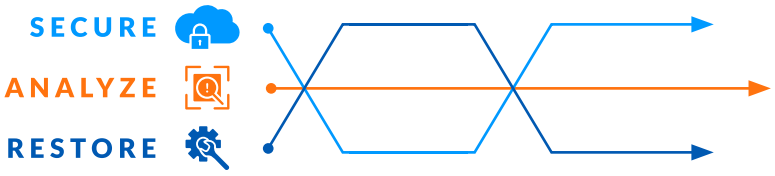
DATASHEET

Arctic Wolf®
Incident Response

Today, highly motivated threat actors target more organizations and launch more cyber attacks against them than at any other time. Threat actors will leverage everything including zero-day exploits, 2-year-old vulnerabilities, social engineering skills that trick employees, or they'll simply slip through the gaps of existing security controls to gain access to your environment.

Once inside, threat actors entrench themselves, establish backdoors, and start feeding on your data.

Based on these market dynamics, it's critical that organizations have access to an incident response (IR) team that has all the capabilities to secure, analyze, and restore an environment as quickly as possible.



Secure

Secure the environment by eliminating threat actor access.

Analyze

Analyze the cause and extent of the activities while inside the network.

Restore

Restore the organization to its pre-incident condition.

Arctic Wolf's insurance-approved incident response team provides the full-suite of comprehensive emergency services you need to minimize downtime and get back to business.

with our best-in-class response times, we'll contain and eradicate threats immediately. Next, our digital forensics, business restoration, and threat actor teams will work in parallel to bring critical systems back online and ensure that your environment is safe. No matter the incident, shortening your recovery time is our primary goal.

15%

Arctic Wolf IR customers recover **15% faster** than the industry average*

Full-Service IR

Arctic Wolf provides the **end-to-end IR services** that you need to recover in-house

30+

Arctic Wolf is a recommended IR provider on over **30 insurance panels** around the world

92%

The Arctic Wolf IR team has **reduced ransom demands by an average of 92%** over the past year**

1,000+

The Arctic Wolf IR team completes over **1,000 incident engagements** a year

*Statista reports that it takes 26 days on average to recover from a ransomware event (Q1, 2022). The Arctic Wolf restoration average is 22 days.

**All cases are different, and ransom reductions are not guaranteed. It is also never a guarantee that threat actors will live up to their word in a ransom situation.

How We Help

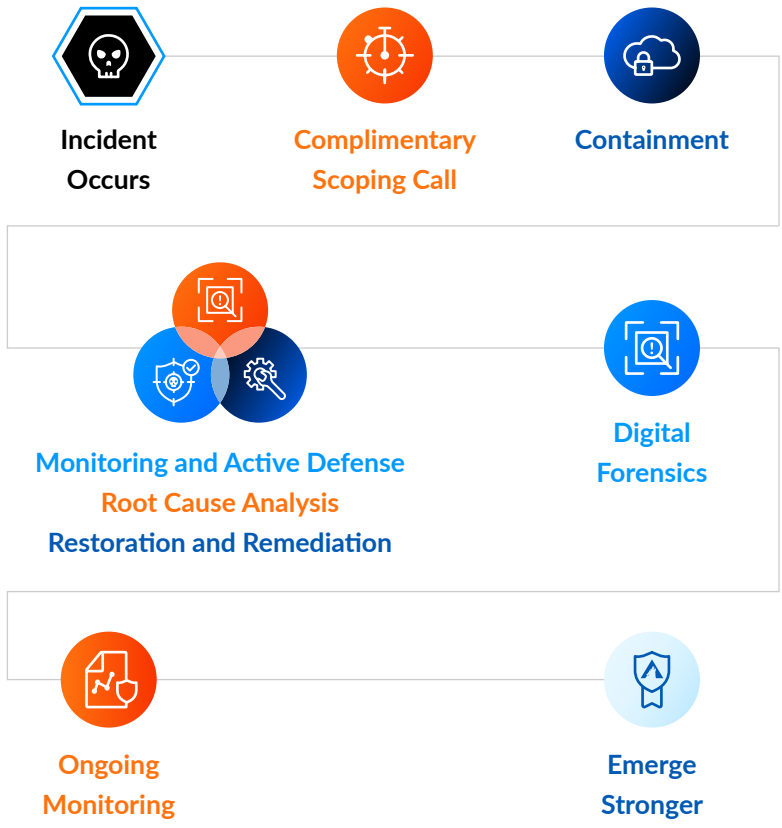
Types of Incidents Commonly Resolved

No matter the attack vector, we have experience mitigating the threat and remediating the damage across endpoint, network, identity, and cloud environments.

- **Ransomware & Data Extortion**
- **Business Email Compromise**
- **Data Breach Response**
- **Active Threat Actors & Compromised Domain Controllers**

Arctic Wolf Incident Response Timeline

A dedicated incident director orchestrates every response and assigns team members based on the attack type, scope of incident, and phase of response. Team members work in parallel through the response to minimize downtime and costs.



Comprehensive Services

Containment & Eradication

Our team of 24×7 IR experts contain the threat, close all points of access, remove threat actors, and eliminate routes to reentry.

Advanced Digital Forensics

The Arctic Wolf digital forensics team conducts a rapid and thorough forensics investigation to identify the root cause, as well as the full impact and scope of the cyber attack.

Business Restoration

Our in-house experts help to restore everything from operating systems, to workstations, to applications, to critical business functions.

Threat Actor Expertise

Arctic Wolf has vast experience managing and negotiating cases for all major threat actor groups across all industries. In addition to negotiation, our IR team is continuously monitoring threat actor profiles on the dark web.

Arctic Wolf Incident360 Retainer

The one-of-a-kind Arctic Wolf Incident360 Retainer combines incident readiness with end-to-end incident coverage from an insurance-approved IR team.

Customers can rest easy knowing that no matter the incident type, they'll receive the remediation and recovery support that they need to get back to business as quickly as possible.

Incident360 Retainer Benefits

Receive end-to-end IR coverage for 1 incident, no matter the incident type

Save up to 70% on a standalone emergency IR engagement

Complete key readiness activities without sacrificing the ability to respond to an incident

Minimize the impact of security events with an IR Plan Review and Tabletop exercise

About Arctic Wolf

Arctic Wolf® is a global leader in security operations, enabling customers to manage their cyber risk via a premier cloud-native security operations platform. The Arctic Wolf Aurora™ Platform ingests and analyzes more than eight trillion security events a week to help enable cyber defense at an unprecedented capacity and scale, empowering customers of virtually any size across a wide range of industries to feel confident in their security posture, readiness, and long-term resilience. By delivering automated threat protection, response, and remediation capabilities, Arctic Wolf delivers world-class security operations with the push of a button.

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

ARCTIC WOLF

AICPA SOC

ISO 27001 CERTIFIED
CYBERGUARD COMPLIANCE