ARCTIC WOLF

THE LEADER IN SECURITY OPERATIONS

FRSECURE®

There's Been an Incident… Now What?

Agenda

01 Welcome
02 Brief Overview of Arctic Wolf & FRSecure
03 Textbook Incident vs Real-Word Incident
04 IR Planning & Prevention
05 Q&A
06 Closing & Resources

Speakers

John Harmon

President

FRSecure

Lane Roush

Sr. VP, Global Sales Engineering

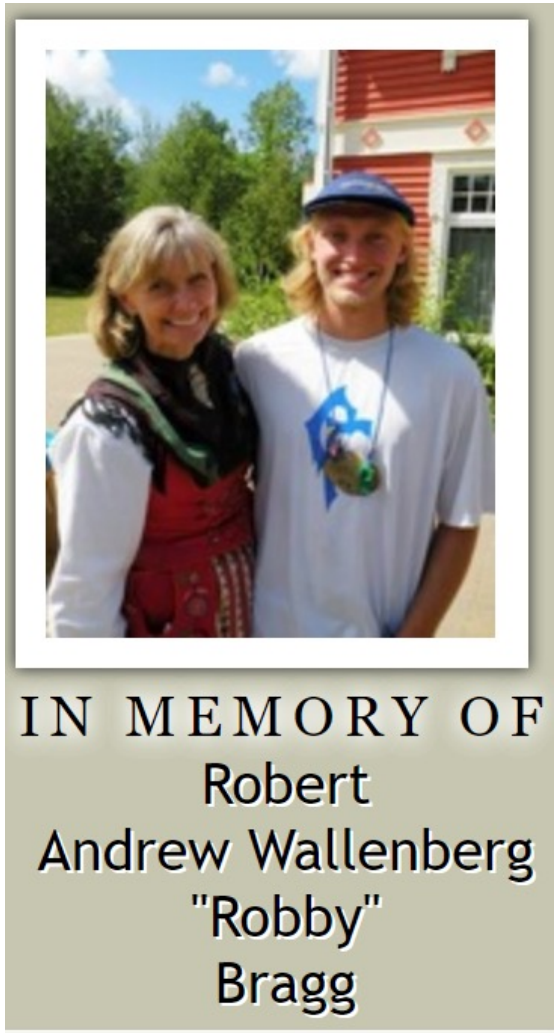
Arctic Wolf

46.4% of adults will experience a mental health illness in their lifetime

~118,000,000: 46.4% of adults

~48,400,000: 41% who receive professional care

~69,600,000: 59% who don't



- **Mental Health First Aid USA** https://mentalhealthfirstaid.org
- **National Suicide Prevention Lifeline (Hours: Available 24 hours.) - 800-273-8255**
- **SAMHSA Treatment Referral Helpline 877-SAMHSA7 (877-726-4727)**
- **Mental Health Hackers -** https://www.mentalhealthhackers.org

FRSecure – Security Experts on a Mission

The information security industry is broken. We need to fix it.

Talent shortage

No common language

Money-grab

Too much focus on IT

Not enough focus on people

Ego

Lack of accountability

Etc. Etc. Etc. (UNSECURITY BOOK)

Need all hands on deck yesterday

Based in MN

Offices in MT & CO. TN, TX and AZ coming soon

~90 Mission-Driven, Wonderful Humans

Product Agnostic

Core Services:

- **Forensics & Incident Response**
- **Security risk assessment**
- **vCISO**
- **Compliance (SOC2, PCI, CMMC, NIST, ISO, etc)**
- **Pen Testing**
- **Red Teaming (DEFCON Biohacking CTF 2021)**

ARCTIC WOLF

END CYBER RISK

How we define Cyber Risk

LIKELIHOOD OF AN INCIDENT

IMPACT OF AN INCIDENT

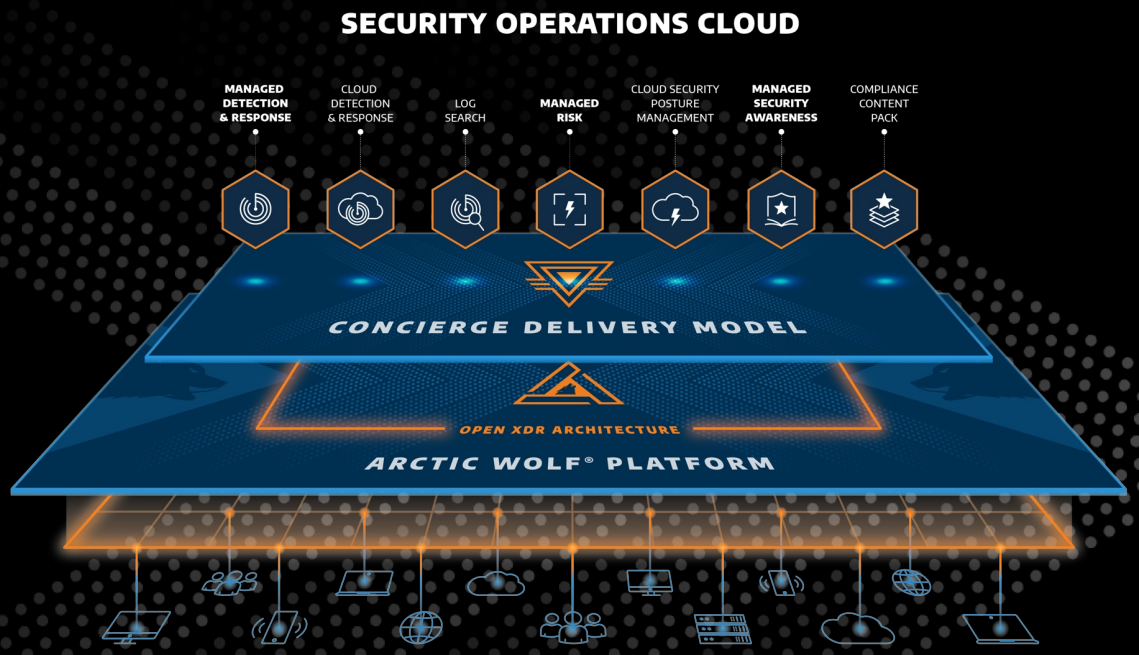
59%
Organizations breached in a year

40 day
Increase to patch ‘critical’ vulnerabilities

$9M
Average cost of a data breach in the US

212 days
Mean Time To Detect

Arctic Wolf: A Snapshot



1.5 Trillion+
Observations/ Week

13400+
Active Sensors

1.5 PB+
Data/ Week

SOC Statistics

5
Security Operation Centers

390+
Security Services Employees

6
University Relationships

90+
Hours of Yearly Analyst Training

5
Certification Levels

>225
Knowledge Domains

Textbook incident timeline

Start

Stuff Happens

Social engineering
Brute force
Honest mistakes
Vendors
Zero-day
Manufacturer failures
Cloud providers

Detect

Something's off
Alerts everywhere
System outage
Wire transfer attempts
Weird e-mails
Ransom messages

Process

IR plan (hopefully)
Call the right people
Response team engages
Call insurance (maybe)
Document & contain
Monitor for residual

Report

I'm not a lawyer – report it to who you need to

Sharing IOC's is a good idea

Finish

Real-world incident timeline – 800 emp co ransomed

Ransom message

Pretty standard: “Pay up or lose your data”

IR Team dives in – backups infected

Insurance called

They negotiate
Attacker gets upset
FBI notified

FBI says “no”

Attacker is linked to terrorism
FBI says do not pay

Insurance fails

Insurance won’t pay ransom

ALSO won’t pay for recovery

Total bill: $700k

Down time
IT co bills
IR team bills
Equipment replacement

1 Start

2

3

4

5 Finish

Lesson:

No incident is textbook

Ransomware Attack Avoided

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

IR Plan Wisdom

You should have one – top priority if you don't

Incident response plans **take work**, but there are plenty of templates to start with

Incident response plans should cover **more than IT**

Incident response plans should be tested **annually or even quarterly**

Have **your own relationship** with an IR Team

A good plan is **your plan**, not mine or anyone else's

You **are** going to have an incident – rodeo rule

Companies who **manage risk** holistically have fewer and less severe incidents

Cyber Insurance is **not a plan**

Basic Security Tips/Recommendations

Phishing/BEC

- **Add [EXTERNAL] to all inbound email subject lines**
- **Don’t click links, hover and validate location**
- **Establish procedure for when/how financial transactions are approved. Email can’t be the final say.**
- **Enable Sender Policy Framework**
- **Create a culture of security awareness**

Malware

- **Validate endpoint prevention tools are installed and updated**
- **Enable perimeter and prevention capabilities (on-prem and in the hyperscalers)**

Vulnerability & Config Management

- **Maintain a routine patch cycle, build a process for out of band patches/config changes.**
- **Understand vulnerabilities and prioritize risk**
- **Cloud adoption, understand the shared responsibility model**

Know Your Attack Surface (e.g.,)

- **Firewall Review**
  - External posture / attack surface before and after
  - Recent changes (get into change control/tracking)
- **Active Directory Review**
  - Review privileged group memberships
  - Validate appropriate audit configuration settings

Why Arctic Wolf?

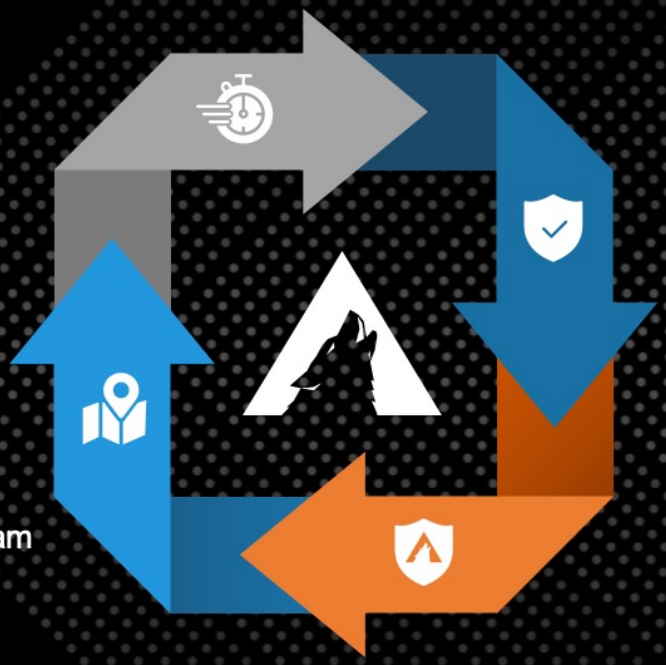
Our innovative Security Operations platform and concierge delivery model enable you to end Cyber Risk

Time to Value

- Leverage existing investments
- Add resources & expertise to your team
- Reduce noise & drive efficiency

Guidance

- Concierge Security Team
- Framework tailored to your environment
- World-class expertise on-demand

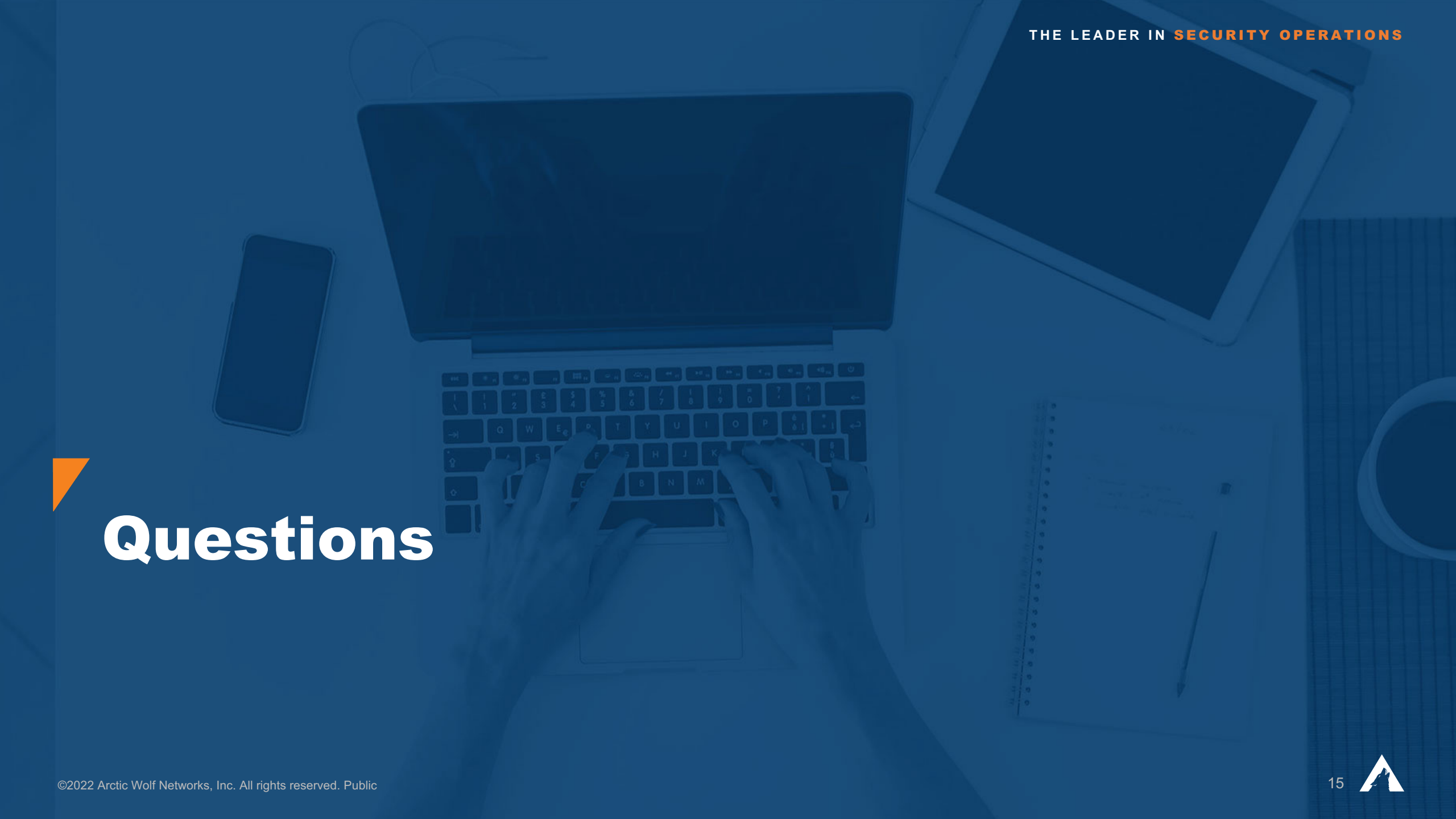


Protection

- Against commodity & advanced threats
- Attack surfaces
- All-the-time (24x7)

Resilience

- Proactive risk mgt
- Continuous posture assessment
- Sustained compliance



Questions

Thank You

Resources:

Arctic Wolf
- www.arcticwolf.com

FRSecure.com
- IR Template
- Security Policies
- LOTS of content
- CSIRT@FRSecure.com
- IR Risk Registration
- CISSP Mentor Program