External Vulnerability Assessment

Proactive External Vulnerability Scanning Delivered by the Concierge Security Team

IT departments everywhere struggle with the complexity of identifying and managing security risks across external domains, IP addresses, web applications, and other services they access.

Left unchecked, these external services can be subject to threats caused by vulnerabilities, misconfigurations, and open ports, as well as account takeover from pervasive password reuse. To address this, IT departments should perform regular vulnerability scans of their external environment, and patch and remediate cyber risks according to severity and business impact.

Part of Arctic Wolf® Managed Risk and Managed Detection and Response solutions, external vulnerability assessment performs monthly scans of your external domains, IP addresses, web applications, and external services to reveal open ports, vulnerabilities, and misconfigurations to reduce the likelihood of an attack on your environment.

Security operations experts from the Concierge Security® Team (CST) work directly with you to help you quantify external risks, and build risk management plans based on severity and classification to prioritize remediation and harden your posture.

Use the Managed Risk Dashboard to access actionable insight about your external risks on demand through exportable reports shareable with your team. These reports are also provided during your regular security posture reviews with your CST.

***Figure 1:** Managed Risk Dashboard view of External Vulnerability Assessment risks*

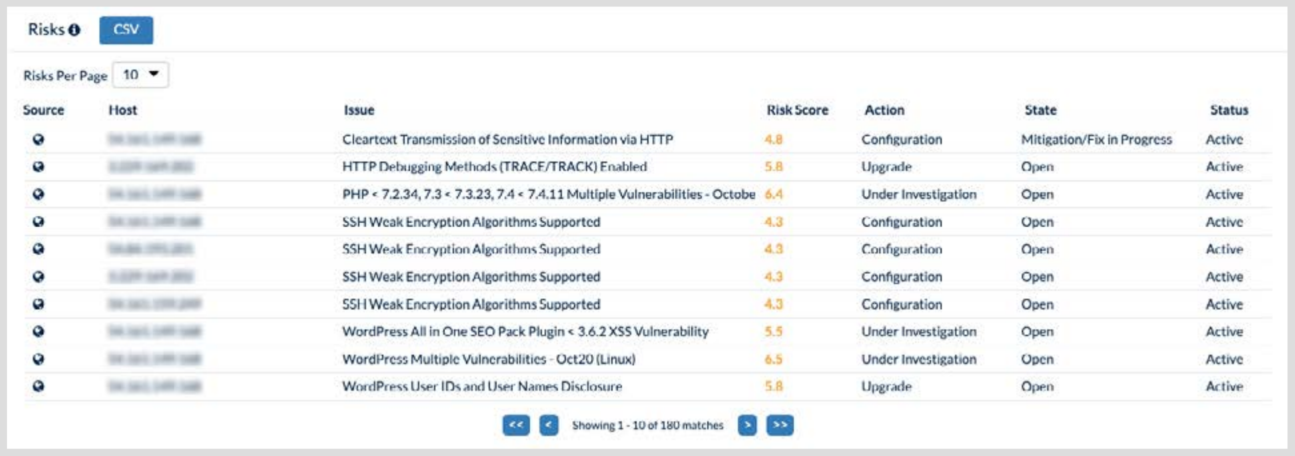
Concierge Security Team

The Concierge Security Team is your single point of contact for your Arctic Wolf solution. Your CST serves as your trusted security advisors and an extension of your internal team, and:

- Customizes the solution to your needs
- Proactively scans your external environment for cyber risks
- Performs monthly risk posture reviews
- Provides actionable remediation guidance
- Develops a customized risk management plan to prioritize remediation and measure progress

External Vulnerability Assessment Details

In addition to scanning your external environment for known vulnerabilities, external vulnerability assessment also regularly scans for common misconfigurations, as well as account takeover exposures that traditional vulnerability scanning tools cannot detect.



Risks ℹ CSV

Risks Per Page 10 ▾

Source	Host	Issue	Risk Score	Action	State	Status
🌐	[redacted]	Cleartext Transmission of Sensitive Information via HTTP	4.8	Configuration	Mitigation/Fix in Progress	Active
🌐	[redacted]	HTTP Debugging Methods (TRACE/TRACK) Enabled	5.8	Upgrade	Open	Active
🌐	[redacted]	PHP < 7.2.34, 7.3 < 7.3.23, 7.4 < 7.4.11 Multiple Vulnerabilities - Octobe	6.4	Under Investigation	Open	Active
🌐	[redacted]	SSH Weak Encryption Algorithms Supported	4.3	Configuration	Open	Active
🌐	[redacted]	SSH Weak Encryption Algorithms Supported	4.3	Configuration	Open	Active
🌐	[redacted]	SSH Weak Encryption Algorithms Supported	4.3	Configuration	Open	Active
🌐	[redacted]	SSH Weak Encryption Algorithms Supported	4.3	Configuration	Open	Active
🌐	[redacted]	WordPress All in One SEO Pack Plugin < 3.6.2 XSS Vulnerability	5.5	Under Investigation	Open	Active
🌐	[redacted]	WordPress Multiple Vulnerabilities - Oct20 (Linux)	6.5	Under Investigation	Open	Active
🌐	[redacted]	WordPress User IDs and User Names Disclosure	5.8	Upgrade	Open	Active

<< < Showing 1 - 10 of 180 matches > >>

Figure 2: *Sample— External vulnerability assessment output in Managed Risk Dashboard*

OWASP Top 10

In addition, external vulnerability assessement includes regular scans of your external webservers to detect cyber risks based on the Open Web Application Security Project (OWASP) Top 10. The Arctic Wolf Concierge Security Team helps share the results of these scans through executive summaries, external vulnerability reports, and charts and graphs displayed in the Managed Risk Dashboard. OWASP scanning covers the top 10 web application security risks across the following categories:

01 Injection
02 Broken Authentication
03 Sensitive Data Exposure
04 XML External Entities (XXE)
05 Broken Access Control
06 Security Misconfigurations
07 Cross-Site Scripting (XSS)
08 Insecure Deserialization
09 Using Components with Known Vulnerabilities
10 Insufficient Logging and Monitoring

ARCTIC WOLF
WordPress All in One SEO Pack Plugin < 3.6.2 XSS Vulnerability
Risks
CSV
Mitigated Risks
CSV

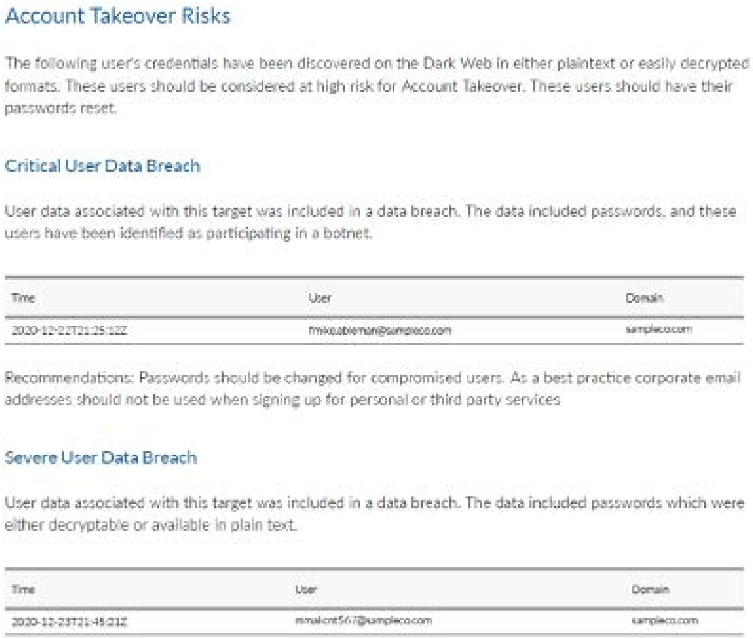
Figure 3: *Managed Risk Dashboard view of WordPress All in One SEO Pack Plugin XSS vulnerability*

| Public

Account Takeover Risks

The solution scans your external domains and IP addresses to report on any personally identifiable information (PII) discovered on the dark web in either plain text or easily decrypted formats. Insight is presented based on the following levels of exposure severity:

- **Critical**—data associated with this target was included in a data breach. These users were also identified as participating in a known botnet.
- **Severe**—data associated with this target was included in a data breach, and included passwords which were either decryptable or available in plain text.
- **Informational**—data associated with this target was included in a data breach, however, the data did not include passwords, or included passwords which were not decryptable.



Account Takeover Risks

The following user's credentials have been discovered on the Dark Web in either plaintext or easily decrypted formats. These users should be considered at high risk for Account Takeover. These users should have their passwords reset.

Critical User Data Breach

User data associated with this target was included in a data breach. The data included passwords, and these users have been identified as participating in a botnet.

Time	User	Domain
2020-12-22T21:25:12Z	fmike.ableman@sampleco.com	sampleco.com

Recommendations: Passwords should be changed for compromised users. As a best practice corporate email addresses should not be used when signing up for personal or third party services

Severe User Data Breach

User data associated with this target was included in a data breach. The data included passwords which were either decryptable or available in plain text.

Time	User	Domain
2020-12-23T21:45:21Z	mmalcnt567@sampleco.com	sampleco.com

***Figure 4:** Sample output of Account Takeover risk report*

Managed Risk Dashboard: Quantify Cyber Risk

A cloud-based dashboard provides actionable cyber risk insight by incorporating meaningful risk indicators from your business. It identifies the highest-priority issues and alerts you to emerging risks before they escalate into real problems. It empowers you to take efficient action to mitigate risk using these key features:

- Comprehensive risk profiling
- Informative user interface
- Notifications and alerts
- Advanced risk data analysis
- Actionable reporting
- API integrations
- Risk management plans

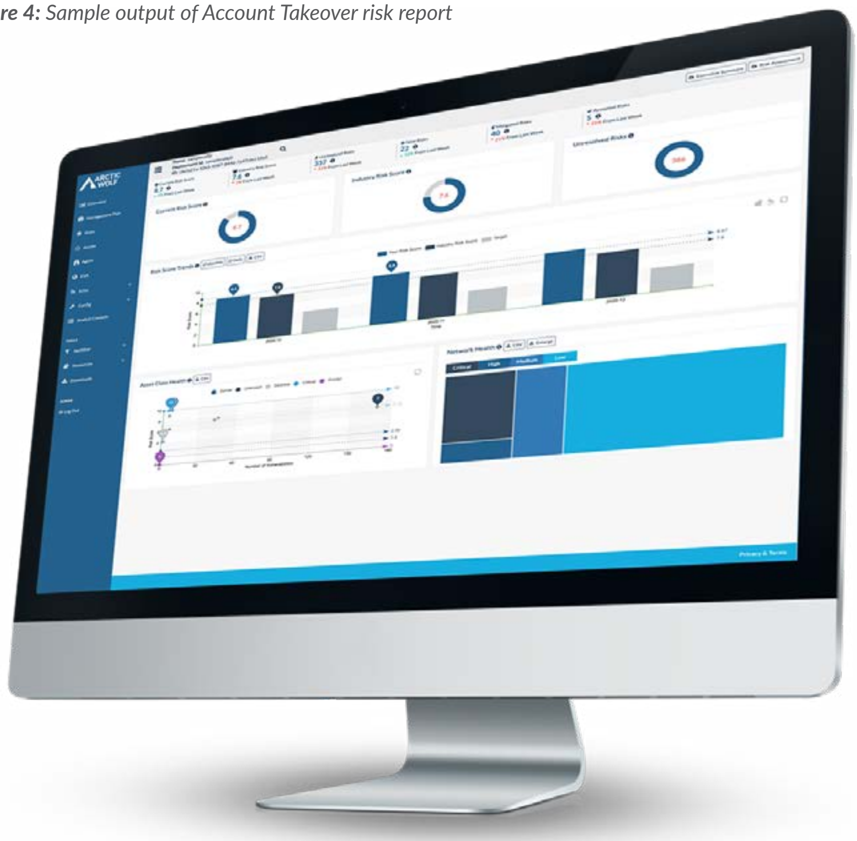


***Figure 5:** Risk posture overview in Managed Risk Dashboard*

ARCTIC WOLF

SOC2 Type II Certified

AICPA SOC

ISO 27001 CERTIFIED

CYBERGUARD COMPLIANCE

Contact Us

arcticwolf.com
1.888.272.8429
ask@arcticwolf.com