



# Arctic Wolf® Managed Security Awareness®



## DATASHEET

### More Than Training

Organizations everywhere struggle to reduce the risk of cyber attacks – especially attacks targeting their employees.

Every day, highly motivated threat actors set their sights on employees who are unprepared to defend themselves. Instead of seeing employees as teachable, contributing members of a united front against cyber risk (and social engineers), employers often dismiss them as untrainable or as an unsolvable part of the risk equation.

Arctic Wolf® believes that you can prepare and equip your employees to reduce cyber risk when their awareness training program is built on microlearning and overseen by awareness experts. Microlearning ensures that employees are regularly informed about the latest threats and how to stop them at the point of attack. Awareness coaching provides expertise and guidance to security teams looking to mature their awareness program, sustain new, long-term employee behavior, and foster a culture of security within their organization.

### Effective Security Awareness

Traditional security tools are optimized for yearly training and “check the box” compliance. To be effective, security awareness must be continuous, positive, and friction-free for employees, which helps drive engagement and participation. Once employees are engaged, program effectiveness can be measured across individuals, teams, and the overall organization. Quantifiable results identify areas for improvement and demonstrate on-going value of the program to upper management.



#### Engage

Train and prepare employees to stop social engineering attacks, like phishing.

- Microlearning
- Fresh and relevant content
- Current threats



#### Measure

Identify employees who fall behind and which threat topics to reinforce.

- Employee performance
- Program effectiveness



#### Transform

Achieve a culture of security and strengthen your security posture.

- Employee confidence
- Security culture
- Cyber resilience

### Concierge Security® Team

Arctic Wolf Managed Security Awareness is delivered as a concierge service. Existing Arctic Wolf customers continue working with their CST. New customers are paired with a named CST who helps them kickoff and advance their awareness program with:

- Awareness coaching
- Program administration
- Attack trends
- Ongoing strategic security reviews
- 24x7 account takeover monitoring

### Security Awareness Training

Prepare employees to stop social engineering attacks with continuous training to recognize current threats, avoid scams, and understand the importance of reporting mistakes.

### Automated Phishing Tests

Measure and reinforce employee awareness with automated assessments and phishing simulations based on real-life attacks. Phishing simulations include an automatic follow-up lesson if employees click.

### 24x7 Account Takeover Monitoring

Minimize risk of account takeovers with immediate notification when employee credentials are found on the dark web.

### Compliance Training

Quickly add comprehensive compliance training to your security awareness program to address HIPAA, PCI, FERPA, Anti-Discrimination, and other important topics.



## The Arctic Wolf Difference

Arctic Wolf Managed Security Awareness is more than training. We don't rely only on training tools to change employee behavior. To be effective, security awareness training requires a holistic approach that includes teaching, testing, and tracking progress toward defined goals. The outcome of an effective awareness program results in fewer incidents related to phishing and human error, and builds stronger cyber resilience across your organization.



### Fully Managed Service

The security awareness program must not burden IT security teams with extra work. Arctic Wolf researches threat topics, designs, and schedules all content for lessons, quizzes, and topic reinforcement.



### Microlearning

Studies show people forget 80 percent of what they learn within one month unless reminded multiple times. Arctic Wolf regularly engages employees with short — three minutes or less — awareness lessons based on current threats targeting organizations.



### Account Takeover Monitoring

There are many ways to measure the success of your awareness program. A key outcome is to prevent threat actors from using employee credentials to access your network and data. By watching the dark web for employee credentials, IT security teams can determine when credentials are breached, change affected passwords, and improve employee behavior.



### Friction-free Learning

Employees are busy. We deliver awareness lessons via email, so employees have quick and convenient access to them. Employees don't have training account credentials, there are no passwords, and all tracking is performed behind the scenes — making employee participation easy.



**“Arctic Wolf Managed Security Awareness keeps our employees engaged and knowledgeable — and keeps our companies compliant — without disrupting our business operations.”**

— Jon Armstrong, Director of IT & Security, Fullsteam



## About Arctic Wolf®

Arctic Wolf is the global leader in security operations, delivering the first cloud-native security operations platform to end cyber risk. Powered by threat telemetry spanning endpoint, network, and cloud sources, the Arctic Wolf® Security Operations Cloud ingests and analyzes trillions of security events each week to enable critical outcomes for most security use cases. The Arctic Wolf® Platform delivers automated threat detection and response at scale and empowers organizations of any size to stand up world-class security operations with the push of a button.

For more information about Arctic Wolf, visit [arcticwolf.com](https://arcticwolf.com).

