Arctic Wolf® Managed Security Awareness® Content Strategy

Arctic Wolf Managed Security Awareness minimizes human risk with 100% relevant microlearning sessions that your employees will actually pay attention to. Being a security expert does not make a person a security awareness expert. Protecting networks and devices is different from preparing people. An effective security awareness program starts with relevant and timely threat-driven content, and this requires expertise in three areas: security, education, and production. Arctic Wolf has all three.

Security Experts

- Concierge Security® Team
- 24/7 Threat Detection
- Internal and External Threat Intelligence
- Incident Response Team

Education Experts

- Raise Awareness
- Change Behavior
- Foster Culture Change

Production Experts

- Hollywood Quality
- Engaging and Memorable
- Appeals to Viewers
- Rapid Delivery

Microlearning for Awareness and Behavior Change

Every day, highly motivated threat actors target organizations via their employees. With 90% of breaches now involving the human element, the current threat landscape has made traditional security awareness training obsolete.

Move beyond fragmented learning experiences and endless admin efforts with a comprehensive security awareness program. Built on microlearning by security, content-delivery, and production experts, Arctic Wolf Managed Security Awareness prioritizes engagement to drive behavior change and achieve the security culture needed to reduce human risk.

Microlearning Benefits

People forget 80% of what they learn in less than a month if they are not re-engaged. Contrast that with ongoing microlearning, which improves retention by 200%.

Learn more about microlearning and the keys to beating the forgetting curve in our **white paper.**

Relevant and Timely Threat-Driven Content

As cyber threats evolve and change, so does our content. We create new lessons every month, including rapid response training on emerging threats.

Defend Against Human Risk the Arctic Wolf Way

Arctic Wolf Managed Security Awareness closes the loop between identifying human risks and enhancing your security posture through education, awareness, training, and testing.

We've made it incredibly easy to deploy and maintain your security awareness program with a proven content delivery method, to ensure that you get the best results.

With our comprehensive approach, employees receive curated learning experiences following a simulated phishing 'click' to remediate the risk. This tailored learning method builds a security culture where employees can easily spot and avoid phishing attempts.

Monthly Cadence

Arctic Wolf's microlearning strategy includes multiple touchpoints per month to keep security top of mind, raise awareness, and change behavior.

Microlearning Sessions

- Videos
- Quizzes
- Interactive Lessons

Phishing Simulations

- Current Threat Vectors
- Integrated Follow-up
- Interactive Lessons

Seamlessly Integrates into Employee Routines

Cybersecurity isn't every employee's primary job function, but every employee needs to be an active participant in the security posture of their organization. Employees are expected to stay up to date on their security awareness training and Arctic Wolf makes it easy for them to get their jobs done while staying secure.

- Delivered to employee inboxes
- No username or password required

- Done in 3 minutes or less
- Monthly report cards with links to missed sessions

Always New, Always Relevant, Never Repeated

As cyber threats evolve and change, so does our content. We are always creating fresh and new content so you can be confident that your employees will be up to date on the latest threat topics.

You never need to schedule or curate lessons because we do that for you as part of a fully managed security awareness solution.

Previous lessons are also available to send to new employees, and topics are frequently reinforced across your organization with fresh lessons to ensure engagement.

> "Arctic Wolf creates the right email to send at the right time for phishing tests. They're very timely and they really help us highlight some strategies we need to put in place to help our employees."
>
> — *Director of IT, Eden Prairie Schools*

EPS
EDEN PRAIRIE SCHOOLS

Threat Topics Include

Recognizing and Defending Against Attacks

- Spear Phishing
- Vishing Calls
- Phishing Emails
- Smishing
- Social Engineering

Security Best Practices

- Remote Work Best Practices
- Cyber Hygiene Best Practices
- Preventing Account Takeover
- Defending Against Credential Theft and Brute Force Attacks
- Identifying Spoofed Websites
- Recognizing Insider Threats

Physical Security

- Dangers of Device Sharing
- Dangers of Public Wi-Fi
- Dangers of Lost or Stolen Devices
- Threat of Shoulder Surfing
- Threat of Dumpster Diving
- Threat of Tailgating

Specialized Content for Industries and Roles

Arctic Wolf Managed Security Awareness delivers security awareness education aligned with the way adults learn and embrace new concepts. Managed Security Awareness Plus is for organizations that require industry- and role-specific lessons for their employees.

Content	Managed Security Awareness	Managed Security Awareness Plus
Fully managed content creation and delivery	✔ Yes	✔ Yes
Three minutes or less	✔ Yes	✔ Yes
Always fresh, never repeated	✔ Yes	✔ Yes
Delivered twice a month	✔ Yes	✔ Yes
Based on recent attacks	✔ Yes	✔ Yes
Designed by security and education experts	✔ Yes	✔ Yes
Covers cyber social engineering attacks	✔ Yes	✔ Yes
Covers physical social engineering attacks	✔ Yes	✔ Yes
Industry-specific content	✖ No	✔ Yes
Role-based content	✖ No	✔ Yes
Compliance content pack	Add-on	Add-on

Industry Content Tracks

Managed Security Awareness customers are provided a content track designed to engage employees multiple times per month with fresh and relevant topics. Organizations in finance, government, education, healthcare, and legal verticals may choose to replace the standard track with any industry track currently available.

Role-Based Content

Role-based lessons are specifically designed to prepare highly targeted roles within organizations. For example, it is important to prepare call center employees to recognize threat actors pretending to be legitimate customers over the phone. As always, lessons are developed in-house and based on recent social engineering attacks and other current events. Role-based content is available to Managed Security Awareness Plus customers for these roles: customer-facing employees (e.g., call center), finance teams, IT, human resources, and executive team members.

Compliance Training

Compliance training content is an add-on for all Managed Security Awareness customers. Compliance training is delivered through the same platform, alongside your security awareness program. Arctic Wolf offers 16 compliance training courses for PCI, HIPAA, FERPA, and other important topics.

01 *Finance Focus*

- PCI for Users, IT, and Managers

02 *Healthcare Focus*

- HIPAA Compliance Courses (Essentials, Privacy Rule, and Security Rule)
- OSHA: Airborne and Bloodborne Pathogens

03 *Higher Education Focus*

- Title IX
- FERPA

04 *HR Focus*

- Anti-Discrimination
- Sexual Harassment Prevention (General and CA State Specific)
- Affirmative Action and Equal Employment
- FMLA (Family Medical Leave Act)

05 *Security Focus*

- Security Essentials
- General Data Protection Regulation (GDPR)

About Arctic Wolf

Arctic Wolf® is a global leader in security operations, delivering the first cloud-native security operations platform to end cyber risk. Powered by threat telemetry spanning endpoint, network, identity, and cloud sources, the Arctic Wolf Aurora Platform ingests and analyzes trillions of security events each week to enable critical outcomes for most security use cases. By delivering automated threat protection, response, and remediation capabilities, Arctic Wolf delivers world-class security operations with the push of a button so customers can defend their greatest assets at the speed of data.

For more information about Arctic Wolf, visit **arcticwolf.com**.

SOC2 Type II Certified