Detectie en Respons

LEON VAN DONGEN – ARCTIC WOLF

ARCTIC WOLF

THE LEADER IN SECURITY OPERATIONS

INFRADAX
IT VAN NU

Arctic Wolf

END CYBER RISK
Leon van Dongen – Sales Engineer

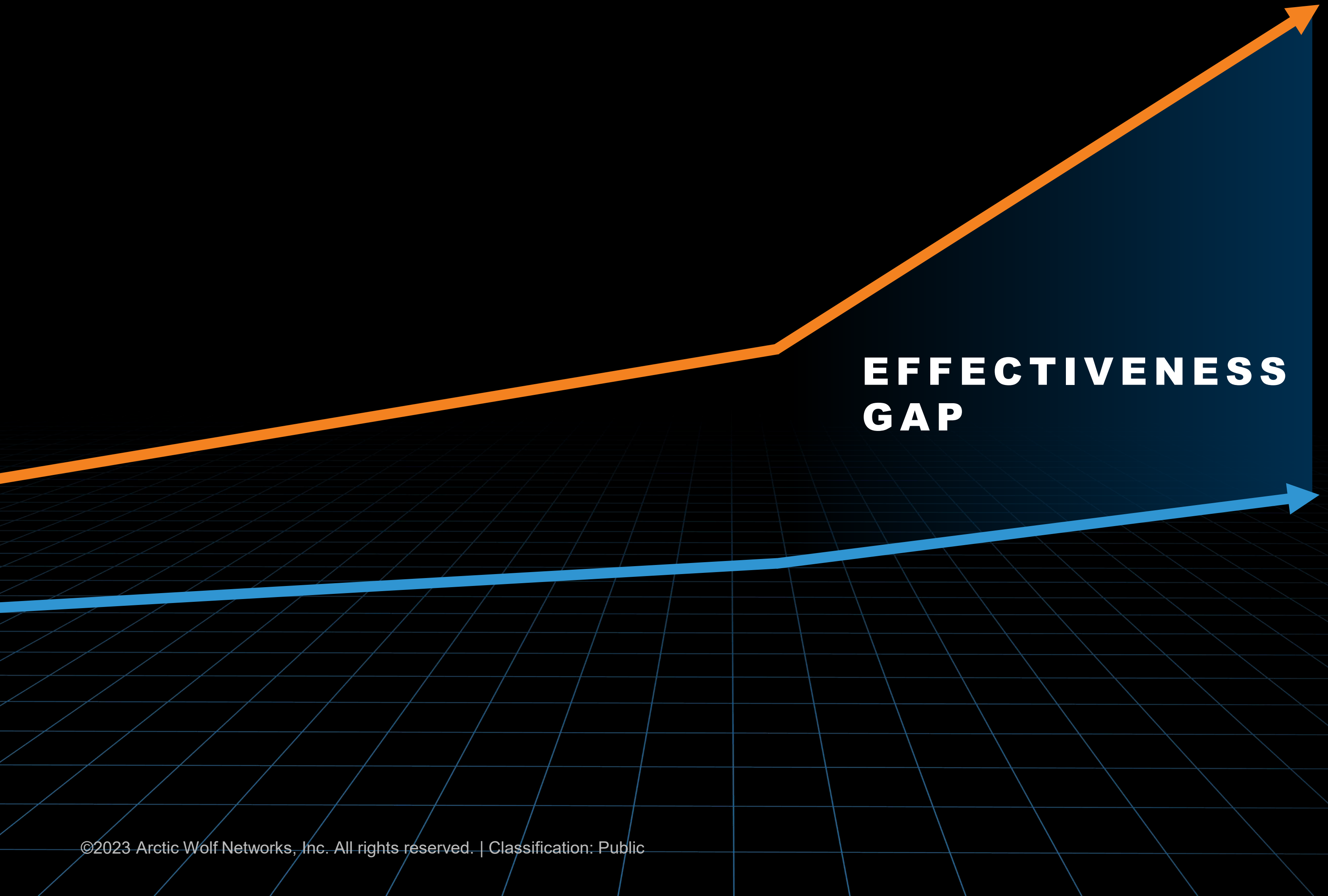
LIKELIHOOD
OF AN INCIDENT

CYBER
RISK

IMPACT
OF AN INCIDENT

©2023 Arctic Wolf Networks, Inc. All rights reserved. | Classification: Public

Accelerating Risk



48%

INCREASE

in Cybercrime Losses in 2022

Total Security Companies:

3,377+

Total Security Spend:

169B

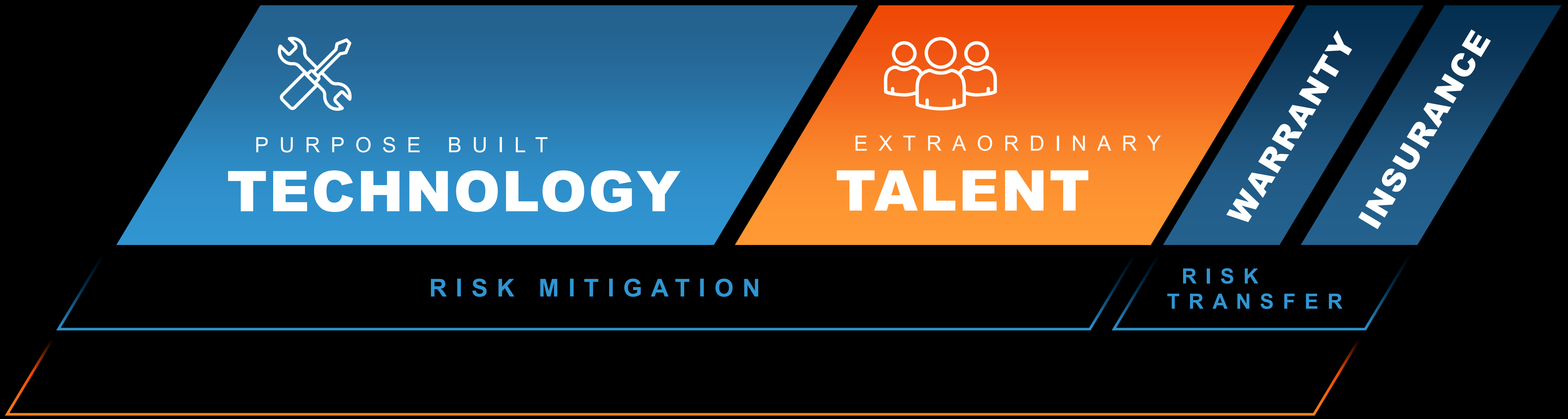
YoY Spend Increase:

11%

©2023 Arctic Wolf Networks, Inc. All rights reserved. | Classification: Public

Sources: IC3, Gartner, It-Harvest

Ending Cyber Risk



PURPOSE BUILT
TECHNOLOGY

EXTRAORDINARY
TALENT

WARRANTY

INSURANCE

RISK MITIGATION

RISK
TRANSFER

TOTAL RISK

©2023 Arctic Wolf Networks, Inc. All rights reserved. | Classification: Public

The Problems We Solve

Protect and Defend Against Threats

Limited Access to Talent

Improve Cyber Insurability

Security Tools Dissatisfaction

Security Spend Efficiency

Need to Demonstrate Compliance

©2023 Arctic Wolf Networks, Inc. All rights reserved. | Classification: Public

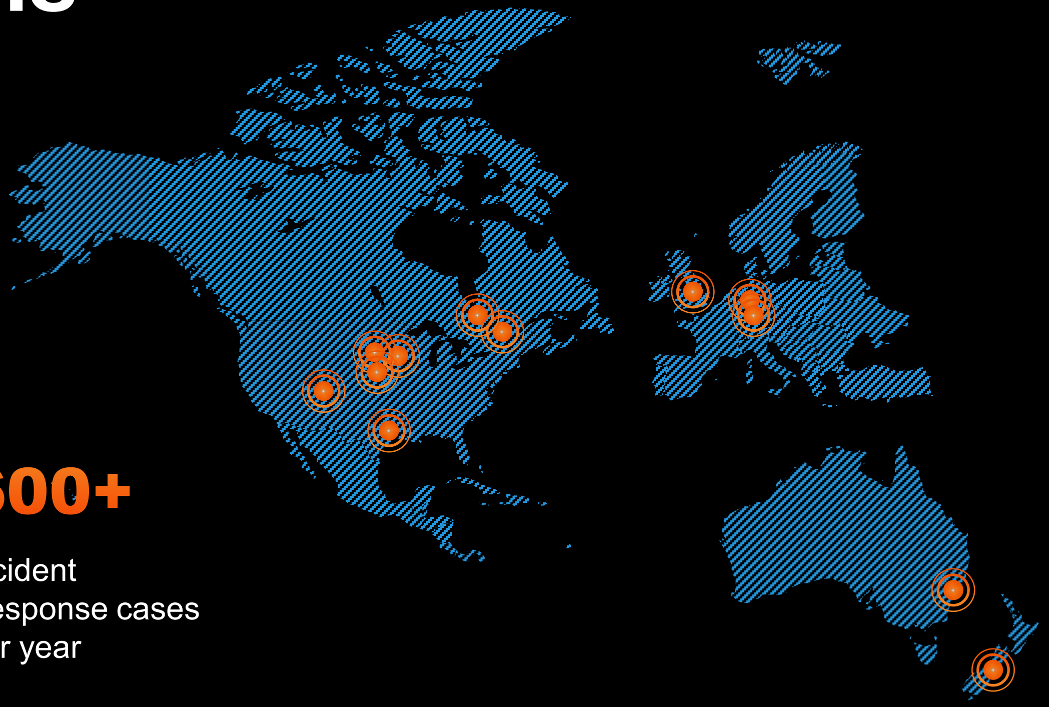
Arctic Wolf Security Operations

We Make Security Work

4,000+
Customers

24x7
Always-On Coverage

570+
Security Engineers



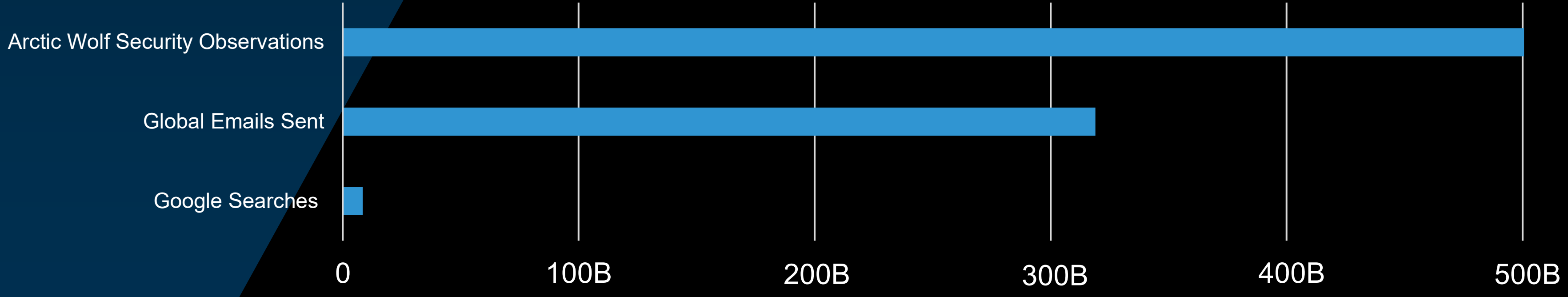
5
Datacenters globally

3.4+
Trillion events per week

2.9M+
AW active agents and 25,000+ sensors

12M+
Vulnerabilities identified per week

600+
Incident Response cases per year



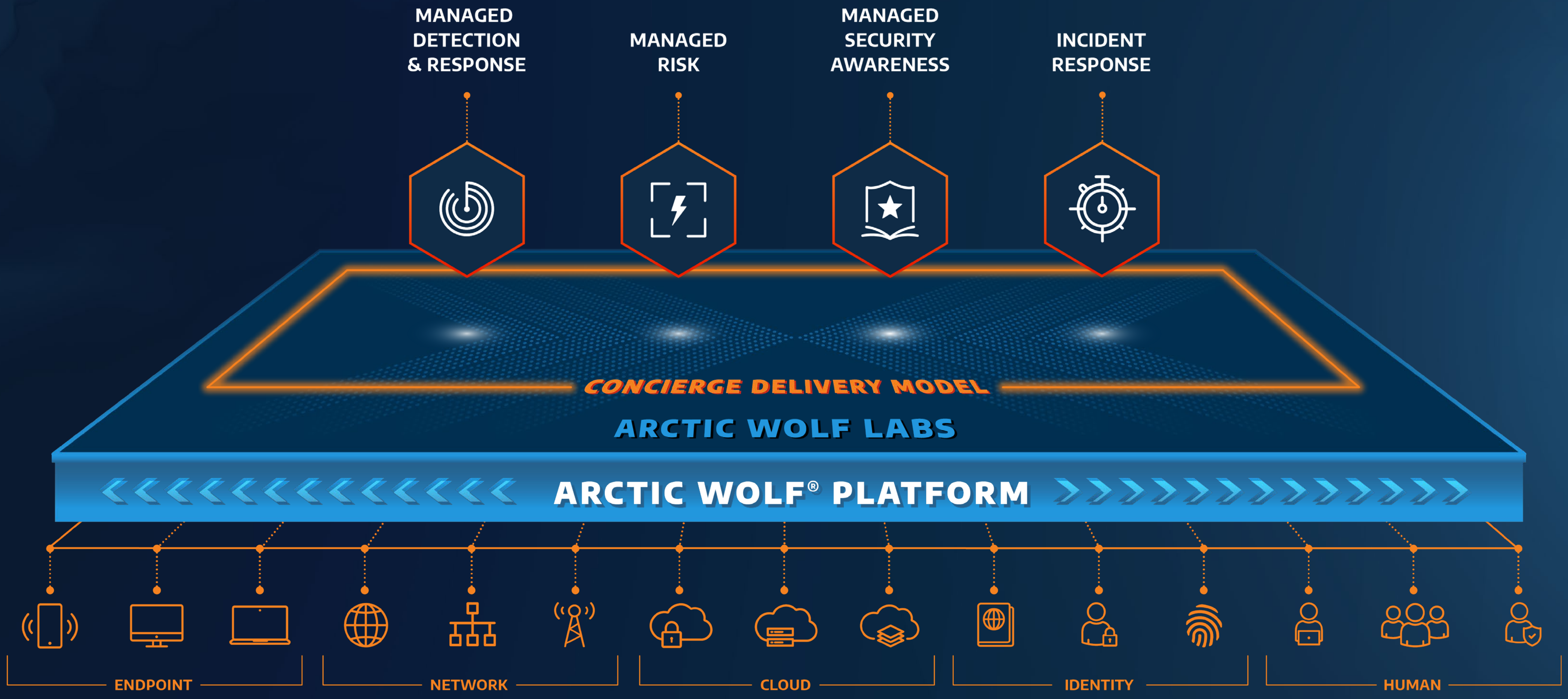
Global Volumes Per Day

©2023 Arctic Wolf Networks, Inc. All rights reserved. | Classification: Public

INFRADAX
IT VAN NU

ARCTIC WOLF

Security Operations Cloud



©2023 Arctic Wolf Networks, Inc. All rights reserved. | Classification: Public

Traditional IR Retainers Haven't Delivered

LARGE UP-FRONT COST

Prepaid bucket of hours costing 10s of thousands of dollars

RUSH TO BURN HOURS

Prepaid hours are "use them or lose them"

NO PLANNING ASSISTANCE

Only if you don't have an incident or pay more upfront for that service

©2023 Arctic Wolf Networks, Inc. All rights reserved. Classification: Confidential

Benefits of IR JumpStart Retainer

- IR planning resources
- 1-hour response time to request for IR services
- Complimentary incident scoping call
- Preferred pricing and financial benefits
- Cyber insurance-approved IR team

RESPOND FASTER. EMERGE STRONGER.

TERMS AND CONDITIONS: https://arcticwolf.com/terms/

©2023 Arctic Wolf Networks, Inc. All rights reserved. Classification: Confidential

Arctic Wolf Incident Response and Infradax

With Arctic Wolf's IR JumpStart

You Own the Outcome

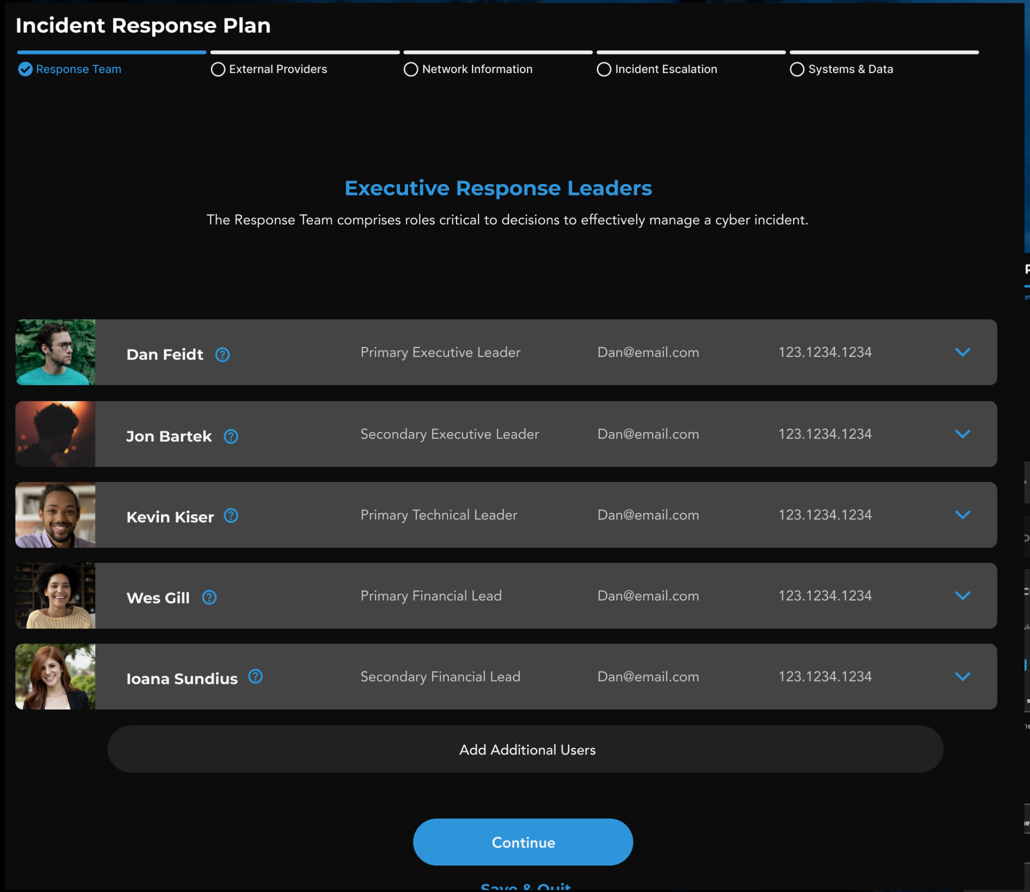
- You prepare jointly with Infradax for an incident with the benefit of building their IR Plan.
- You have a clear path to engage Arctic Wolf in the event of an incident.
- You have a trusted partner providing you an IR solution.
- Depending on need, you can ask Infradax to assist with remediation with Arctic Wolf direction.

©2023 Arctic Wolf Networks, Inc. All rights reserved. Classification: Confidential

IR Planning & Review Session

PLANNING BENEFITS

- Identify key contacts
- Organize data and network assets
- Secure online file storage
- Partner and customer collaboration on plan-building process and review



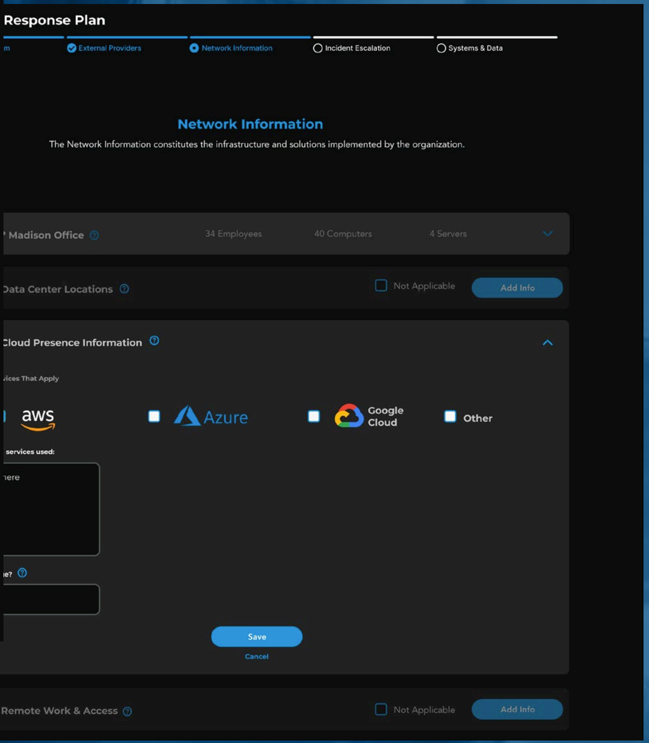
Incident Response Plan

Executive Response Leaders

The Response Team comprises roles critical to decisions to effectively manage a cyber incident.

Dan Feidt	Primary Executive Leader	Dan@email.com	123.1234.1234
Jon Bartek	Secondary Executive Leader	Dan@email.com	123.1234.1234
Kevin Kiser	Primary Technical Leader	Dan@email.com	123.1234.1234
Wes Gill	Primary Financial Lead	Dan@email.com	123.1234.1234
Ioana Sundius	Secondary Financial Lead	Dan@email.com	123.1234.1234

IR Plan Builder



Response Plan

Network Information

The Network Information constitutes the infrastructure and solutions implemented by the organization.

Madison Office	34 Employees	40 Computers	4 Servers

Data Center Locations ☐ Not Applicable

Cloud Presence Information

ices That Apply

☐ aws ☐ Azure ☐ Google Cloud ☐ Other

services used:

ere

e?

Remote Work & Access ☐ Not Applicable

©2023 Arctic Wolf Networks, Inc. All rights reserved. Classification: Confidential

A New Approach

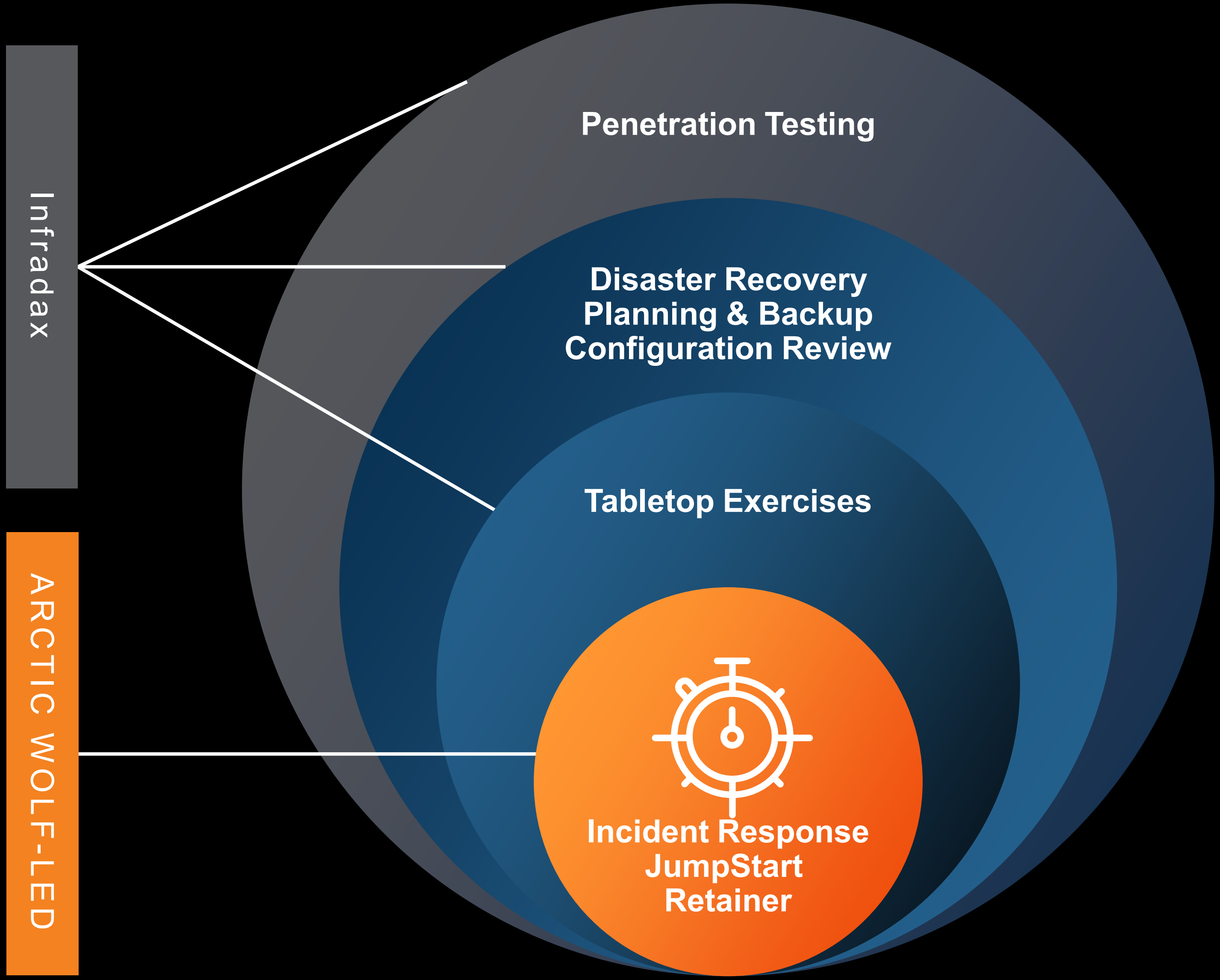
IR Preparedness Services Package

- A tailored service package to best serve you
- Short-term progress toward reducing your cyber risk before an incident
- No time crunch to burn down unused hours
- We are your trusted advisor throughout the entire lifecycle

Key Benefits

- IR SLA: 1 hour or less
- Prepare and securely store your IR plan (partner and customer)
- Complimentary scoping call in the event of an incident
- Discounted IR hourly rate of €270/hr EUR in the event of an incident*
- No up-front purchase of IR hours

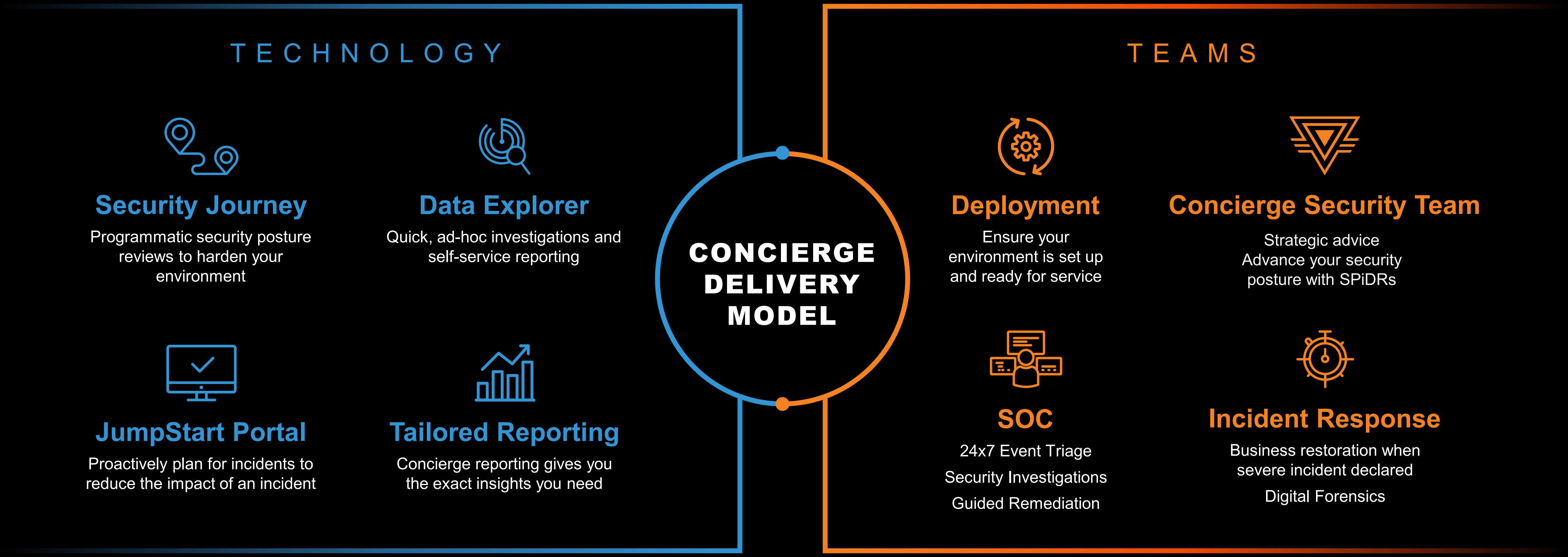
* USD Dollar bound


Infradax
ARCTIC WOLF-LED
Penetration Testing
Disaster Recovery Planning & Backup Configuration Review
Tabletop Exercises
Incident Response JumpStart Retainer

©2023 Arctic Wolf Networks, Inc. All rights reserved. Classification: Confidential

Concierge Delivery Model

Technology and Teams Delivering Real Security Outcomes



TECHNOLOGY

Security Journey
Programmatic security posture reviews to harden your environment

Data Explorer
Quick, ad-hoc investigations and self-service reporting

JumpStart Portal
Proactively plan for incidents to reduce the impact of an incident

Tailored Reporting
Concierge reporting gives you the exact insights you need

CONCIERGE DELIVERY MODEL

TEAMS

Deployment
Ensure your environment is set up and ready for service

Concierge Security Team
Strategic advice
Advance your security posture with SPiDRs

SOC
24x7 Event Triage
Security Investigations
Guided Remediation

Incident Response
Business restoration when severe incident declared
Digital Forensics

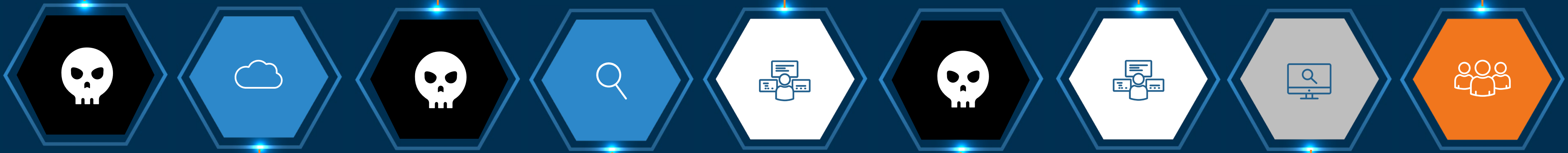
©2023 Arctic Wolf Networks, Inc. All rights reserved. | Classification: Public

[REAL] INCIDENT TIMELINE
Business Email Compromise

©2021 Arctic Wolf Networks, Inc. All rights reserved. Restricted

Business Email Compromise - Manufacturing

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



12:57

- 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

Source: Duo

The Arctic Wolf Platform logs MFA successful for [User1]

13:16

- 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.

13:16

Source: Office 365 Logs

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

13:18

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

13:22

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

13:25

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

13:25

- Customer confirms [User1] compromise
- Customer disables account

13:31

- 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.

©2021 Arctic Wolf Networks, Inc. All rights reserved. Restricted

Key Takeaways

Attack Type

Email Account Takeover

Time to Detect

12:57 - 13:16 | 19 Minutes

Data Sources

Office 365
Duo

©2021 Arctic Wolf Networks, Inc. All rights reserved. Classification: Public

[REAL] INCIDENT TIMELINE

Ransomware

©2021 Arctic Wolf Networks, Inc. All rights reserved. Restricted

Ransomware Attack – Local Government

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

05:23

Source: Active Directory

[USER1] user account begins logging into multiple systems

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]

05:26

05:28

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

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

05:29

05:48

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

Remediation

Customer responds that the device has been contained and passwords reset

06:13

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

©2021 Arctic Wolf Networks, Inc. All rights reserved. Restricted

Key Takeaways

Attack Type

Ransomware Attack

Time to Detect

05:23 - 05:28 | 5 Minutes

Data Sources

Active Directory
Arctic Wolf Sensor

©2021 Arctic Wolf Networks, Inc. All rights reserved. Classification: Public

Arctic Wolf: The Best Value in Cyber Security

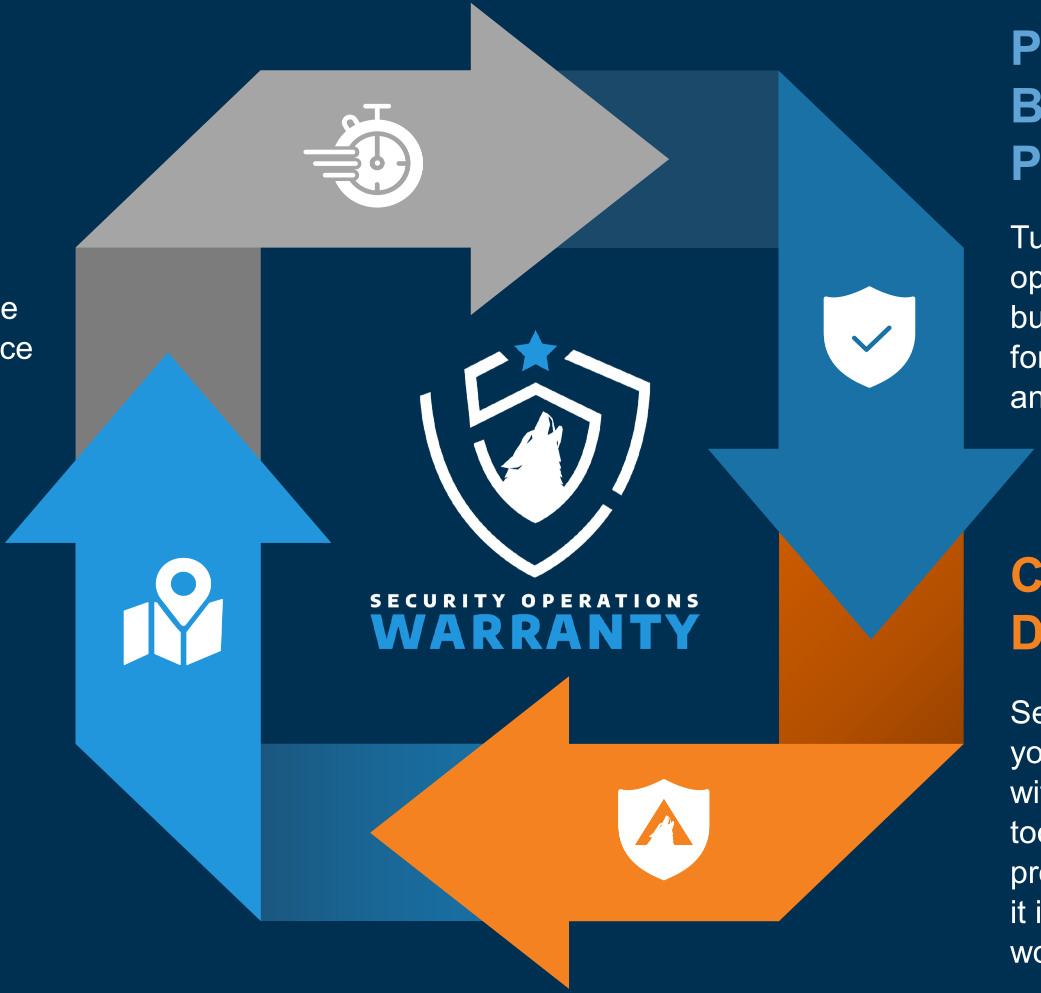
At a fraction of the cost of going it alone, Arctic Wolf provides comprehensive coverage and a holistic approach to ending cyber risk.

Time to Value

Leverage existing investments, add resources and expertise to your team, and reduce noise with a turnkey solution

Cyber Risk Management

Mitigate cyber risk with our Security Operations Cloud and transfer residual risk via our Warranty and Insurance partnerships



Purpose Built Platform

Turn-key security operations at scale, built on Open-XDR for broad coverage and 24x7 protection

Concierge Delivery

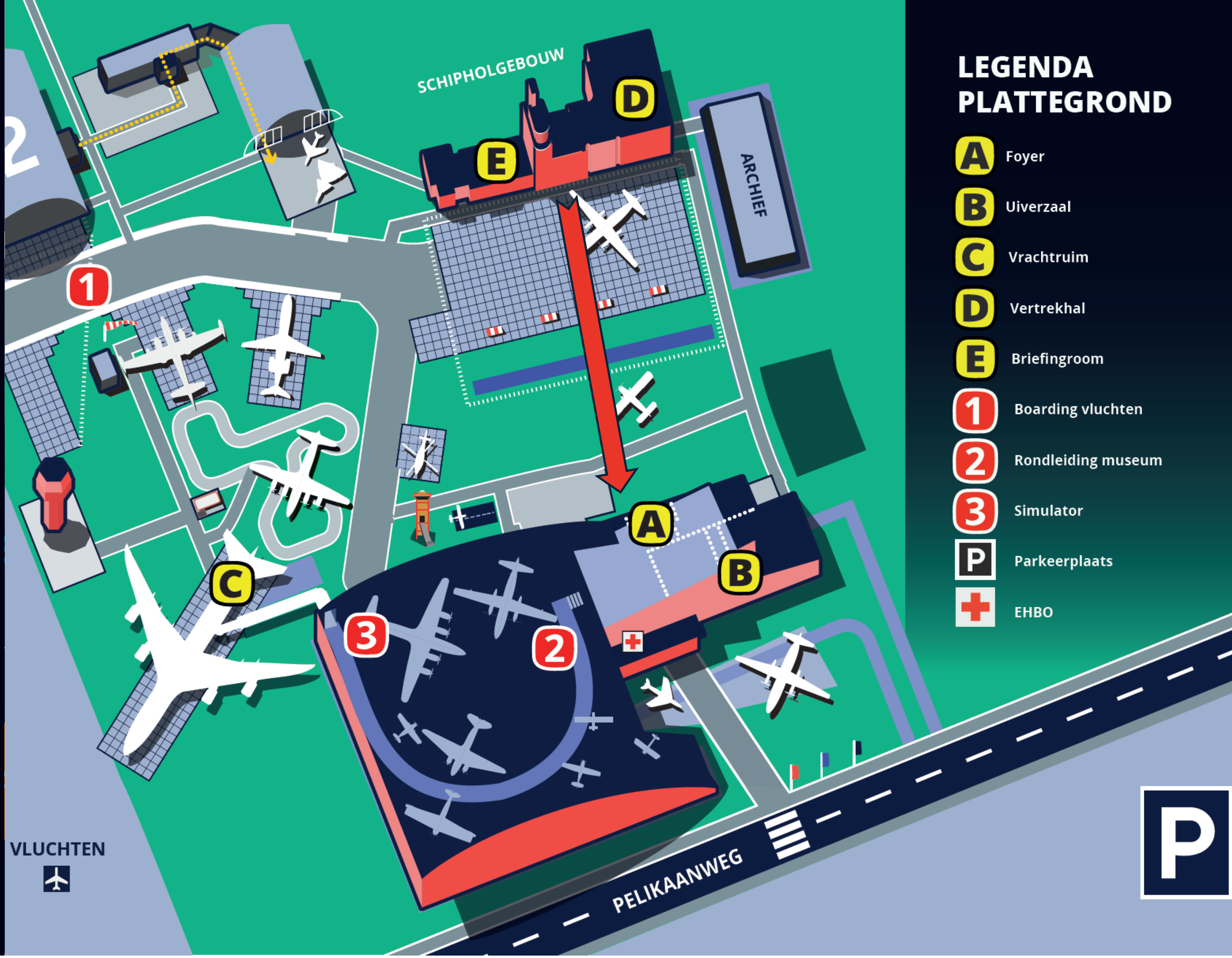
Security tailored to your specific needs with flexibility in the tools, people, and processes to deliver it in whatever way works best for you

©2023 Arctic Wolf Networks, Inc. All rights reserved. | Classification: Public

Thank You

©2023 Arctic Wolf Networks, Inc. All rights reserved. | Classification: Public

	FRIENDSHIP FOYER	UIVERZAAL	VRACHTRUIM	VERTREKHAL	BRIEFINGROOM
08:30 - 09:00	Ontvangst & inschrijving				
09:00 - 09:20		Opening			
09:30 - 10:10		**Werkplek** Panelsessie	**Infradax Overheid** Advanced Datacleaning 1/2	**Veeam** Dataprotectie & recovery	**Dynamics Experts** CRM
10:20 - 11:00		**Security** Panelsessie	**Infradax Overheid** Advanced Datacleaning 2/2	**JSR** Slimmer Samenwerken	**Dell Technologies** Datacenter als datawarehouse
11:10 - 11:30	Koffiebreak				
11:30 - 12:10		**Datacenter** Panelsessie	**Infradax Overheid** ICT-regievoering	**Holm Security** Vulnerability Management	**Microsoft** Microsoft 365
12:20 - 13:00	Lunch groep **1**		**Cumlaude.ai** AI		
13:10 - 13:50	Lunch groep **2**		**Microsoft** Business Applications		
14:00 - 14:40		**AI** Panelsessie	**HPE** Hybrid Cloud	**Fortinet** Networking & Security	
14:50 - 15:10	Koffiebreak				
15:20 - 16:00			**Arctic Wolf** Detectie en Respons	**KPN** (Tele)communicatie	
16:10 - 17:00	Borrel				



LEGENDA PLATTEGROND

A	Foyer
B	Uiverzaal
C	Vrachtruim
D	Vertrekhal
E	Briefingroom
1	Boarding vluchten
2	Rondleiding museum
3	Simulator
P	Parkeerplaats
✚	EHBO

INFRADAX IT VAN NU

ARCUS IT

JSR

INFRADAX OVERHEID

ARCUS IT | Dynamics Experts