ARCTIC WOLF

Day in a Life of

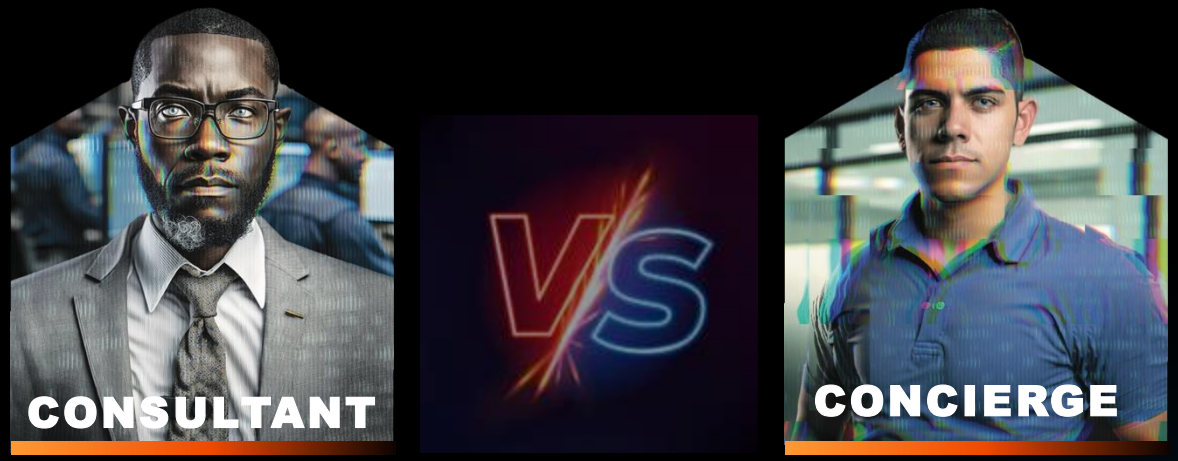
Arctic Wolf EMEA

Ing. Maurice Leon B.Eng.

Concierge Delivery Model

What Can You Expect?

Concierge VS. Consultant



- < 3 Customers
- Project driven
- Individual
- Focus on one topic
- Specialist

- > 30 Customers
- Project independent
- Vendor neutral
- No sales goals
- Works in a team
- Trusted Advisor for **all** Cyber Security topics

Concierge Delivery Model

- Ensure your environment is set up and ready for service

- Strategic advice
- Advance your security posture with SPiDRs

- 24x7 Event Triage
- Security Investigations
- Guided Remediation

- Business restoration when severe incident declared
- Digital Forensics

PLATFORM

SUPPORTING TEAMS

CSM
Business Outcomes

GTO
Availability and Support

AW Labs
Threat Research

How we interact with you

…or, it's a journey…

SCHEDULED INTERACTIONS

- Best Practices
- Service Customisation
- Risk Assessments
- Posture Improvement

Ad-Hoc

- Tickets
- Advice and Support
- Ad-Hoc Calls
- Mega Incidents

5

Security Journey Example

Customization Focus Steady-State Focus Detour/Ad-hoc Focus

Initial Focus

First 90 Days Initialization

- Concierge Kick-off
- SPiDR - Architecture review and initial tuning
- SPiDR - Health Validation

Q1 Focus

- Account Review
- SPiDR - External and Visibility Assessment
- SPiDR - Cloud Visibility Assessment

Q2 Review

- Account Review
- SPiDR - Password Policies, Managers, and Security Awareness
- SPiDR - Cloud Configuration Deep Dive

Q3 Focus

- Account Review
- SPiDR - Firewall Configuration Review
- SPiDR - Endpoint Configuration Review

Detour: Ransomware Attack

- SPiDR - Customer Incident Report
- SPiDR - Architecture and Visibility Assessment
- SPiDR - Anomalous Traffic Analysis
- SPiDR - Ransomware and Malware Hardening

Q4 Focus

- Account Review
- SPiDR - Active Directory Services Review
- SPiDR - Anomalous Traffic Analysis

Detour: Emerging Threat

Arctic Wolf Intelligence team will actively notify and initiate detour when new exploits or emerging threats arise in industry

Example SPiDRs:

- Identified Security Gap
- Commonly Exploited CVE review
- Zero-Day Threat Hunting review

Arctic Wolf SonicWall Mega Response

22nd August 24

On August 22nd, 2024, SonicWall released details about CVE-2024-40766

26th August 24

Initial Security Bulletin sent targeted to customers

28th August 24

SonicWall expanded the scope of the vuln to include SSLVPN where it was previously just management access

6th September 24

SonicWall Confirmed Exploitation, Internal Tipper and Follow-up Security Bulletin released

9-11th September 24

TIO started investigating and tracking cases, coordinated support from TIR and IDR for IDD Detections

12th September 24

Threat Event met level 2 – high severity based on potential versus actual and S2 responds with all region tickets to potential customers and tiger team stand up

Detections

- 1 ASN detection deployed
- 1 Mid Kill Chain Detection Deployed

13th September 24

CST Callouts made to customers found to be at higher risk of being vulnerable

14-15th September 24

cSOC monitors for any/all customer responses in connection to CVE over the weekend

16th September 24

Mega called to a close

- 1 Additional Late Kill Chain detection deployed; ASN detection updated with CISA shared findings

Assess your Cyber Risk: Cyber Resilience Assessment

Advance cyber resilience by assessing an organisation's posture against industry-standard frameworks

Available to: All Arctic Wolf Customers

The Arctic Wolf Cyber Resilience Assessment enables customers to proactively expose and mitigate risks in their security posture to better protect their organization from cyber risk

Use Cases and Outcomes

- Measure against industry standard frameworks, such as: CIS Critical Security Controls v8 and NIST CSF 1.1
- Leverage insights from the assessment to address gaps in security posture and track progress over time as mitigations are completed
- Identify and prioritize highest impact capabilities to mitigate risk
- Insurability rating enables organizations to identify and address risks in their security posture to reduce risk profile and improve insurability

Security Focus Planner

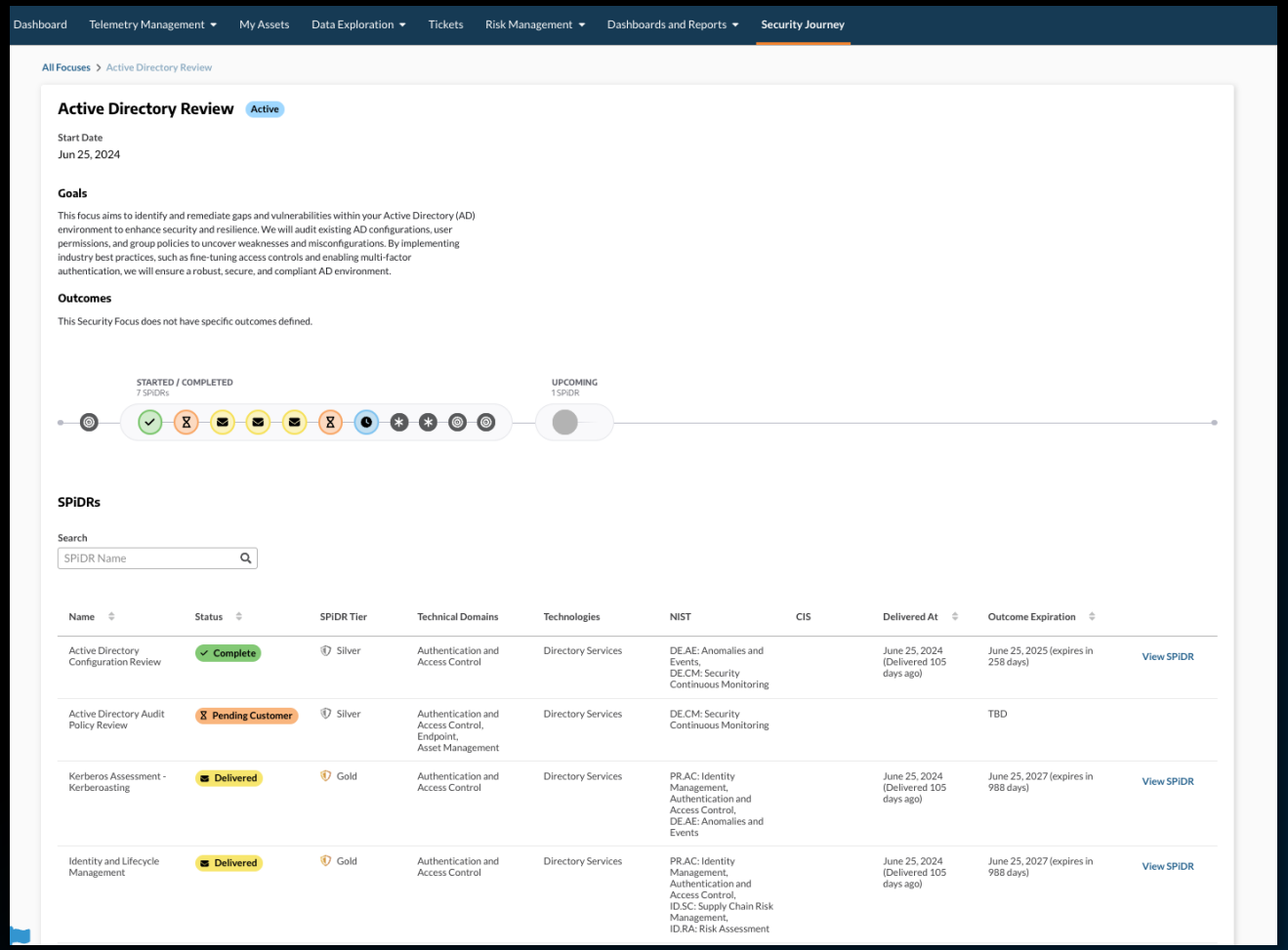
Collaboratively strengthen your cyber security posture with the Concierge Security Team by reviewing your strategic plan with Security Focus Planner

Applicable for: MDR, MR

The Security Focus Planner brings visibility into which Security Posture in-Depth Reviews (SPiDRs) are completed and planned with a customer's Concierge Security Team (CST).

Use Cases and Outcomes

- Unlock visibility into a Security Focus so customers can discuss and prioritise posture hardening activities with their Concierge Security Team based on their security needs
- Access the roadmap of past and future posture assessments, reviews, and related activities and easily track the benefits of accessing of up to ~150 proactive hardening activities
- Capture and share a record of the completed objectives in one easy-to-view dashboard and reports



Podcast

Wolfshöhle

Arctic Wolf Networks Germany

Folgen • • •

Alle Folgen

NIS2 - Europas Cyber-Schutzschild

Wolfshöhle

In dieser Episode unseres Podcasts haben wir einen herausragenden Gast: Malte Wannow, einen angesehenen Experten für Cybersicherheit. Gemeinsam mit Malte begeben wir uns auf eine informative...

17. Jan. · 35 Min. 36 Sek.

Insider-Einblicke - Die Welt des Cyber Security Recruitings mit einem Headhunter

Wolfshöhle

In dieser Folge geht es um das Thema "Headhunter für den Cyber Security Bereich". Mit der

Informationen

Ob Script-Kiddies, finanziell motivierte Cyber-Krim
oder politisch motivierte Akteure: Unternehmen we
heutzutage von sehr unterschiedlichen Angreifern
attackiert – und jede Angreifergr

... Mehr anzeigen

5 ☆ (7)

Technologie