Cybersecurity Defense in Depth: A Real-Life Case Study

Presented by

Nikola Stojsin, CIO, PhD CCIE # 12888

Security Evolution at ACME Company

1

Foundation

In 2019, ACME Company established a robust security posture.

2

Upgrades

Recent security infrastructure improvements (2024-2025) enhanced protection capabilities.

3

Validation

Latest incidents provided real-world validation of security measures.

4

Current State

Defense-in-depth strategy now actively protects against multiple threat vectors.

Supplemental Defense Layers

Arctic Wolf 24/7 Monitoring

Continuous surveillance of all endpoints, devices, and cloud services.

Active Directory Restriction Policies

Prevents unauthorized software installation in user profiles.

Alternate-Vendor IDS

Secondary intrusion detection system provides redundant protection.

Zero-Ports-Open Policy

Strict network access control at all perimeter devices.

Arctic Wolf Protection Layer

24/7/365 Monitoring

Continuous surveillance of all network endpoints, devices, and services.

Cloud Integration

Comprehensive monitoring of Microsoft 365, Mimecast, Duo, and other services.

On-Premises Hardware

Network anomaly detection security appliance provides local threat intelligence.

Endpoint Protection

In addition to EDR/XDR (SentinelOne), an additional security agent is installed on all endpoints for enhanced protection.

Active Directory Security Controls

Profile Protection

Blocks software installation attempts within user profiles and prevents users from installing unauthorized software or drivers.

Multi-Factor Authentication

A cost-effective strategy against brute-force attempts.

Vector Elimination

Minimizes end users as as potential malware vectors.

Perimeter Defense Strategy

Alternate-Vendor IDS

Intrusion Detection System module operates through Cisco Firepower device.

Monitored by Arctic Wolf for additional oversight.

Zero-Ports-Open Policy

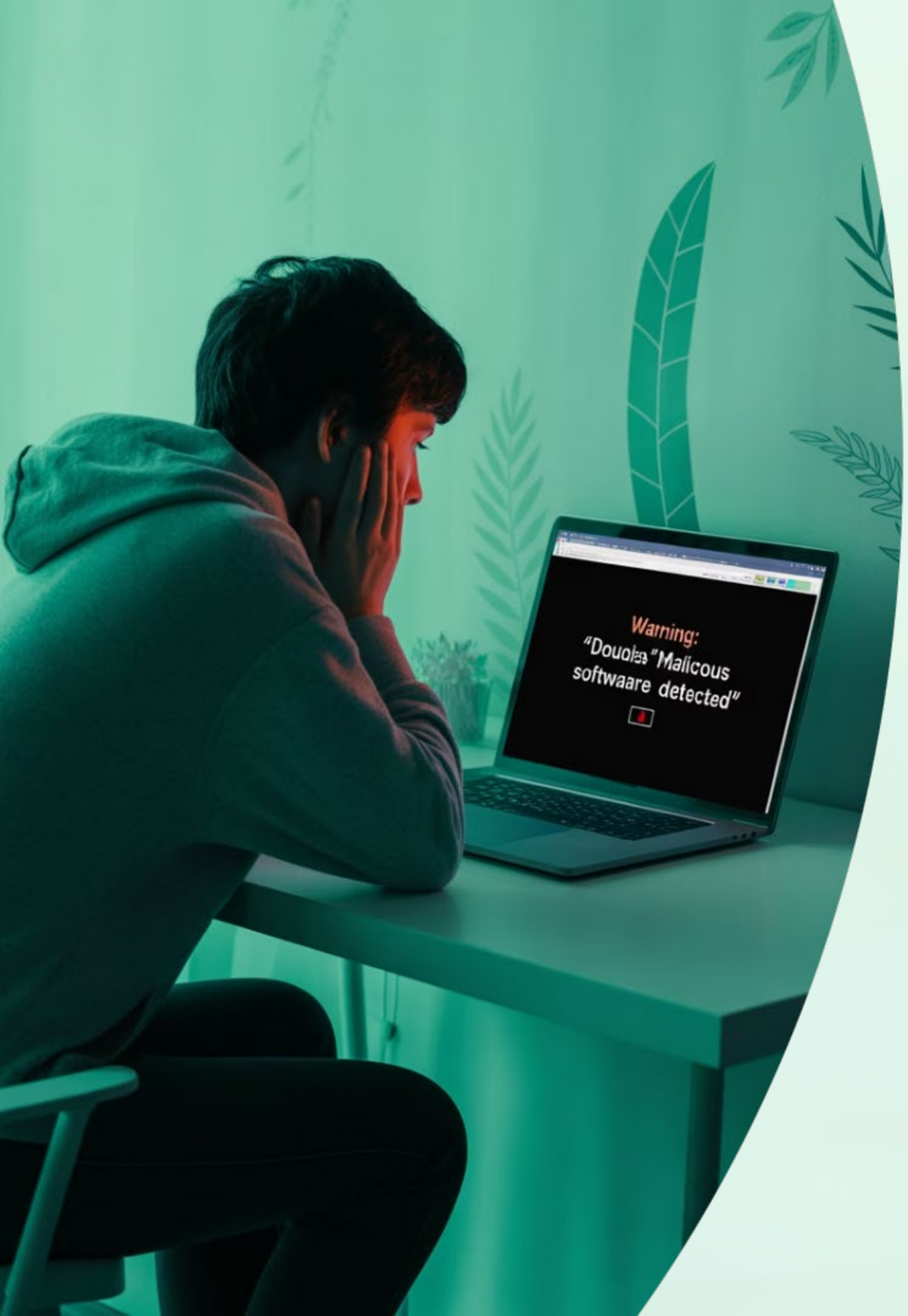
All perimeter devices operate with strictly closed ports.

Multi-factor authentication required for for VPN access.

Standard Protocols

Multi-factor authentication deployed across systems.

Sentinel One (S1) protection on all endpoints.



Incident Timeline: Initial Compromise

9:30 PM, April 26, 2025

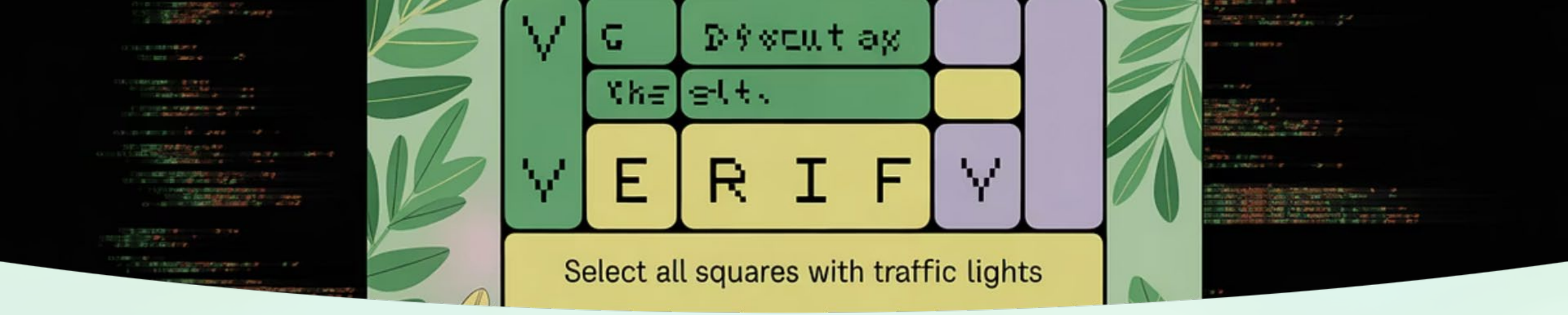
Remote employee accesses laptop after business hours.

NHL Playoff Search

User searches for free streaming site to watch hockey game.

Malicious Site Encounter

User unknowingly navigates to compromised streaming website.



Attack Vector: Fake CAPTCHA

Deceptive Interface

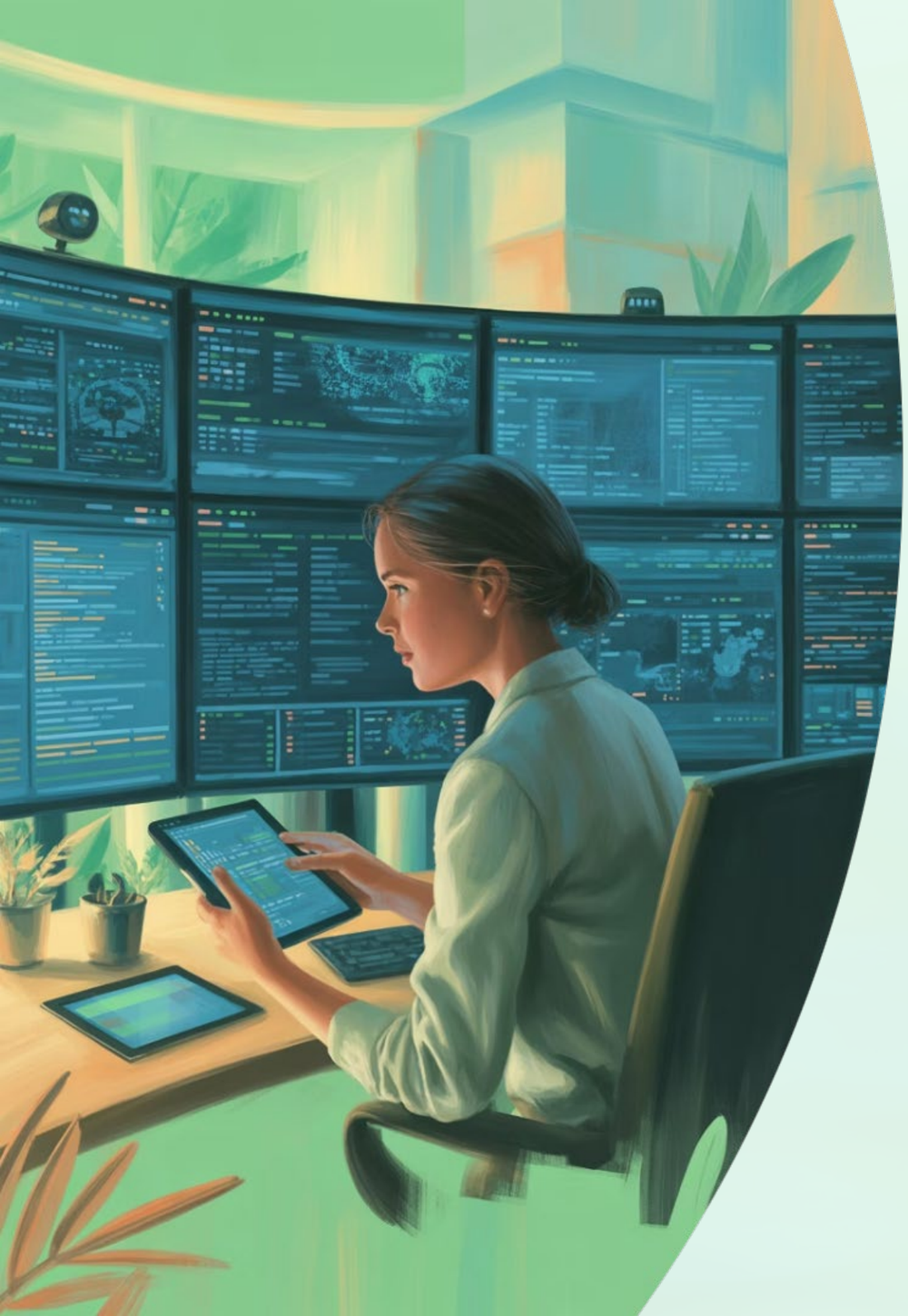
User encounters convincing fake CAPTCHA challenge on streaming site.

User Interaction

Employee completes the fake verification verification process, triggering hidden code.

Attack Launch - 9:38 PM

Site attempts remote script execution targeting privilege escalation.



Arctic Wolf Response

1

9:38 PM - Detection

Arctic Wolf agent intercepts and blocks the remote script execution attempt.

9:38 PM - Alert

Agent notifies Arctic Wolf Security Operations Center of the incident.

9:39 PM - Containment

SOC engineer remotely disables the compromised laptop.

9:39 PM - Notification

Arctic Wolf engineer calls security contact's mobile number.

ACME Company Incident Response

Response Plan Activation

Cybersecurity incident response procedures initiated immediately.

Account Lockdown

All user’s accounts disabled as precautionary measure.

Device Quarantine

Laptop powered off and shipped to ACME Company's office for analysis.

User Contact

Employee contacted by phone for instructions and interview.

Incident Analysis & Findings

No Compromise Confirmed Confirmed

Thorough investigation determined determined no successful breach occurred.

AD Policy Validation

Analysis confirmed Active Directory policies would have blocked payload installation.

S1 Detection Capability

Testing showed Sentinel One would have identified payload file as malicious.

Defense-in-Depth Benefits

3+

Protection Layers

Multiple security systems provide redundant protection.

0

Data Breaches

Serious security incident contained with with no compromise.

99.9%

Uptime

Recent S1 outage became a non-event event due to layered security.

Conclusion

1. Learn from past experience
2. Defense in Depth
3. Incident Response Plan

Questions?

Contact Information

Nikola Stojsin

nikolas@networkmakers.com