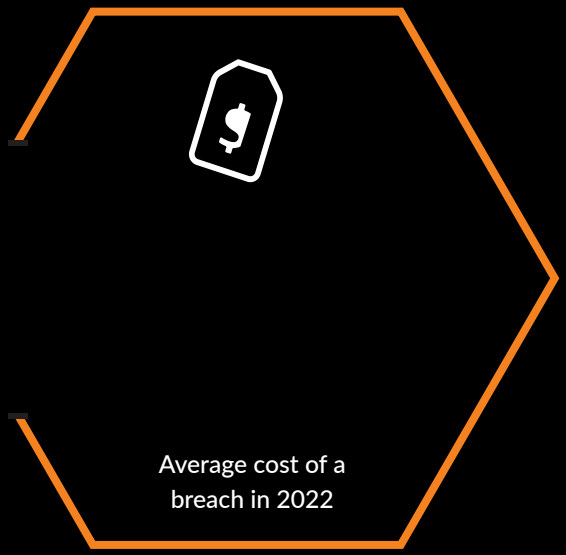
END CYBER RISK

EVERY MINUTE MATTERS:

THE ARCTIC WOLF INCIDENT RESPONSE TIMELINE

TABLE OF CONTENTS

Every Minute Matters: The Arctic Wolf® Incident Response Timeline

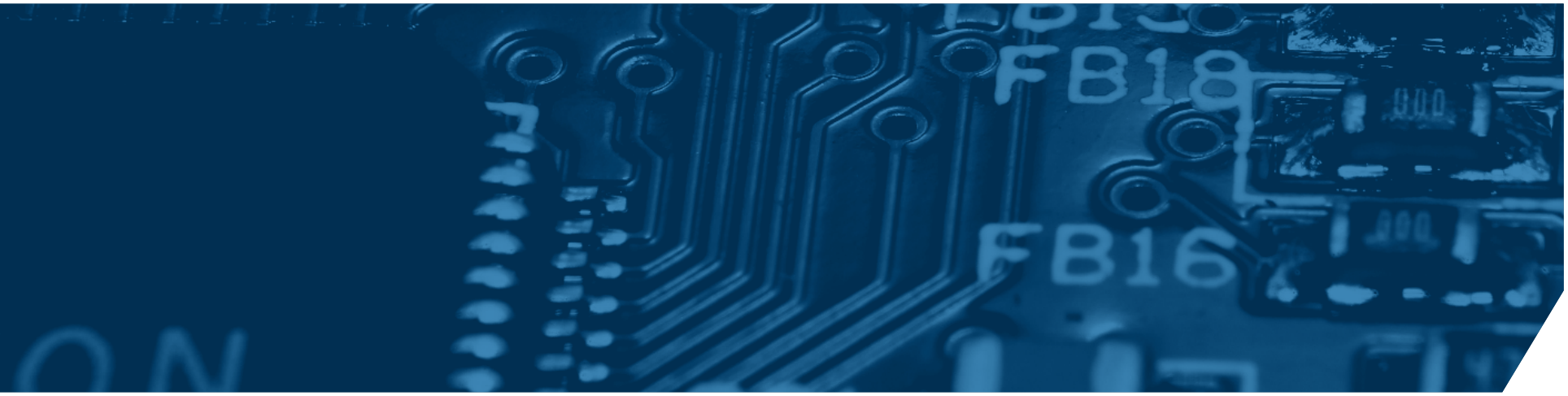


Source: https://www.ibm.com/reports/data-breach

One key metric to always measure is “dwell time” — the length of time a breach goes undetected. Typically, the longer the dwell time, the larger the losses.

According to research conducted by Ponemon Institute on insider attacks, when they are detected in fewer than 30 days, the cost stands at $7.12 million. When it takes an organization more than 90 days to detect an insider attack, however, losses basically double to $13.71 million. To truly mitigate any damages from such a breach, the dwell time needs to no longer be measured in days but minutes.

Organizations understand their ability to act quickly is critical in mitigating risk. However, there are challenges that stand in the way, such as the tools they employ and the talent they lack — especially as the threat landscape now requires 24x7 coverage if businesses even hope to stay protected.



Many organizations attempt to keep up by investing in the latest security tools, but these often come with distinct shortcomings.

Security information and event management (SIEM) platforms, for example, can create a lot of "noise" in the form of false positives. This overabundance of noise results in a paralyzing degree of alert fatigue for IT security staff, who are already stretched far too thin.

SIEMs can also provide a false sense of security because such platforms tend to gather and analyze data inconsistently, with only some of the logs from log-producing systems being ingested. This creates a blind spot that ultimately puts organizations at risk.

Many businesses end up chasing their tails.

As the volume and severity of threats intensify and losses continue to grow at a rapid rate, their IT and security teams find themselves overwhelmed with alerts while forced to wage a war for increasingly scarce cybersecurity talent. So, it's no surprise when they struggle to respond to the continually increasing risk of cyber threats quickly and effectively.

Arctic Wolf customers, like most organizations, need to quickly detect and remediate attacks.

By combining technology, in form of the Arctic Wolf® Platform, and human expertise provided by the Arctic Wolf Triage Team and Concierge Security® Team (CST), we provide clients with an immediate response to threats — and apply this learning to strengthen resilience over time.

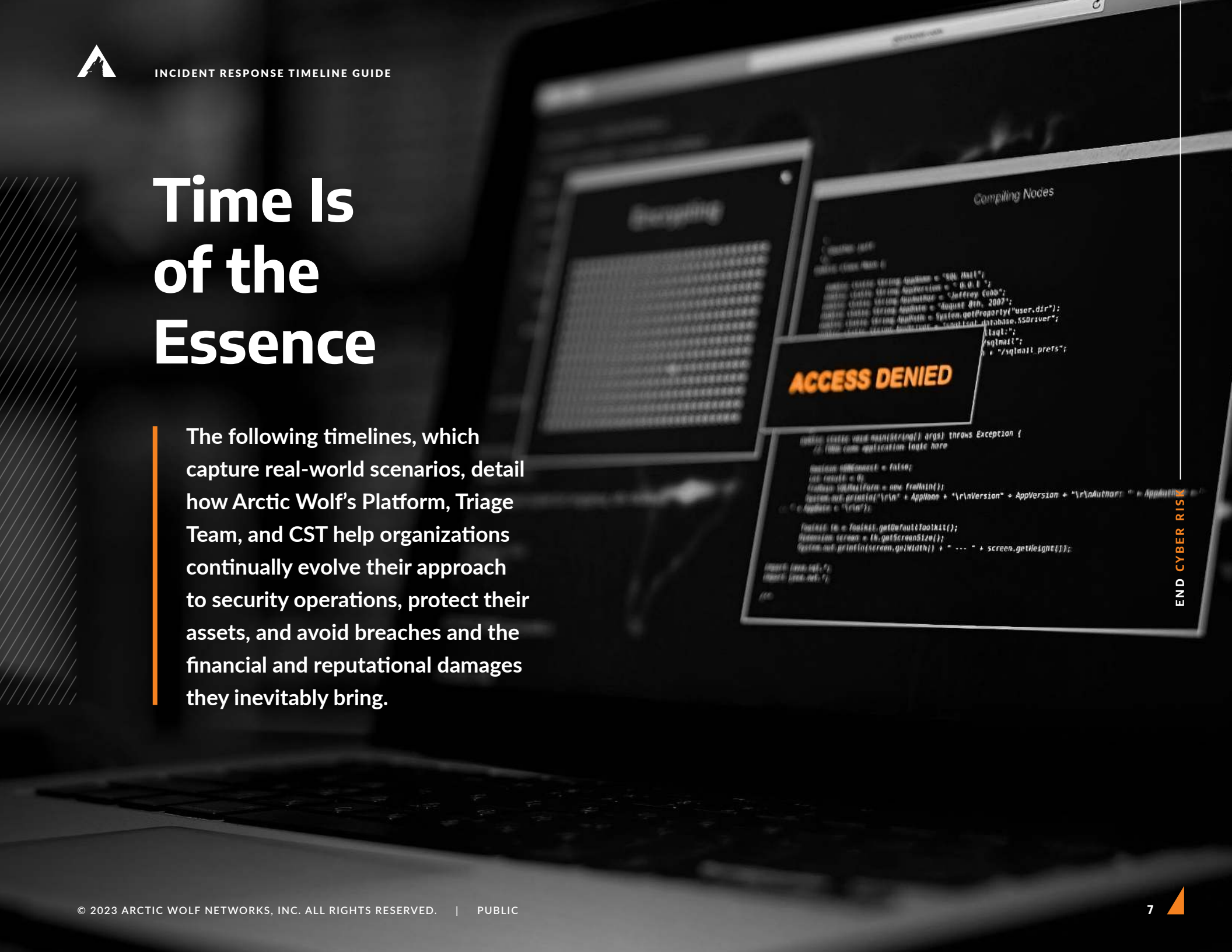
As the name suggests, the Triage Team focuses on tactical approaches to incidents as soon as they arise. When Arctic Wolf's Platform detects an anomaly, the Triage Team initiates an investigation to confirm or refute the threat. The Triage Team then relays the results of its investigation to the customer, ranging from a simple notification to ongoing collaboration with the customer until the incident is resolved.

The CST focuses on the relationship with the customer and the strategic implications of an attack to improve its security operations over the long term.

Regardless of the path to resolution, the CST receives a detailed explanation of the incident from the triage team. The CST then helps the customer identify areas

Time Is of the Essence

The following timelines, which capture real-world scenarios, detail how Arctic Wolf's Platform, Triage Team, and CST help organizations continually evolve their approach to security operations, protect their assets, and avoid breaches and the financial and reputational damages they inevitably bring.



RANSOMWARE CONTAINMENT: UTILITIES

Arctic Wolf Platform | Arctic Wolf Triage Team | Customer | CST

5:53 pm

Source: Arctic Wolf Agent

- Detected possible Malicious Encoded PowerShell Script (Base64)
- Arctic Wolf Platform automatically Decoded suspicious Encoded Obfuscated LOAD String
- [LOCAL ADMIN PASSWORD] is changed by PowerShell Script

Investigation Triggered

- Indicators previously curated by the Arctic Wolf Labs team trigger an event of interest
- Arctic Wolf Platform correlates potential malicious activity with other known IoCs
- Incident escalated to Triage Team forensic dashboard with Urgent status

5:54 pm

BUSINESS EMAIL COMPROMISE: MANUFACTURING

Arctic Wolf Platform | Arctic Wolf Triage Team | Customer | CST | Adversary

12:57 pm

- Attacker leveraged previously stolen [User1] credentials and sends Duo MFA pushes to legitimate user.
- [User1] accepts Duo MFA push from attacker.
- Attacker establishes ActiveSync with [User1] mailbox.

EXCHANGE EXPLOIT:
CONSTRUCTION

Arctic Wolf Platform | Arctic Wolf Triage Team | Customer | CST | Arctic Wolf Continually Monitoring

- Customer completes 30-day onboarding, Service Delivery starts

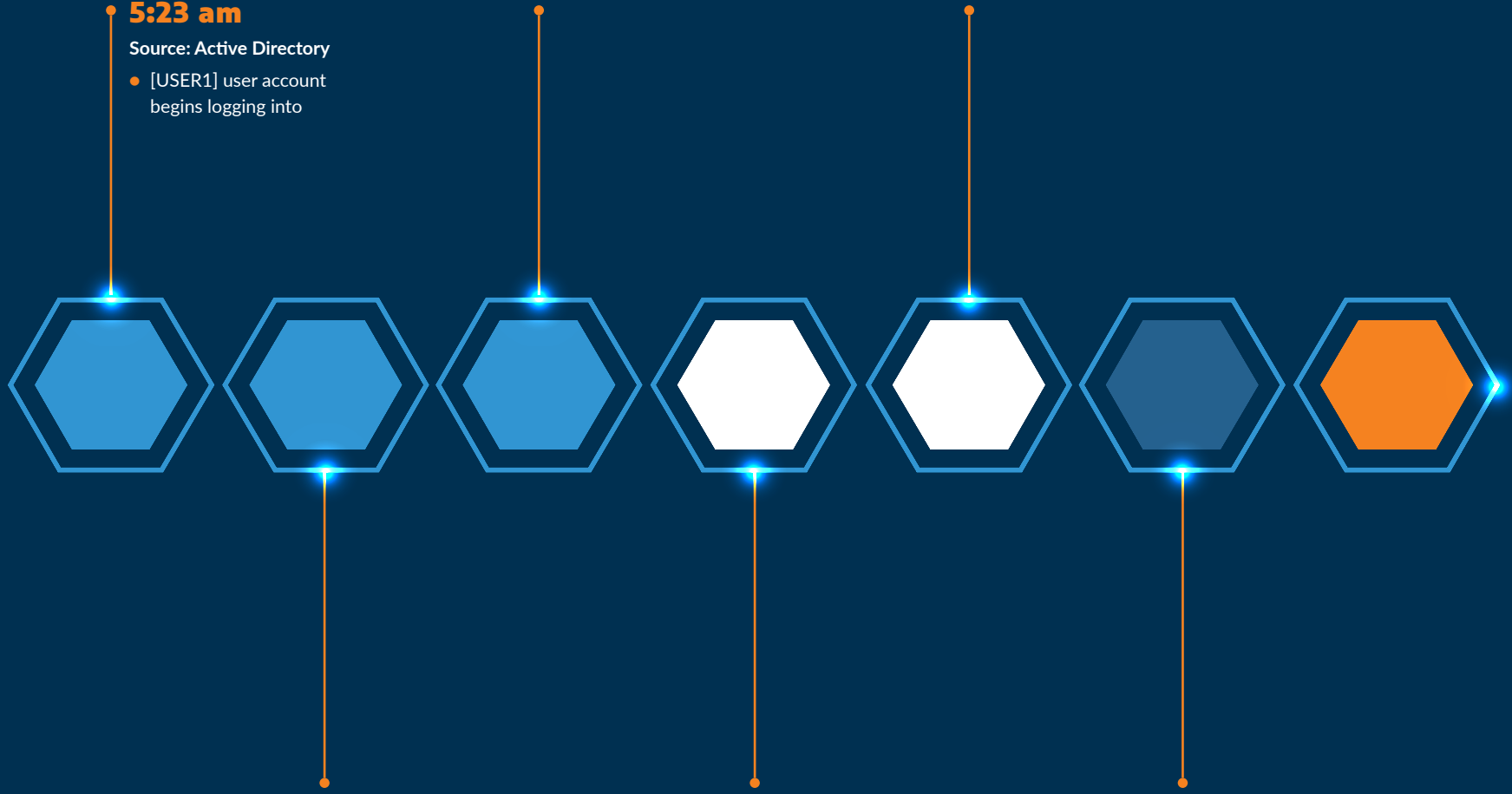
RANSOMWARE CONTAINMENT:
LOCAL GOVERNMENT

Arctic Wolf Platform | Arctic Wolf Triage Team | Customer | CST

5:23 am

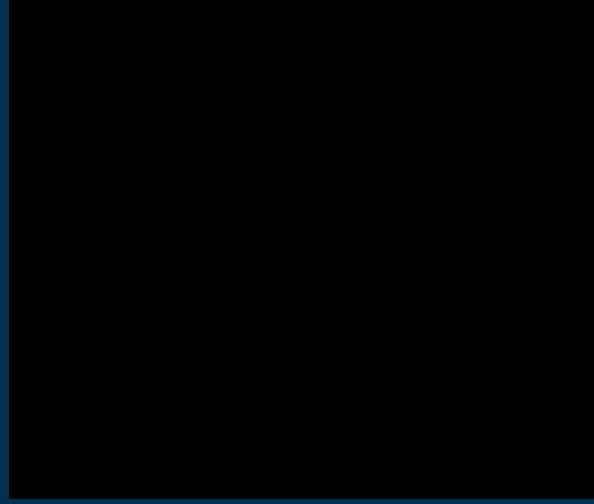
Source: Active Directory

- [USER1] user account begins logging into



PASSWORD SPRAY: LEGAL

Arctic Wolf Platform Arctic Wolf Triage Team



The Key to Effective Security Operations

The difference between an attack failing or succeeding often depends on speed of action. The faster an attacker can identify and exploit weaknesses, the more likely they will achieve their goals. Conversely, the longer it takes an organization to respond, the more likely they will succumb to an attack.

Organizations need strategic security partners who can detect threats quickly and analyze them for root causes. Those partners must also possess the ability to marry threat analysis with in-depth knowledge and expertise of the evolving landscape and provide actionable steps to improve an organization's security posture. They need visibility across their entire attack surface to be able to detect threats and correlate events effectively.

Together, the Arctic Wolf Platform, Triage Team, and CST provide customers with a cohesive and scalable approach to security operations that evolves as the threat landscape changes.

Arctic Wolf moves fast and effectively when time is a critical factor to ensure our customers

END CYBER RISK

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.

REQUEST A DEMO

SOC2 Type II Certified

Contact Us

arcticwolf.com
1-888-272-8429
ask@arcticwolf.com