Arctic Wolf®
Incident Response

DATASHEET

Arctic Wolf Incident Response

When cyber attacks turn into major incidents, organizations need a proven partner to help them fully eradicate the threat and restore normal business operations.

Today highly motivated threat actors target more organizations and launch more cyber attacks against them than at any other time. They exercise brute force tactics, use social engineering skills to trick employees, or simply slip through the gaps of existing security controls. Once inside, threat actors entrench themselves, establish backdoors, and start feeding on your data.

Arctic Wolf® believes that to fully eradicate the threat and restore normal business operations, you need a full-service incident response (IR) provider. It's not enough to simply delete the threat. Instead, finding the root point of compromise, documenting what happened, and restoring business operations to pre-incident conditions are vital in every response scenario to get the organization back online and prevent future incidents.

Full-Service Incident Response

Incident Response is available from a variety of companies, each offering a range of services directly to organizations or through cyber insurance carriers. Be sure to select a full-service vendor with in-house expertise to provide comprehensive digital forensics and data recovery services. Only full-service providers eliminate the threat actor's access to the environment, analyze the cause and extent of the attack, and restore the business to normal pre-incident operations.

Effectively achieving all three of these objectives, requires an IR firm with a multifaceted team of in-house expertise. Coordination across the team and with the customer is vital to the response process, and everyone from the SOC to the board room needs to understand the status of the investigation and the significance of the findings.

In-Depth Forensics Investigations

Our team of digital forensics analysts work to determine root point of compromise, lateral movement, and if data was accessed, deleted, or stolen.

Exceptional Client Experience

Our primary goal is to return every client to normal operations as quickly as possible. We provide thoughtful communication and timely guidance to provide confidence during a chaotic situation. This includes:

- Named Incident Director
- Progress updates and milestone tracking
- Clear explanations of digital forensics investigation findings

Dedicated IR Experts

A named Incident Director is assigned to every IR case. The Incident Director is intimately familiar with your specific situation and remains your primary point of contact throughout the incident response process.

IR JumpStart Retainer

Organizations can ensure priority access to Arctic Wolf Incident Response through our IR JumpStart Retainer. The Arctic Wolf® IR JumpStart Retainer is the first proactive incident response retainer that combines incident response planning with a 1-hour SLA and no prepaid hours. Learn more.

> **"This is one of the most significant threats to this organization's existence that I have encountered in my 32 years here. On behalf of each and every one of us in this entire organization, I thank you, with the greatest sincerity and respect."**
>
> *— CEO, National Manufacturing and Logistics Company*

Incident response support was the customer's first engagement with Arctic Wolf.

Go Beyond Traditional Incident Response with Arctic Wolf

We know that finding an active threat actor inside your network is one of the worst situations that your business could experience and we're here to help. We will forever challenge ourselves to continuously enhance every aspect of our service and provide you with an exceptional customer experience. You can count on us to provide full-service incident response and help prevent this kind of event from ever happening again.

Digital Forensics

- Determination of root point of compromise
- Persistent access threat investigation
- Data compromise investigation
- Analysis of the full extent (scope) of compromise to inform legal liabilities

Threat Actor Expertise

- Neutralization of attacks originating from every threat group
- Recovery and decryption of data from all current ransomware variants
- Continuously updated threat actor profiles and TTPs database

Business Operations Restoration

- Assignment of dedicated named Incident Director
- Rebuild of system operating system and applications
- Collaboration and partnership with top cyber privacy attorneys

Technology Agnostic

- Leveraging of existing security tools during investigation
- Recovery from any OS including Windows, MacOS, Linux
- Cloud IR expertise spanning infrastructure (IaaS), platform (PaaS), and applications (SaaS)

Data Recovery

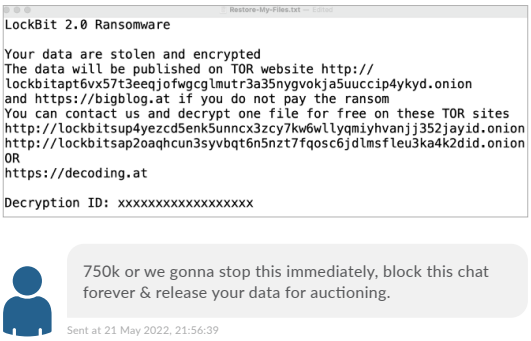
- Backup restoration
- Data decryption
- Advanced recovery of corrupted and deleted data

Frictionless Escalation

- Arctic Wolf's stored data on your organization helps us accelerate the response
- Arctic Wolf Security Services and our Concierge Security Team remain your first call in a crisis

Do not attempt to negotiate with threat actors or decrypt ransomed data on your own.

Contact Arctic Wolf to save time, money, and your data.



Elastic Incident Response Framework

SECURE

Secure the environment by eliminating threat actor access.

- Remediate root point of compromise
- Monitor for re-entry attempts
- Collect and preserve data and evidence

ANALYZE

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

- Establish dwell time
- Investigate which files may have been accessed, deleted, or stolen
- Thorough explanation of forensics findings

RESTORE

Restore the organization to its pre-incident condition.

- Data recovery
- System restoration
- Threat actor negotiations
- Ransom settlements

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, identity, 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.

Arctic Wolf Incident Response team engagement is in English. All statements of work (SOW) are transacted in US dollars (USD). We support the operating system of the devices being worked on and support the local language.

SOC2 Type II Certified

ISO 27001 CERTIFIED
CYBERGUARD COMPLIANCE