SOC for All: Making SOC a Priority for Businesses of All Sizes

Charlie Otis
Senior Enterprise SE
Arctic Wolf

Andrew Roberts
Chief Cybersecurity Strategist
cStor

cStor: AN AWARD-WINNING PROVIDER

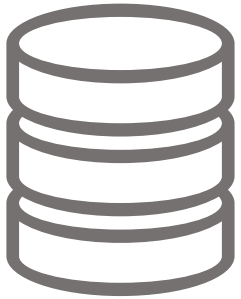
- Helps clients solve tough IT challenges with best-of-breed technology and expert consulting
- Creates and implements end-to-end solutions to fit your business needs
- Helps create a cost-effective architecture
- Displays a competitive advantage over other providers
- Creates flexibility by offering vendor agnostic solutions
- Always puts clients first

SOLUTION OFFERINGS

Professional Recommendations to Ensure Your Infrastructure Evolves Alongside Your Business

DIGITAL TRANSFORMATION

CYBERSECURITY



DATA CENTER SOLUTIONS

cStor

OUR APPROACH

Our mission is to put people on a path to success

Clients First

Vendor Agnostic

Highly Specialized

cStor SERVICES

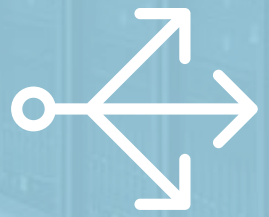
CONSULTING AND OPTIMIZATION

STAFF AUGMENTATION

DELIVERY

CYBERSECURITY

CLOUD



DATA MIGRATION

MANAGED SERVICES

SOC for All: Making SOC a Priority for Businesses of All Sizes

Charlie Otis
Senior Enterprise SE
Arctic Wolf

END CYBER RISK

Cybersecurity should reduce cyber risk

87%

of security leaders believe their organizations is falling short in addressing cyber risk.

Source: IDG Security Priorities Study 2020

Cybersecurity has an **effectiveness** problem.

Some Observations

Why aren't security leaders feeling confident?

LIKELIHOOD OF AN INCIDENT

IMPACT OF AN INCIDENT

59%
Organizations breached in a year

40 days
Increase to patch 'critical' vulnerabilities

$8.6M
Average cost of a data breach in the US

>200 days
Mean Time To Detect

The DIY SOC Approach

Where most companies want to be

GAP

Where most companies are today

Basic

Passwords / AD

Patch Management

Backups

Perimeter

Firewalls

SPAM / Web Filters

WAF/Proxy

Defense-in-Depth

Endpoint (AV, AEP)

DLP / SSL Inspection

Anti-DDoS/IPS/CASB

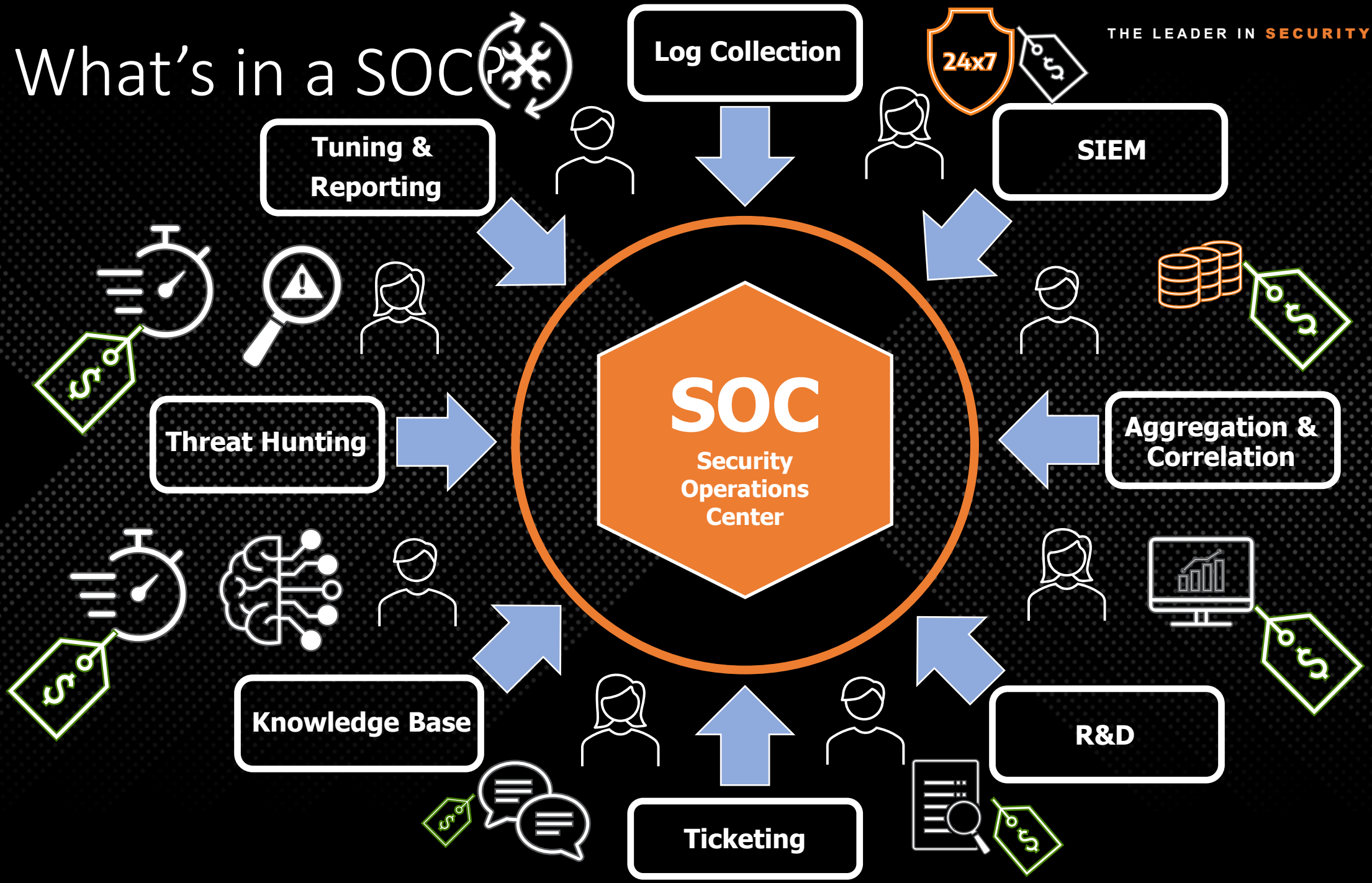
In-house Security Operations Center

Continuously Improve Security Posture

Policy Update

Speed-up Remediations

What's in a SOC?



The Pain Points We Hear

Broad Visibility

24x7 Coverage

Access to Expertise

Strategic Guidance

Compliance

Switch your thinking from a tools mindset to an operational mindset

Optimize

Optimize your existing tech stack and send to the cloud

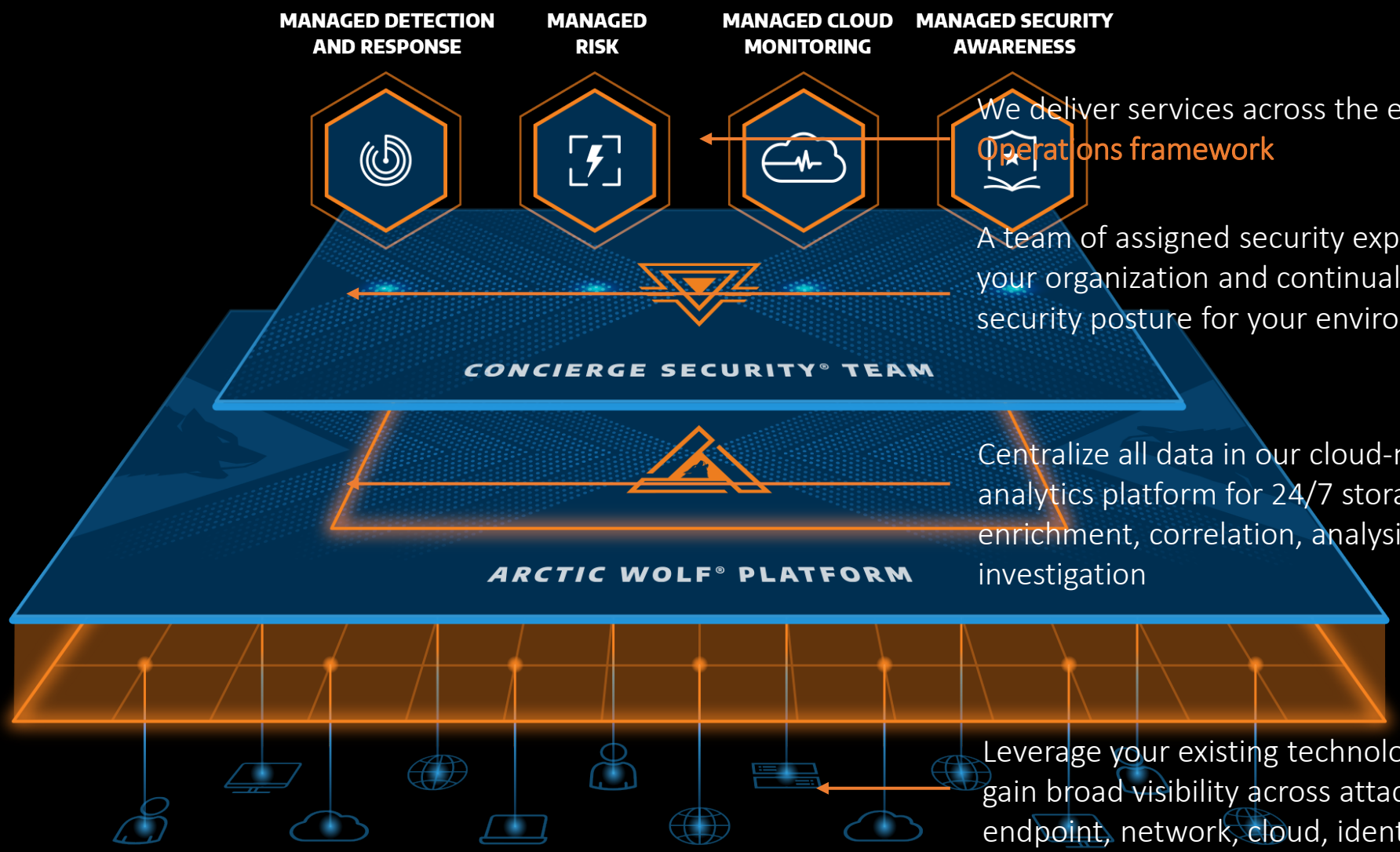
Embrace Security Operations

Focus on a complete security operations framework with broad coverage across attack types and attack surfaces

Build Resilience

Add expert guidance, 24x7 protection, and implement tactical and strategic actions across the security operations framework

Arctic Wolf Platform

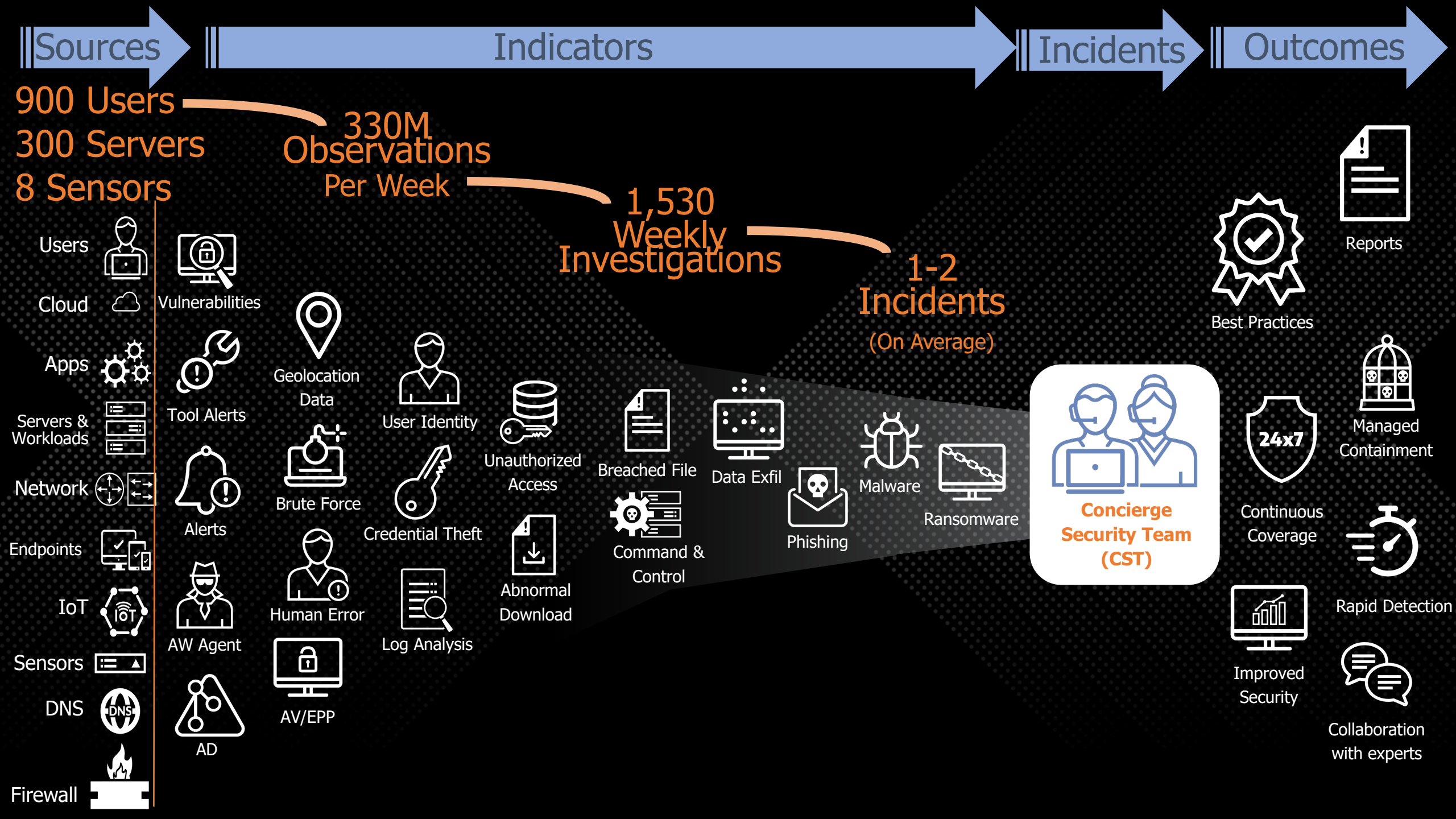


We deliver services across the entire Security Operations framework

A team of assigned security experts who learn your organization and continually optimize your security posture for your environment

Centralize all data in our cloud-native security analytics platform for 24/7 storage, enrichment, correlation, analysis and investigation

Leverage your existing technology stack to gain broad visibility across attack surfaces: endpoint, network, cloud, identity & human


Sources
Indicators
Incidents
Outcomes
900 Users
300 Servers
8 Sensors
330M Observations Per Week
1,530 Weekly Investigations
1-2 Incidents (On Average)
Users
Cloud
Apps
Servers & Workloads
Network
Endpoints
IoT
Sensors
DNS
Firewall
Vulnerabilities
Tool Alerts
Alerts
AW Agent
AD
Geolocation Data
Brute Force
Human Error
AV/EPP
User Identity
Credential Theft
Log Analysis
Unauthorized Access
Abnormal Download
Breached File
Command & Control
Data Exfil
Phishing
Malware
Ransomware
Concierge Security Team (CST)
Reports
Best Practices
Managed Containment
24x7
Continuous Coverage
Rapid Detection
Improved Security
Collaboration with experts

[REAL] INCIDENT TIMELINE
Ransomware

Ransomware Attack at [redacted]

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

Key Takeaways

Attack Type

Ransomware Attack

Time to Detect

5:23am - 5:28 pm | 5 Minutes

Data Sources

Active Directory
Arctic Wolf Sensor

[REAL] INCIDENT TIMELINE
Business Email Compromise

Email Compromise at [redacted]

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

Source: Duo

The Arctic Wolf Platform logs MFA successful for [User1]

12:57 pm

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.

Source: Office 365 Logs

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

1:16 pm

1:18 pm

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

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

1:22 pm

1:25 pm

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

- Customer confirms [User1] compromise
- Customer disables account

1:25 pm

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.

Key Takeaways

Attack Type

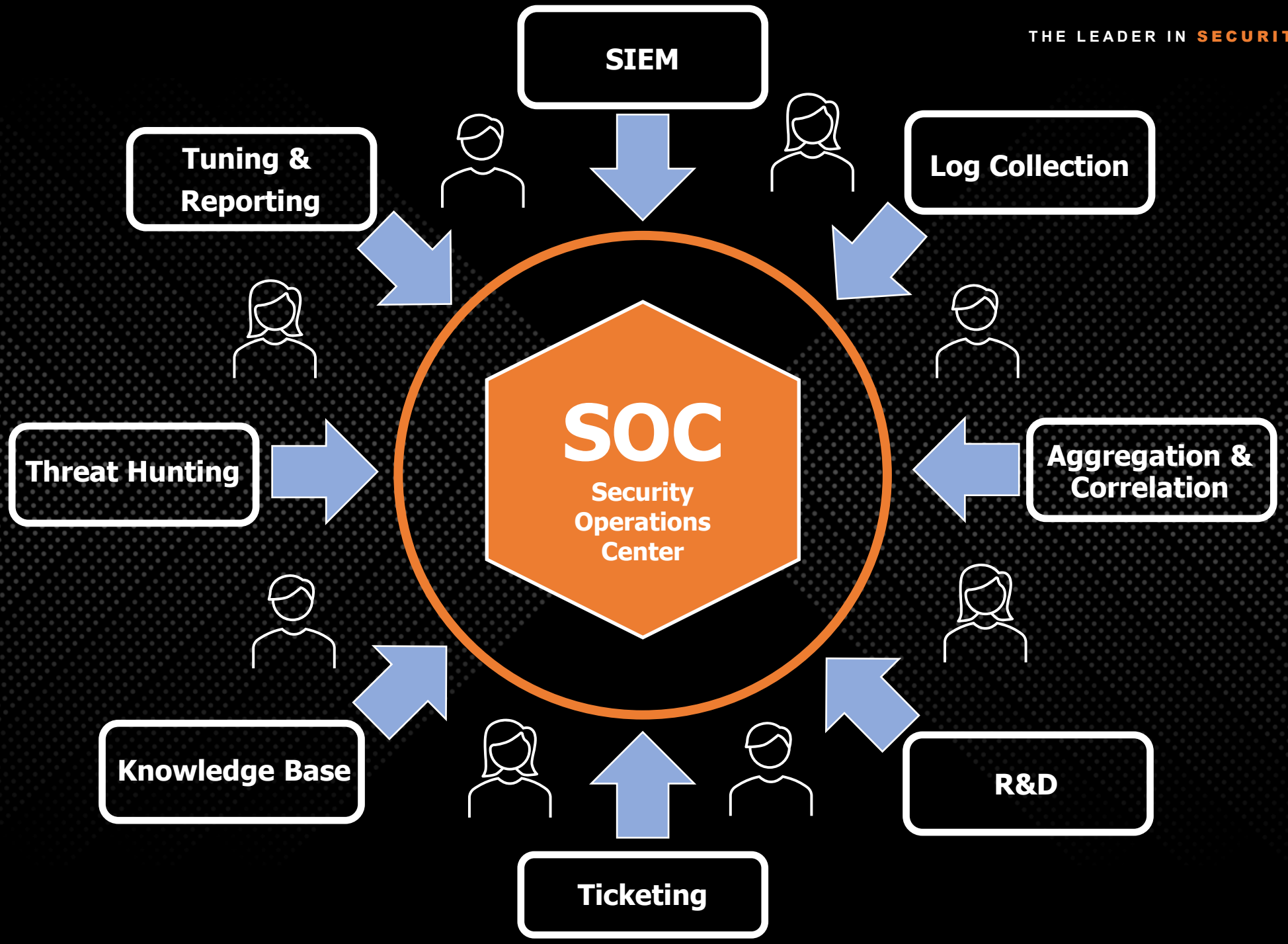
Email Account Takeover

Time to Detect

12:57pm - 1:16pm | 19 Minutes

Data Sources

Office 365
Duo

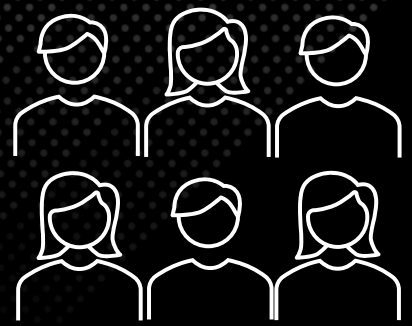

SIEM
Log Collection
Aggregation & Correlation
R&D
Ticketing
Knowledge Base
Threat Hunting
Tuning & Reporting
SOC
Security Operations Center

Cost for a SOC

- SIEM
- R&D
- Log Collection
- Threat Hunting
- Aggregation & Correlation
- Knowledge Base
- Tuning & Reporting
- Ticketing

= Cost for tools, subscriptions, PS for implementation, and 12-24 months to deploy

24 x 7 x 365



= Salary cost for 6+ dedicated security specialists; plus, payroll taxes, PTO, benefits, etc …

Arctic Wolf cost

SIEM

R&D

Log Collection

Threat Hunting

Aggregation & Correlation

Knowledge Base

Tuning & Reporting

Ticketing

24 x 7 x 365

Arctic Wolf augments what you already own!

Where most companies want to be

Arctic Wolf Security Operations bridges the gap

GAP

Where most companies are today

Basic

Passwords / AD

Patch Management

Backups

Perimeter

Firewalls

SPAM / Web Filters

WAF/Proxy

Defense-in-Depth

Endpoint (AV, AEP)

DLP / SSL Inspection

Anti-DDoS/IPS/CASB

Manage Detection And Response (MDR)

Log Aggregation & Correlation

Human / Threat Intelligence

Incident Detection & Response

In-house Security Operations Center

Continuously Improve Security Posture

Policy Update

Speed-up Remediations

Managed Risk

Discover – Benchmark - Harden

- Know when you're exposed and prioritize security posture improvements
- Continuously scan your networks, endpoints, and cloud environments to quantify digital risks.
- Concierge Security Team works directly with you to discover risks beyond simple vulnerabilities, benchmarks the current state of your environment, and implement risk management.

Managed Awareness

Improve Protection

- Prepare employees to recognize and neutralize social engineering attacks, like phishing.

Strengthen Resilience

- Empower employees to identify cyber risks and report mistakes that could expose sensitive data.

Achieve Compliance

- Deliver security awareness training for regulatory compliance.

Managed Detection & Response

Detect - Respond - Recover

- Leverage your existing tech stack to identify advanced network, endpoint, and cloud threats
- 24x7 coverage and guided response stops threats before they can do harm
- Find root cause, validate remediation, and collaborate to continuously improve your overall security posture

Concierge Security Team

Personalized Digital Risk Management that discovers more, benchmarks against industry trends, and tailors' protection to strategically harden your security posture over time.

Detection and response tailored to the specific needs of your organization that eliminates alert fatigue and false positives to promote a faster response

Predictable Pricing

Users

- ✓ Knowledge Workers / Mailboxes
- ✓ SaaS Applications

(*NOT* endpoints!)

Servers

- ✓ Physical & Virtual
- ✓ On-prem or Cloud

(*NOT "Log Sources"*!)

Sensors

- ✓ One per Internet Ingress/Egress (Firewall)

(*NOT "GB/day" "EPS" or Incidents!*)

ARCTIC WOLF

cStor

Questions?

ARCTIC WOLF

cStor

We look beyond IT

Thank You!