

AI as a Force Multiplier in a Wartime SOC

Yevhenii Zhuk

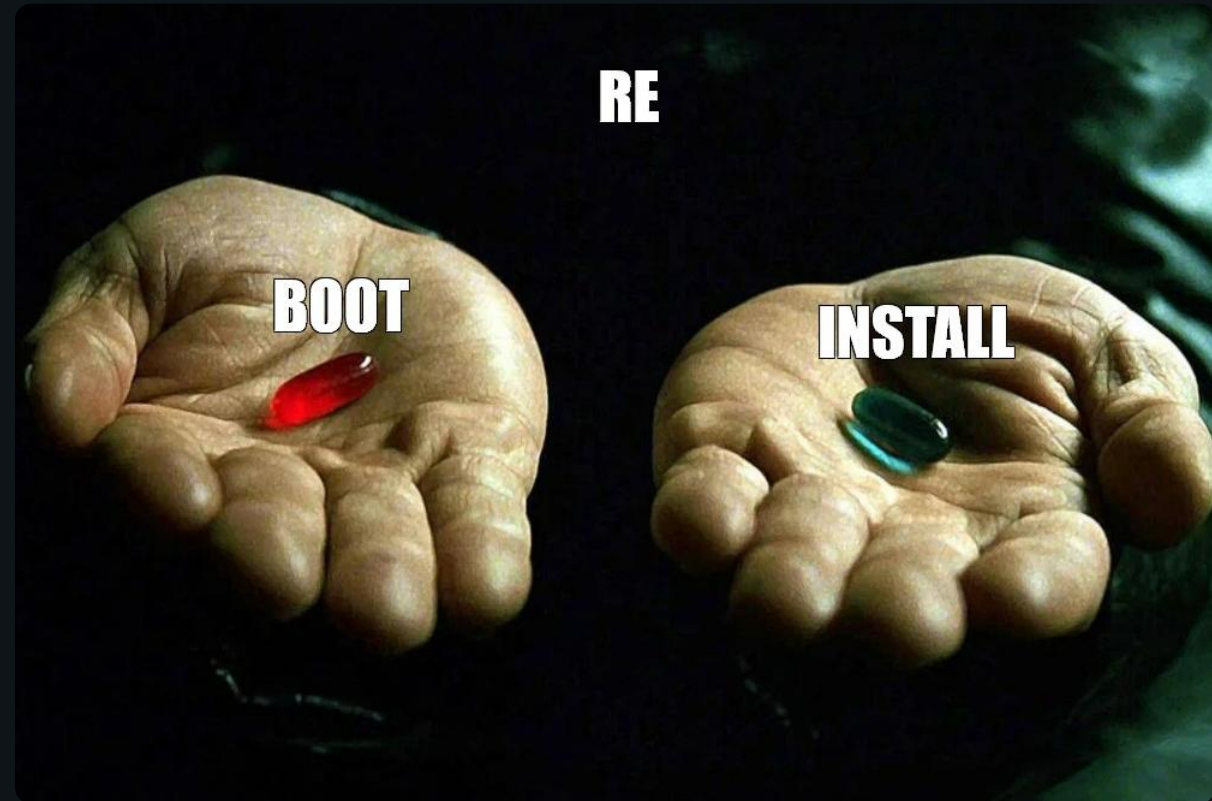
Lead Information Security Analyst

VENDOR SUPPORT

What vendor support looked like



The average vendor support agent



...and when they finally reply

What we fixed without the vendor

SYMPTOM	ROOT CAUSE	WHAT WE DID WITH AI
No analytics after first deployment	UI time range locked before 1970; ANALYTICS_METADATA table and relation_tags index missing; OERMC empty	Created the missing table and index by hand; populated OERMC with file-access events (4663, 4656, 5145)
Dashboard frozen on old dates	~1.25M events a day arrived, but analytics tables stayed empty and no behavioral baseline was built	Traced the pipeline pod by pod, checked clocks across pods, forced analytics runs
No events ingested for 11 days	TH routing lived in ephemeral storage and vanished on pod restart; a stuck Kafka COPY locked a Vertica table	Rebuilt the TH routing config by hand, killed the stuck COPY, restarted Vertica and the Kafka scheduler
Proxy events never reached UEBA	Intelligence connector filter passed only Microsoft Windows events; the proxy loader knew nothing about McAfee	Rewrote the connector filter, added McAfee vendor and product strings to the proxy loader SQL
Failures noticed only days later	No built-in alerting on ingestion gaps or disk growth;	Wrote our own health checks: last event time, Kafka scheduler state, disk usage;

Analytical skills assessment



SIEM Analysis Training

Security Event Investigation

Total Events: 25

Analyzed: 0

Remaining: 25

Time Remaining: 37:35

Timestamp	Severity	Event Type	Description	Source IP	Destination	Status
09/29/2026 21:19	HIGH	File Download	File downloaded from internet	192.168.1.89	94.232.47.156	PENDING
09/30/2026 00:40	MEDIUM	USB Device	USB device connected	192.168.1.98	192.168.1.98	PENDING
09/30/2026 05:22	MEDIUM	Network Connection	Outbound connection established	192.168.1.157	185.220.101.42	PENDING
09/30/2026 05:13	HIGH	DNS Query	DNS resolution request	192.168.1.112	192.168.1.15	PENDING
09/30/2026 16:03	HIGH	Process Execution	Process started	192.168.1.223	192.168.1.223	PENDING
09/30/2026 10:54	LOW	VPN Connection	Remote connection established	203.0.113.45	198.51.100.10	PENDING
09/30/2026 07:39	HIGH	DNS Query	DNS resolution request	192.168.1.203	45.61.136.207	PENDING
09/30/2026 06:25	MEDIUM	User Authentication	Remote login recorded	45.32.101.23	192.168.1.210	PENDING
09/30/2026 08:47	MEDIUM	Software Installation	Application installed	192.168.1.122	192.168.1.122	PENDING
09/29/2026 19:45	MEDIUM	File Access	File system access recorded	192.168.1.198	192.168.1.220	PENDING
09/30/2026 10:30	MEDIUM	Web Request	HTTP request to external server	192.168.1.87	52.97.145.162	PENDING
09/30/2026 01:15	MEDIUM	Physical Access	Badge access recorded	192.168.1.45	192.168.1.210	PENDING
09/30/2026 10:02	HIGH	Process Execution	Process started	192.168.1.78	192.168.1.78	PENDING
09/30/2026 09:33	MEDIUM	Authentication Failure	Login attempt failed	192.168.1.167	192.168.1.210	PENDING
09/30/2026 10:20	MEDIUM	Network Connection	Outbound connection established	192.168.1.156	13.107.42.14	PENDING
09/29/2026 21:02	HIGH	Email Attachment	Email attachment processed	192.168.1.145	192.168.1.250	PENDING
09/30/2026 09:34	MEDIUM	Web Request	HTTP request to external server	192.168.1.178	198.12.75.112	PENDING
09/30/2026 03:52	MEDIUM	USB Device	USB device connected	192.168.1.67	192.168.1.67	PENDING

Application installed

Severity: MEDIUM | Type: Software Installation | 09/30/2026 08:47

Malicious

Suspicious

False Positive

Event ID

2w028w0zp

Source IP

192.168.1.122

Destination IP

192.168.1.122

Destination

localhost

Hostname

WS-MARKETING-05

Username

ACMECORP\jennifer.white

Application

uTorrent BitTorrent Client

Installer Path

C:\Users\jennifer.white\Downloads\uTorrent.exe

Installation Time

14:22:15

Version

3.5.5.45852

Hash Md5

8f14e45fcee3167a5a36dedd4bea2543

Raw Logs

[2024-06-12 14:22:15] Installation initiated: uTorrent BitTorrent Client [2024-06-12 14:22:16] User approval p
rompt displayed [2024-06-12 14:22:18] Installation completed

Raw Event Data

Click to expand

New Training Session

Company Documentation

Investigation Tools

ACMECORP Security Documentation

Company Overview

ACMECORP Inc. is a mid-size technology consulting firm founded in 2010, specializing in digital transformation and cloud solutions.

We employ 35 staff across 3 locations:

HQ: New York (28 employees) - Executive, Sales, Marketing, Finance
Tech Hub: Austin (10 employees) - Development, DevOps, IT Operations
EU Office: London (2 employees) - European sales and support

Business Hours: Monday-Friday 0800 - 1800 local time

Remote Work: Hybrid model - employees work remotely 2-3 days per week

Access Control Policy

Database Access

- Database Admins (incl. backup, development)
- Finance Team (customer billing, data only)
- HR Team (employee records only)
- Security Guards, Contractors, interns
- Outside business hours without approval

Physical Access

- Employees 0800 - 2200
- Security Guards 24/7
- Cleaning Crew 2200 - 0600
- Contractors after hours
- Visitors without escort

Approved USB Device IDs

- ba67810d5047 (Sparkle Corp. Laptop)
- ba69303d4543 (Roshini Corp. USB3.0)
- ba60911d1f446 (Plington Data/Traffic)
- ba13912d4209 (Insanity Secure USB)
- Non-encrypted devices

Approved Applications

- Microsoft Office Suite
- Adobe Creative Cloud (Design team)
- Slack (Business communications)
- Zoom (Video conferencing)
- Visual Studio Code (Development)
- Chrome, Firefox, Edge browsers
- FTP file sharing software
- Cryptocurrency miners
- Remote access tools (non corporate)

Employee Access Matrix

Employee	Department	Role	Database Access	Admin Rights	Physical Access	Work Schedule	Remote Access
James Wilson	Executive	CEO	Executive Dashboard	Full	24/7	Flexible	Authorized
Sarah Martinez	Executive	CTO	Technical Systems	Full	24/7	Flexible	Authorized
Tom Rogers	IT	IT Administrator	All Systems	Full	24/7	0800-1800	Authorized
David Wilson	IT	Network Admin	Network Logs	Network	Business Hours	0800-1700	Authorized
Mike Chen	IT	DevOps Engineer	Application Logs	Limited	Business Hours	0800-1800	Authorized
Peter Johnson	IT	Senior DevOps	Application Logs	Limited	Business Hours	0500-1800	Authorized
Kevin Park	IT	System Administrator	Server Logs	Limited	Business Hours	0800-1700	Authorized

Administration skills check

System Preparation Tasks

Cluster Troubleshooting

Help

CentOS System Preparation Guide

Overview

Prepare a CentOS 7.9 system for enterprise platform deployment. Research and implement the required configuration changes.

System Prerequisites

- CentOS 7.9 minimal installation
- Minimum 16GB RAM, 8 CPU cores
- 500GB+ storage space
- Network connectivity
- Root access

Task 1: Configure Network & Firewall

Research and open the following ports for platform communication:

- SSH access (port 22)
- HTTP traffic (port 80)
- HTTPS traffic (port 443)
- Management interface (port 8443)
- Database connections (port 5432)
- Search engine (port 9200)
- Kubernetes API (port 6443)

Hint: Use `firewall-cmd` to manage firewall rules permanently.

Example: `firewall-cmd --add-port=80/tcp --permanent`

To complete: Open ALL 7 required ports with `--permanent` flag, then run `--reload` to apply changes

Task 2: Create & Configure Swap

Platform requires 8GB swap space. Research how to:

- Create a swap file using `dd` command
- Set proper permissions (600)
- Initialize the swap file
- Activate the swap
- Make it persistent across reboots

Training Terminal

Training Environment - Local Connection

ACME Corporation - Infrastructure Training

Welcome to the enterprise infrastructure training environment. This simulation provides hands-on experience with:

- CentOS system administration and preparation
- Kubernetes troubleshooting and debugging
- Security incident investigation (CTF challenges)

Type 'start' to begin training or 'help' for available commands.

acme-training@jumphost:~\$ start

ACME Corporation Training Program

Welcome to the Infrastructure Security Training Environment

Available Training Hosts:

- `prod-centos-01.company.local` - CentOS 7.9 system preparation
 - Configure firewall and network security
 - Setup swap, NTP, and system services
 - Install and configure enterprise platform
- `k8s-master-01.company.local` - Kubernetes troubleshooting
 - Investigate pod crashes and service issues
 - Debug storage and networking problems
 - Find hidden security flags in logs (CTF challenges)

Training Objectives:

- Master Linux system administration skills
- Learn Kubernetes troubleshooting techniques
- Develop security incident investigation abilities
- Practice with real-world enterprise scenarios

Connection Instructions:

```
ssh root@prod-centos-01.company.local    (System preparation)
ssh root@k8s-master-01.company.local    (Kubernetes troubleshooting)
```

Training environment initialized. Choose a host to begin:
acme-training@jumphost:~\$ |

Host: jumphost

Tasks: Not connected

Flags: 0/3 found

What we improved in SOAR

01

Round-robin assignment

Script in the SOAR database splits cases equally across analysts

02

AbuseIPDB context

Domain, ISP and number of reports now shown on the case

03

MISP enrichment fixed

False “no events” marker removed; threat level shown correctly

04

ipinfo.io enrichment fixed

Results now reach the case; Python compatibility bug fixed

05

Port-to-service lookup

New enrichment: which service most likely runs on a port

Five arenas, one ranked season

nyx_operator

Script Kiddie

0 pts

CYBER ARENA

RANKED PVP ARENA

SEASON 2

NAVIGATE

Home

Library

Knowledge Base

Users

OVERALL

RANKED

1

nyx_operator

YOU

0

CHOOSE YOUR ARENA

Welcome back, nyx_operator.

Duel a live target, fight to hold the hill, or take the analyst chair.



Attack / Defense

Breach or defend a live target, head-to-head.

role-swap

live



King of the Hill

Root the box and hold the crown against the field.

live

vs the field



Lab Race

Race an opponent to diagnose and repair a broken Kubernetes SOAR cluster — root shell on every node.

live

1v1



SOC Battle

ArcSight ESM event hunts and SOAR playbook duels — from the analyst chair.

ESM

SOAR



Watch Live

Spectate ongoing Attack/Defense and King of the Hill matches, read-only.

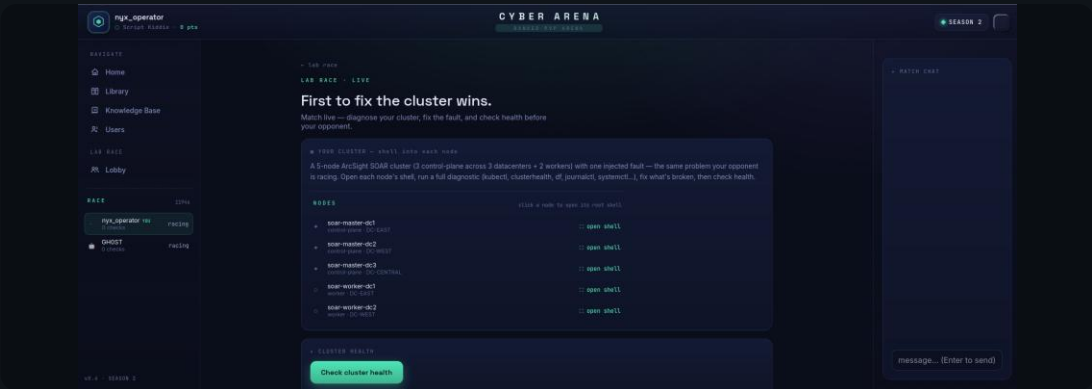
spectate

live

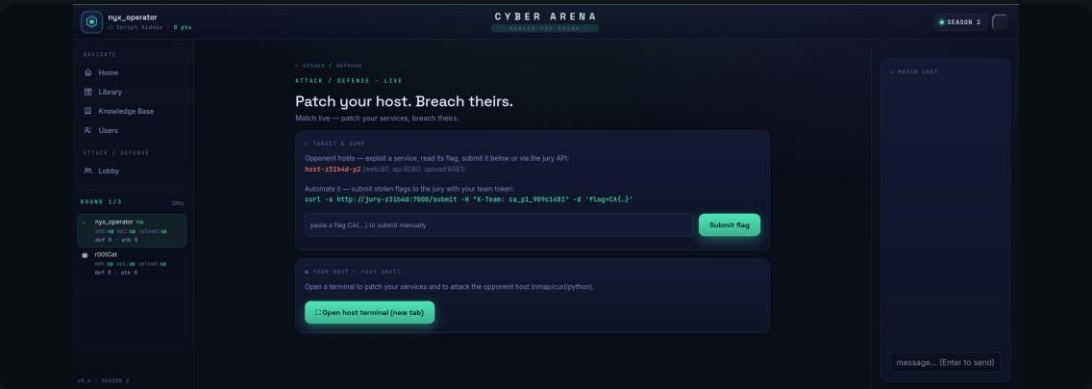
v0.4

SEASON 2

Training through competition



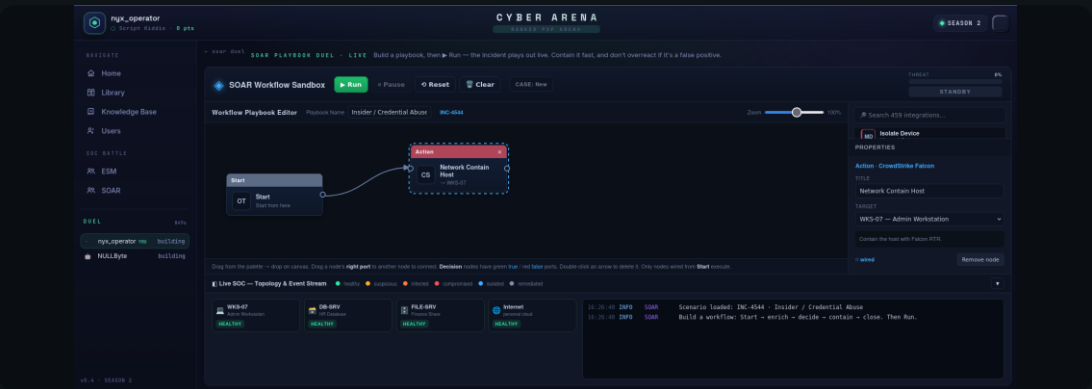
Lab Race: fix the broken SOAR cluster



Attack / Defense: patch yours, breach theirs



SOC Battle: ESM event hunt



SOC Battle: SOAR playbook duel

AI inside our SOAR

☆ Outbound Traffic to a Suspicious Address

Filter: All

+ Add New Scope Item

50002

178.251.109.237

50014

10.183.36.143

Bad Web Bot, P...

UDP

6 scope items

Q

1

New Case

Edit

Close

Enrich

Action

Execute

Case #843984

Open

High

Document

Rule name

Outbound Traffic to a Suspicious Address

MITRE ATT&CK Technique ID

T1095

Description

Automatically created alert case

Device Event Class Id

rule:102

File Path

/All Rules/Real-time Rules/Threat Intelligence Platform/Suspicious Activity/Outbound Traffic to a Suspicious Address

Alerts (1 total)

#131255116

Details

Network

Current Playbook: Network Traffic

Playbook execution started at 2026-09-30 15:14:32

Then

Add Case Label on ArcSight SOAR Integration

Check IP on AbuseIPDB

Identify Port Service on Port Service Identifier

Check IP on AbuseIPDB

Decision

Else

Analyst Decision

Progress

Show

10 All

Comments

Enrichments

Actions

Playbook Executions

Tasks

Others

«

<

1

>

»

⚙

A

2 minutes ago - A AI Assistant commented

AI Analysis Summary

Alert: Outbound Traffic to a Suspicious Address

Severity: Medium

Category: Suspicious Network Activity

Observed Activity:

Internal host 10.183.36.143 attempted outbound UDP communication from source port 50014 to external IP 178.251.109.237 on destination port 50002. The connection was blocked by the firewall (action=drop). Source zone: INSIDE Destination zone: OUTSIDE.

Additional Context:

The destination IP 178.251.109.237 has an AbuseIPDB confidence score of 21% and has been reported 67 times by 28 distinct reporters, with the latest report submitted approximately 1 week ago. Recent reports include Bad Web Bot, Port Scan, Hacking, Web App Attack, and Brute-Force activity. The IP belongs to Ultratnet Group LLC (AS35297), a fixed-line ISP network located in Ukraine. While the address has been associated with suspicious activity, the reputation score is relatively low and should be treated as contextual information rather than confirmation of malicious activity.

AI Assessment:

A single outbound connection attempt to an IP address with previous abuse reports was detected and successfully blocked by security controls. No evidence of successful communication, additional related alerts, malware activity, or endpoint compromise was identified from the available event data.

Conclusion:

The event appears to be an isolated blocked connection attempt to an IP address with an elevated reputation score. Since the traffic was prevented by the firewall and no additional indicators of compromise were observed, the activity is assessed as low risk. No further action is recommended unless additional correlated events or indicators are identified.

2 minutes ago - ot added watcher

A AI Assistant