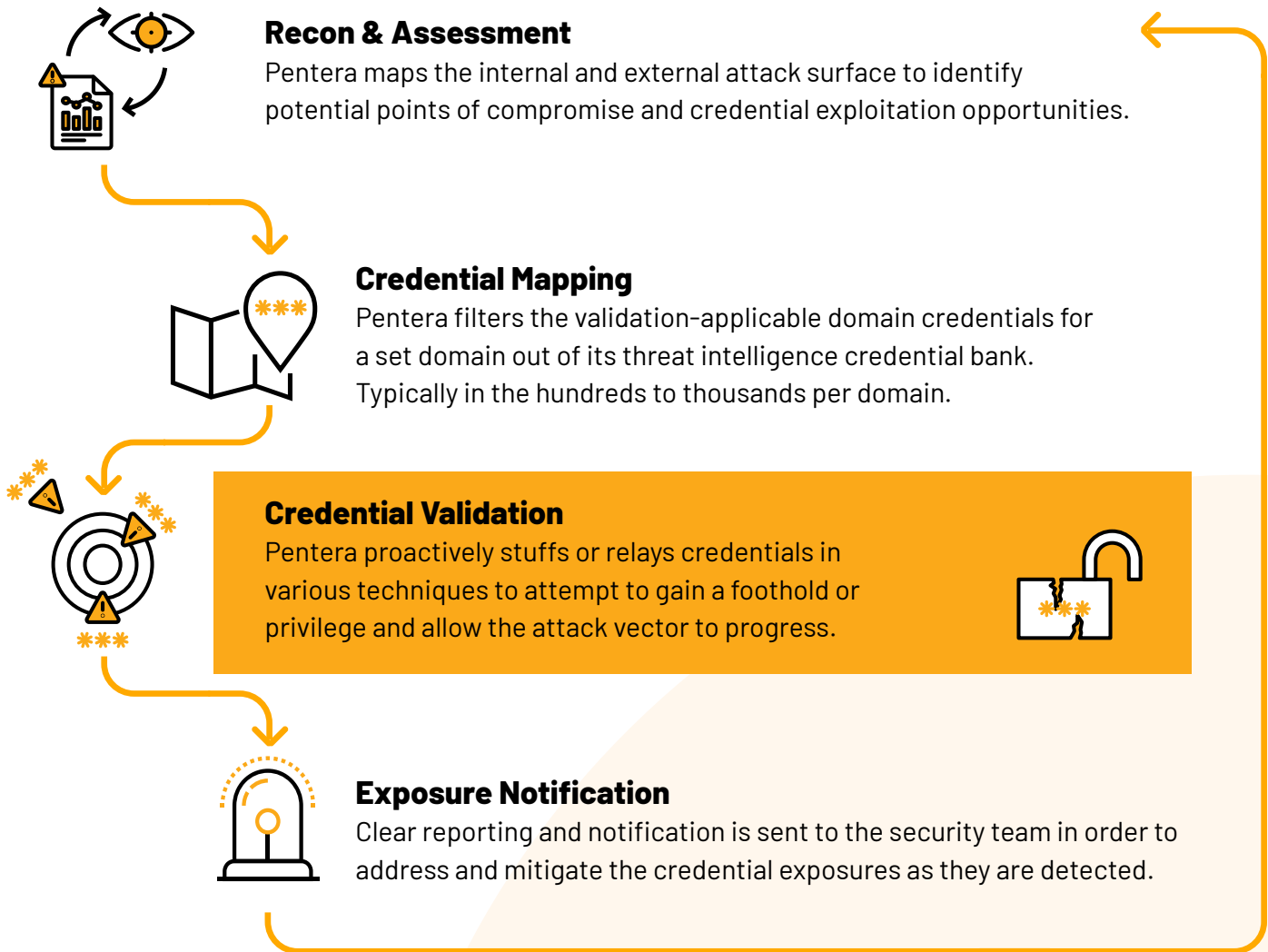
Pentera validates leaked credentials in multiple formats, whether they are hashed, appear in clear text, or show full or partial user and login sets.



All Attack Surface

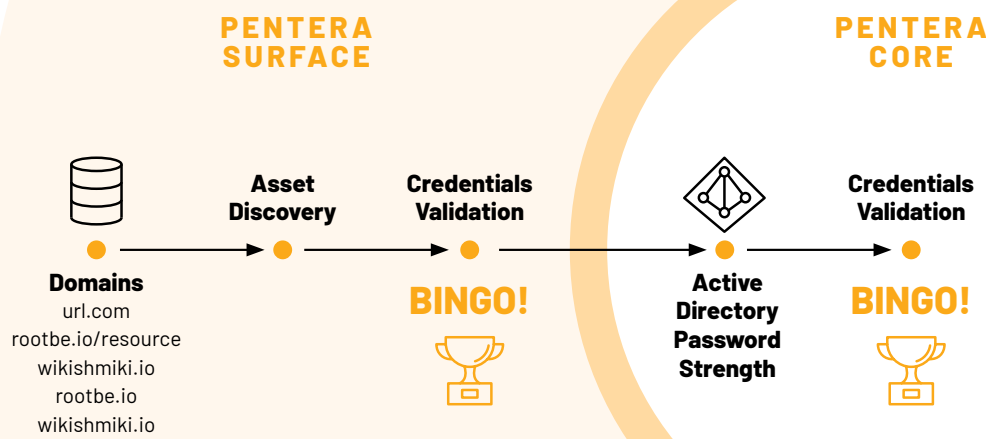
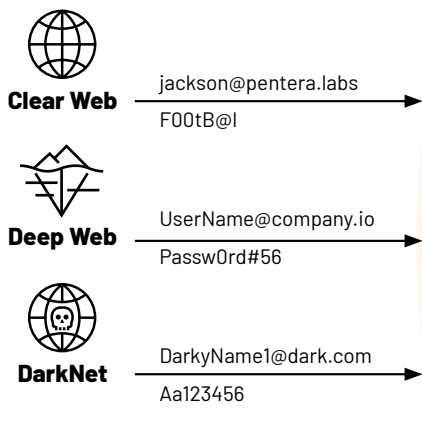
Credential Exposure validation works on the external attack surface, including web application interfaces, as well as cloud and perimeter assets.

How it works







Threat Intelligence

(Based on leaked credentials data sources)



9.0 Severity	Leaked username matches domain credentials 16 occurrences Adversaries may gather information about a victim's identity and use it to target their attacks. Personally identifiable information covers a wide range of data, including employee names, email addresses, etc. and often sensitive information such as credentials.															
	<table border="1"> <tr><td>odin</td><td>lok1</td><td>thor</td></tr> <tr><td>beowulf</td><td>sif</td><td>freya</td></tr> <tr><td>krbtgt</td><td>space2</td><td>guest</td></tr> <tr><td>longuser</td><td>special</td><td>lowpriv2</td></tr> <tr><td>maor</td><td>lowpriv</td><td>longuser2</td></tr> </table>	odin	lok1	thor	beowulf	sif	freya	krbtgt	space2	guest	longuser	special	lowpriv2	maor	lowpriv	longuser2
odin	lok1	thor														
beowulf	sif	freya														
krbtgt	space2	guest														
longuser	special	lowpriv2														
maor	lowpriv	longuser2														
9.2 Severity	(10) 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.															
8.1 Severity	(16) Validated leaked username 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	(10) Validated leaked password hash Adversaries may hunt for leaked account credentials directly associated with the targeted victim organization, but they can also take advantage of behavioral exposures due to people's tendency to reuse the same passwords across personal and business accounts.															
8.1 Severity	(8) 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.															

Benefits

- 
Accelerate Time to Mitigate Credential Risk
Beat adversaries in identifying and remediating leaked and stolen credential exposures
- 
Reduce Data Analyst and Manual Work
Completely remove the man-in-the-loop of correlating 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
- 
Eliminate Duplicity
With one platform to validate both internal and external attack surfaces you can unify your credential risk reduction efforts

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. For more information, visit [Pentera.io](https://www.pentera.io).