



# Arctic Wolf® Concierge Security®



## DATASHEET

## Harden Your Security Posture. Programmatically. Continuously.

The Arctic Wolf Concierge Security Team (CST) works with organizations to proactively harden their environments and mitigate cyber risks and amplify resilience.



### Focus

Arctic Wolf's Concierge Security is designed to identify and target specific best practices, risks, and/or threats that are of the highest interest for your organization. Working with your CST, you can focus on malware, business email compromise, or ransomware hardening or conducting attack surface configuration reviews, and much more.



### Mitigate

In partnership with your CST, establish a Security Focus and work on mitigating risk by hardening and configuring your environment via a sequence of Security Posture in-Depth Reviews (SPiDRs). Each SPiDR is designed to be actioned quickly and easily, enabling your organization to incrementally and successfully improve your security posture.



### Adapt

Working with your CST, your named team of security experts who understand your unique business context and security challenges, adapt your Security Focus in response to changes in the threat landscape, incidents, and your environment via Detours before returning to your primary Security Focus.

## Security Expertise On-Demand

Your Concierge Security Team act as strategic advisors to help harden your environment and proactively mitigate risk, generally available 9 a.m. to 5 p.m. in your time zone.

You always have 24x7 access to members of the Arctic Wolf Security Team by calling into the SOC (find the number at [arcticwolf.com](https://arcticwolf.com)) or sending an email to [security@arcticwolf.com](mailto:security@arcticwolf.com) to help answer any immediate questions you may have.

## Amplify the Value of Penetration Tests

Your CST will work with you to ensure you maximize the value of a penetration test (pen test) by proactively hardening your environment against common TTPs.

In response to pen tests, work with your CST to evaluate the results and determine mitigation strategies to maximize security efficacy.

## Custom Reports

Get support for custom reports from your CST. They will help guide you through the Arctic Wolf dashboards and tools, such as:

- Unified Portal Dashboards
- Data Explorer
- Data Explorer Lite

Additionally, they can support certain data requests.



## Key Features

### 01

#### **Programmatic Security Posture Hardening**

Programmatically improve your security posture and harden your environment with a security focus designed with your CST to target your most pressing security needs.

### 02

#### **Experts Who Know Your Context**

With Arctic Wolf not only do you get the foundational tools and technology you need to respond to threats, but you also get security experts who help you operationalize those tools and tackle ongoing security questions.

### 03

#### **Designed for Adoption and Implementation**

Easily consumed Security Posture in-Depth Reviews are designed to support your organization incrementally improve your security posture and harden your environment.

### 04

#### **Technology and Vendor Agnostic Approach**

Much like our open-XDR platform, our CST takes a vendor-, technology-, and attack-surface agnostic approach, as they offer support for firewall configuration, cloud-app configuration, policy best practices, and much, much more across tools and vendors.

## Set the Pace for Your Security Organization

The Arctic Wolf Concierge Security Team works with organizations to proactively harden their environments and mitigate cyber risks via the Security Focus program. With Arctic Wolf, you can select the engagement type that best suits the needs and pace of your organization's security team.

SILVER	GOLD	PLATINUM
Named Security Team 24x7x365 SOC Support Escalation Follow-up Reporting Support		
<b>Up to 4 Scheduled Security Touchpoints</b> focused on delivering core security activities to achieve core security outcomes.	<b>Up to 12 Scheduled Security Touchpoints</b> focused on delivering advanced activities to support your organization's outcomes.	<b>Up to 18 Scheduled Security Touchpoints</b> focused on tailoring the service to achieve your organization's outcomes.
<b>Silver SPiDR Library</b>  Core security activities to drive the necessary actions required to achieve basic security outcomes  <b>Examples:</b> <ul style="list-style-type: none"><li>• Security Best Practices</li><li>• CSPM Assessment</li><li>• Pentest Response</li><li>• Breach Recovery</li></ul>	<b>Gold SPiDR Library</b>  Advanced security activities for teams looking to take a more active approach to hardening their environment  <b>Examples:</b> <ul style="list-style-type: none"><li>• Threat &amp; Attack</li><li>• Compliance Assessment</li><li>• Ransomware Hardening</li><li>• BEC Hardening</li><li>+ Silver Library</li></ul>	<b>Platinum SPiDR Library</b>  Tailored experiences for technology migration and high-touch ongoing proactive improvement  <b>Examples:</b> <ul style="list-style-type: none"><li>• Anomalous Traffic Analysis</li><li>• Decoy</li><li>• AD Attack Path Assessment</li><li>• Industry Threat Mapping</li><li>• Data Exfil Hardening</li><li>+ Focused Tailoring</li><li>+ Silver and Gold Libraries</li></ul>



SOC2 Type II Certified

