AWN CyberSOC™

Security Operations Center-as-a-Service

Benefits of AWN CyberSOC™

- Dedicated Concierge Security Engineer™ who understands your IT and business operations
- Managed detection and response protects against breaches
- Service is operational in 60 minutes
- Proactive and improved security posture
- Threat and vulnerability management
- Predictable OpEx through fixed monthly subscription
- Security compliance monitoring

AWN CyberSOC™ delivers end-to-end security for mid-sized companies. The affordable outsourced security service focuses on early detection of threats and quick incident response known as managed detection and response (MDR). AWN CyberSOC™ extends the capabilities of your IT team without requiring investment in additional hardware, software or staff.

Rapid deployment: SOC-as-a-service in 60 minutes

AWN CyberSOC™ is a distributed, cloud-based security operations center (SOC) available as an affordable monthly subscription service. The deployment is simple and starts with an AWN sensor being installed in your network. The sensor immediately starts gathering machine data and sending it to the Arctic Wolf SOC, where it is analyzed in real time. Threat monitoring begins as soon as the pre-configured sensor is racked in your network.

SOC protects your IT and business

AWN CyberSOC™ combines human and machine intelligence to analyze millions of events in real-time for 24x7 threat detection. The machine learning, threat intelligence feeds and big data security analytics tools collect and correlate security events from all infrastructure, security devices and applications before delivering events to your designated Arctic Wolf Concierge Security Engineer™ (CSE) to review and respond to in seconds. If a threat is detected, the CSE notifies you with details, forensic analysis and recommended remediation for incident response. This not only helps protect your organization from a data breach, but also saves valuable time for your IT and security teams.

AWN Portal gives customers visibility into the security of their networks, applications and data. Actionable security intelligence is delivered by the service that is proactively monitored and managed by the customer's dedicated AWN Concierge Security Engineer™.

Features of AWN CyberSOC™

- Threat intelligence analysis
- Malware analysis
- Forensic analysis
- Security training
- Log management and storage

Security experts to augment your IT team

AWN CyberSOC™ is backed by a team of 25 security experts. We analyze over 4 billion events per day for hundreds of customers. You get a dedicated security engineer who is working in a large 24x7 SOC with the whole team to monitor your network and analyze your security events so threats are detected in real time.

Security monitoring of compliance controls

Compliance and security have more than half of their policies in common. Compliance is usually a byproduct of a good security practice. Typical compliance policies are about data privacy, log collection, log storage, forensic capability, encryption, firewall zoning, electronic signatures, network mapping and others. AWN CyberSOC™ covers the majority of compliance policies, so PCI and HIPAA can easily be built based on these principles.

Visibility into your security posture

All companies invest in security technologies, but it's difficult to get a snapshot of your security posture based on your prevention tools. You need a SOC that integrates all of your prevention technologies to tell you how you're doing from a cybersecurity perspective. AWN CyberSOC™ provides this through the customer portal, weekly check-ins with your CSE, and executive summary reports. Some of our customers take these reports and present them to their board or C-level executives on a regular basis.

Managed detection and response (MDR)

MDR is focused on threat detection and incident response services (as opposed to traditional device management and basic alerting in managed security services). MDR removes the burden of figuring out the best method or technologies to use for threat detection and response capability. AWN CyberSOC™ delivers security operations center capabilities focused solely on threat detection and cybersecurity incident response. AWN CyberSOC™ has all the necessary human and machine intelligence needed to collect and analyze your machine data in real time, detect threats and send you recommended remediation actions.

Advanced persistent threats (APT)

A SOC is a combination of people, process and technology to defend against APTs. AWN CyberSOC™ combines best-of-breed technologies to analyze millions of security events in real-time through different tools. Strong algorithms, correlation rules, machine learning, real-time threat intelligence and analytics tools help detect new threats exploiting zero-day vulnerabilities. AWN CyberSOC™ has machine learning capabilities that share anonymized threat intelligence between teams to proactively hunt for threats known or detected by other teams.

Improved security posture

AWN CyberSOC™ provides continuous monitoring of your security and critical infrastructure devices for threat detection. We also monitor your user behavior, manage the security training, and scan your network for external vulnerabilities regularly. This ensures good security practices and overall good hygiene for your network and IT, resulting in an improved security posture.

AWN CyberSOC™ for end-to-end security

AWN CyberSOC™ is the industry's easiest to deploy SOC service and can be up and running in less than one hour. It is based on an affordable monthly subscription model that lets you use only a fraction of your security budget to have a full SOC capability. It augments your existing prevention/network/security tools and does not require any changed or additional hardware, software or security experts. It is anchored through a dedicated security engineer who acts as an extension of your IT team and conducts both real-time and hunting tasks to protect you against known and future threats. AWN CyberSOC™ addresses the complete security value chain of threat detection and response.

ARCTIC WOLF Layer 7 Data Solutions

Contact us
arcticwolf.com
1.888.272.8429
ask@arcticwolf.com