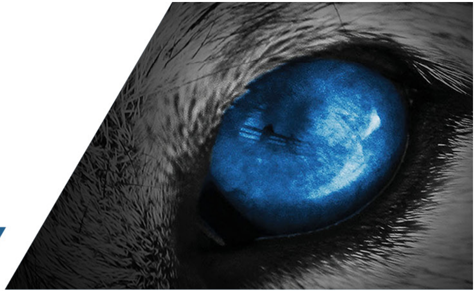
ARCTIC WOLF



PERSONAL | PREDICTABLE | PROTECTION

City of Burleson – at a glance

- Employees – 480
- Servers – 60
- o365 - 580
- Sensors- 2x – 1000 Series
- Log retention – 1 year
- Required Solutions
  - Arctic Wolf® Managed Detection and Response
  - Arctic Wolf® Managed Risk

Arctic Wolf capabilities :

- Real-time security event analysis
- Mature SOC processes with <30 day time to value
- Cyber security incident response
- Vulnerability scans and analysis
- Threat intelligence analysis
- Malware analysis
- Forensic analysis
- Security training
- Log management and storage

City of Burleson Background and Project Objectives

City of Burleson is looking for a Security Partner to add a greater degree of Cybersecurity expertise to enable more proactive hunting of known and unknown cybersecurity threats.

- Provide a fast track for time to value for improving City of Burleson's security posture – Fully funtional SOC in 30days
- Ability to work with existing security investments- No rip and replace
- Broad vendor agnostic visibility across all Network, Cloud and Endpoints- 100% protection for entire attack surface. No Vendor Lockin for the future
- Dedicated team to become the central point of contact for all alerts, and to limit the City of Burleson team members in wasted time chasing down alerts and false positives – Time back to work on strategic initiatives for the City and 99.9% true postives delivered
- Provide support for compliance and reporting including audit support and complete SOC services
- Centralization of security logs for correlation and analysis
- 24x7 coverage looking for vulnerabilities, system misconfigurations, and account takeover exposure on the dark web
- Proactively detect and respond to critical security incidents within minutes, (vs. 206 day industry average) to prevent the spread of threats.
- Development of customized Remediation Playbook based on incident
- Unlimited Log Sources and Capacity
- $0 IR Retainer included with 1hour SLA if ever needed
- 500k Security Ops Warranty included for additional financial assurance

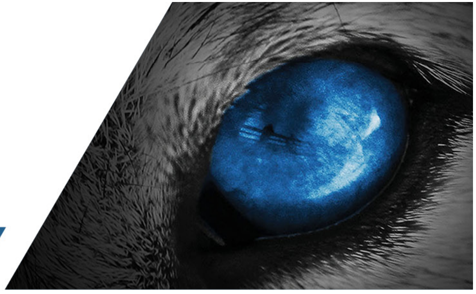
Arctic Wolf – Not just an MSP:

Managed Detection and Response (MDR) is managed security service for enterprises that is focused solely on threat detection and quick incident response. MDR includes hardware, software, operations, maintenance, and resources to secure your organization efficiently.

Arctic Wolf Delivers:

- Three Concierge Security Engineers who understand your IT & business
- SOC-as-a-Service operational in 60 minutes
- Improved security posture
- Protect breaches through early detection and quick response with a 5 minute internal, 30 minute to customer SLA on all critical incidents
- Threat and vulnerability management
- Security compliance monitoring
- $0 IR Retainer

ARCTIC WOLF



PERSONAL | PREDICTABLE | PROTECTION

Arctic Wolf® Security Operations

The Importance of Security Operations Solutions

Today's leading organizations need to protect themselves against the most advanced threats, but lack the internal resources to address the high costs, complexity, and additional personnel that's required to build an impactful security operations center.

Organizations face fundamental security challenges

Too Much Noise

Alert fatigue, vendor fatigue, compliance, and regulation fatigue—the journey never ends

Security Skill Shortage

Recruiting and retaining cybersecurity talent is hard, sometimes impossible

Cost of Response Time

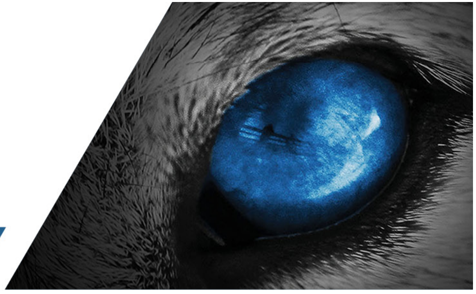
The longer it takes to respond to an incident, the more expensive it is to remediate

Arctic Wolf redefines the economics of security – through Security Operations Services

Arctic Wolf Networks is redefining the economics of security through an affordable, turnkey SOC-as-a-Service solution that deploys in less than 60 minutes. With designated Concierge Security Engineers™, a proprietary cloud-based SIEM, 24x7 monitoring, incident response, vulnerability scans, and a tailored escalation & ticketing process, AWN cSOC provides an end-to-end security monitoring at a fraction of a cost of a security engineer.

Using the cloud-native Arctic Wolf Platform, we help organizations end cyber risk by providing security operations as a concierge service. Highly trained Concierge Security experts work as an extension of your team to provide 24x7 monitoring, detection, and response, as well as ongoing risk management to proactively protect systems and data while continually strengthening your security posture.

ARCTIC WOLF



PERSONAL | PREDICTABLE | PROTECTION

Arctic Wolf Security Operations Warranty

Mitigate Cyber Incident Costs With Financial Assistance Benefits

Arctic Wolf's mission to end cyber risk focuses on defense-in-depth protection for every layer of cybersecurity. Arctic Wolf security operations solutions, including Arctic Wolf Managed Security Awareness®, Managed Risk, Managed Detection and Response, and Managed Cloud Monitoring, function in concert to reduce the likelihood of cyber incidents and mitigate their impact, minimizing cyber risk to organizations.

However, no single cybersecurity tool can stop attacks perfectly every time. Cybersecurity, IT, and risk management leaders need a plan to manage the outcomes of inevitable cyberattacks their businesses will face.

Security Warranty Is Here

Arctic Wolf Security Warranty is the answer. This unique customer benefit offers a key financial layer to cybersecurity.

Our security warranty is an exclusive, no-cost benefit, offered by Arctic Wolf in partnership with a third-party that supports the program delivery and underwriting. It is available to customers with a robust security partnership with Arctic Wolf. In the event of a cyberattack, Arctic Wolf Security Warranty provides up to $1,000,000 in financial assistance for recovery activities, legal and regulatory expenses, and other associated business costs.

Eligibility Requirements

Total Benefit Amount	$1,000,000	$500,000
Qualifying Solutions	MDR, Managed Risk, and Managed Security Awareness (3 years upfront)	MDR, plus one of either Managed Risk or Managed Security Awareness
Ransomware and BEC	$200,000	$100,000
Compliance	$200,000	$100,000
Cyber Legal Liability	$500,000	$250,000
Business Income Loss	$100,000	$50,000

Managed Detection and Response

Built on the industry's only cloud-native platform to deliver security operations as a concierge service, the Arctic Wolf®Managed Detection and Response (MDR) solution eliminates alert fatigue and false positives to promote a faster response, with detection and response capabilities tailored to the specific needs of your organization.

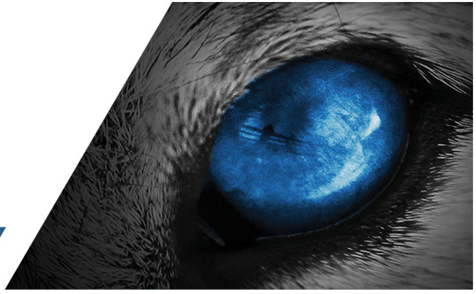
Managed Risk

Arctic Wolf® Managed Risk enables you to continuously scan your networks, endpoints, and cloud environments to quantify digital risks, discover risks beyond simple vulnerabilities, benchmark the current state of your environment, and implement risk management processes that harden your security posture over time.

Managed Security Awareness

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.

ARCTIC WOLF



PERSONAL | PREDICTABLE | PROTECTION

Arctic Wolf at a Glance

- Headquarters – Eden Prarie, MN
- Employees – 1750+
- Market Leader in Security Operations
- Solutions
  - Arctic Wolf® Managed Detection and Response
  - Arctic Wolf® Managed Risk
  - Arctic Wolf® Managed Security Awareness

Solution Differentiators

- Concierge Security Team (CST) – Trained, credentialed Security Experts assigned to your individual account focused on delivering actionable outcomes
- **Broad Visibility** – Eliminate blind spots with complete visibility across endpoints, network and cloud
- **24X7 Coverage -** eyes on glass coverage of your environment by trained, credentialed Security Experts
- **Strategic Guidance** – CST expertise combined with knowledge of your environment consistently increases security posture
- **Continuous Improvement** Regular posture reviews track progress to ensure consistent improvement
- **Pricing** – Simple, predictable pricing based on consistent inputs like users, servers and network egress points

Summary of Services to Support Objectives

Arctic Wolf's cloud-based Security Operations Center as a Service provides a platform to ingest, correlate and action data from cloud, network and endpoint. This is accomplished through the assignment of two named, certified security experts (the Concierge Security Team) to assist in both mitigating the above vulnerabilities and taking a proactive focus on continually improving the overall security posture.

Accelerate Time to Value with Streamlined Service Installation

The AWN Concierge Onboarding team includes a dedicated project manager and technical resource who manages all aspects of your onboarding experience, and:

- Identifies key assets and log sources, including cloud applications
- Validates log sources and tests basic telemetry
- Gathers external vulnerability scanning requirements to assess exposed attack surfaces
- Fine-tunes the service to improve signal-to-noise ratio
- Identifies reporting and compliance requirements that meet your IT and security needs

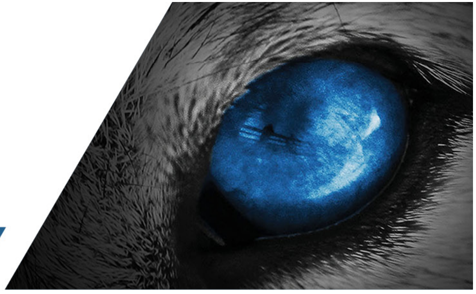
Pricing Summary

Managed Detection and Response & Managed Risk
480 Users, 60 Servers, 580 o365 Users, 1 year of Log Retention, 2 x Network Sensors (1000 series w/10g Bypass)

Product		Extended Price
Managed Detection & Response	Service	$65,487.50
Managed Risk	Service	$21,222.00
Managed Awareness	Service	Not Included
MDR One Time Costs	Onboarding	$2,879.70
Managed Risk One time Costs = Shipping	Onboarding	$1,194.70
Total One Year Cost	Service + Onboarding)	**$90,663.90**
Total Second Year Cost	Renewal at 5% (reduced from 8%)	**$90,663.90**

*Official quote is provided by Authorzied Partner SHI

ARCTIC WOLF



PERSONAL | PREDICTABLE | PROTECTION

Arctic Wolf Managed Detection and Response includes: $65,487.50 + One time $2,879.70

- Fully managed and hosted SIEM
- 3-person Concierge Security Team (CST) to work as extension of your IT team
- 24x7x365 monitoring
- Compliance & Audit support (unlimited reporting, time with CST)
- Managed Containment
- Managed IDS collecting of all network flow data
- Weekly, Monthly and Quarterly reporting
- Ad hoc reports generated at your request
- Unlimited Log Volume and coverage of network, endpoint, & cloud
- 1- year Log Retention
- Arctic Wolf Endpoint Agent
- Account Takeover (Dark Web) Scanning & Detection
- Monthly/Quarterly Deep Dive Security Maturity Reviews with your CST
- External Vulnerability Scan – Run Monthly
- Unlimited Custom Rules – We tailor the service to you

Arctic Wolf Managed Risk includes: $21,222 + One time $1,194.70

External Vulnerability Assessment

- Asset discovery based on root domains & IP addresses
- Automatic IP, domain, sub-domain detection
- Dynamic perimeter model
- External vulnerability scanning
- Dark Web Data Sources

Internal Vulnerability Assessment

- Dynamic asset discovery and credential scanning
- Asset inventory, categorization, notes, and tags
- Asset mapping – IP, DNS, Netbios history
- Continuous internal vulnerability scanning
- Scanning schedules with blacklisting capability

Account Takeover Scanning

- Dark Web scanning for compromised credentials
- 19% of data breaches in 2019 were caused by compromised credentials (IBM)
- 70% of AW customers had PII exposure on dark web, 6% had passwords exposed online

Host-based Vulnerability Assessment

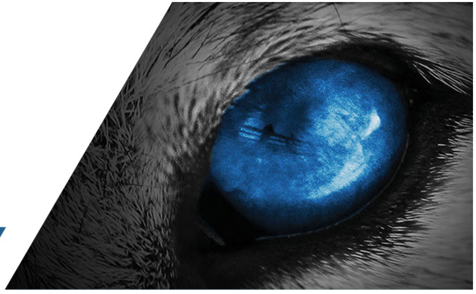
- Arctic Wolf Agent
- Proactive risk monitoring
- Audit reporting
- Configuration Baselines

3-Person Concierge Security Team (CST)

- Named security team
- Monthly & Quarterly Security Deep Dive reviews with CST
- Critical Vulnerability Alerting 24x7
- Strategic Security Advice, Answers to Security Questions

Arctic Wolf Analytics and Reporting

- Risk roll-up of internal + external vulnerabilities
- Risk prioritization and workflow integration
- Integrated threat feeds, latest exploits
- Executive reporting snapshots
- Custom reporting for analytics or alerts



DIY vs SOC-as-a-Service TCO/ROI Estimate

DIY IN-HOUSE SOC (Not a 24x7x365 shop**)**

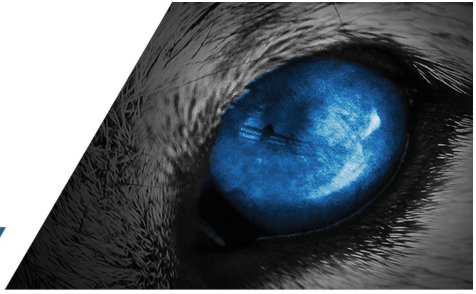
Average SOC Costs Across Major Vendors	Notes	Annual Cost
SIEM Costs (software, compute, storage)	Range $100k – $200k	$150,000
Vulnerability Management Tooling Costs	Range $25,000 - $50,000	$40,000
Opportunity Cost of Install, Training, Compliance Fulfillment and Continuous Maintenance	Range $5k - $12k	$10,000
IT Security Resource Annual Salary	Using $150,000k x 1.2 Benefits Multiplier	$180,000
IT Time spent on security related incidents	From Forrester Study	40%
Opportunity Cost of IT (all personnel) Time spent on security related incidents (4 at average salary of $120,000)	$480,000 x 0.4	$192,000
DIY SOC Cost Estimate		**$562,000**

ARCTIC WOLF SOC-AS-A-SERVICE (24x7x365 Security Operations)

All-Inclusive Arctic Wolf Detection, Response, and Risk		$105,492
Opportunity Cost of Install	AW Onboarding cost	$Included
SIEM + Vulnerability Management Tools	Included	$0
Opportunity Cost of Training, Compliance Assistance and Continuous Maintenance	Included	$0
Arctic Wolf Security Staff Costs	Included	$0
Threat Intelligence Costs	Included	$0
Total Cost: Arctic Wolf Scenario		**$105,492**

ARCTIC WOLF SOC-AS-A-SERVICE vs DIY over 1 Year

Cost Savings of Arctic Wolf over DIY in 1 Year	**$456,508**
Time to value >30 Days- vs- 10-12 Months deployment of SIEM	**Priceless**



PERSONAL | PREDICTABLE | PROTECTION

Arctic Wolf®– Cyber Insurance: Key Control Alignment

The Importance of Security Operations Solutions

Cyber insurance underwriters look for several key controls when issuing coverage. If an organization does not meet all controls, they can face non-renewal, limits on coverage triggered by a ransomware event, and/or a significant increase in premiums.

The Arctic Wolf Security Operations services (Managed Detection Response, Managed Risk, and Managed Awareness Training) map directly to the key controls that are being reviewed by many cyber insurance carriers.

Key Controls	Arctic Wolf Delivers
MFA-Controlled Access	- Authentication monitoring and alerting - Secure Posture Reviews/Recommendations around MFA/Auth activities
Secured & Tested Backups	- Secure Posture Reviews/Recommendations around general backup policies
Managed Vulnerabilities	- Managed Risk (External IP Vulnerability scanning and prioritization, External OWASP Top 10 scanning and prioritization, Internal Network Testing, Host Based Vulnerability scanning and prioritization)
Patched Systems & Applications	- Managed Risk validates patching is taking place and vulnerabilities are being mitigated.
Protected Privileged Accounts	- Monitor Directory for privileged groups, access changes, and potential compromised credentials as well as user/entity behavior activity (UEBA).
Protected Network	- Integration and monitoring of existing perimeter/prevention tools. - Additional network threat intelligence and monitoring with our sensor, including the aggregation of flow records
Secured Endpoints	- Integration with endpoint security solutions. - Additional endpoint detection capabilities with AW Agent. - Host based isolation with AW Agent.
Logged & Monitored Network	- Broad, vendor agnostic visibility into all network, cloud, and on-prem systems and services. This is the core of the AW MDR service.
Phishing-Aware Workforce	- AW Managed Awareness Training equips and educates users on cyber threats and how to neutralize them and protect the organization.
Hardened Device Configuration	- MR (Secure Config Benchmark reporting and CSPM) - Secure Posture Reviews for areas of weakness - Our proactive emerging threat notifications
Prepared Incident Response	- Coordinate with customer’s in-house and/or 3rd party IR team - Provide deep-dive findings of data captured through the AWN Platform - Provide an Incident Report of findings from the AWN - Provide recommendations, documentation, and best practices for response