IJARSCT

International Journal of Advanced Research in Science, Communication and Technology

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

ISSN: 2581-9429

Volume 5, Issue 3, April 2025

Impact Factor: 7.67

Cybercrescendo: Interactive Cybersecurity Virtual Lab for Real-Time Attack Simulation and Hands-On Defense Training

Prof. Pallavi Chandratre[1], Satyam Bhosale[2], Mayank Kamble[3], Mitesh Kamthe[4]
Faculty, Department of Computer Engineering[1]
Students, Department of Computer Engineering[2,3,4]
Shivajirao S. Jondhale College of Engineering, Dombivli East, Maharashtra, India

Abstract*: Traditional cybersecurity learning often falls short in offering realistic, hands-on experiences. Cybercrescendo: A Virtual Lab bridges this gap by recreating enterprise-level network environments using VirtualBox.It integrates systems like Windows Server with Active Directory and Ubuntu-based threat monitoring tools to simulate real-world IT infrastructures. Equipped with offensive and defensive tools like Kali Linux, Suricata, and Wazuh SIEM, the lab immerses users in real-time cyber scenarios, empowering them to explore threat hunting, incident response, and ethical hacking in a controlled, risk-free space.*

Keywords: Cybersecurity Training, Virtual Lab, Real-Time Attack Simulation, Network Defense, Ethical Hacking, Red Team Blue Team, Threat Detection, Incident Response, SIEM, IDS/IPS, Hands-on Security Learning

I. INTRODUCTION

Cyber threats today are increasingly complex, yet most training remains theoretical. Cybercrescendo: A Virtual Lab addresses this gap by simulating real-world enterprise networks, allowing users to practice both offensive and defensive cybersecurity skills. Like a flight simulator for cyber defense, it offers hands-on experience in threat detection, incident response, and system hardening—safely and interactively.

II. PROBLEM STATEMENT AND OBJECTIVES

Problem Statement

As cyber threats grow increasingly sophisticated, organizations face mounting challenges in protecting their digital infrastructures. Traditional cybersecurity tools, such as firewalls and antivirus software, often fail to detect modern attack techniques like advanced persistent threats (APTs), malware polymorphisms, and complex social engineering tactics. With evolving cyberattacks leveraging obfuscation methods and zero-day vulnerabilities, existing solutions can leave critical systems exposed. Additionally, the complexity of enterprise network environments and their interconnected systems further complicates detection and mitigation efforts.

Many organizations lack comprehensive, hands-on training environments that accurately simulate the breadth and variety of modern cyber threats. As a result, cybersecurity professionals often face difficulty in preparing for the diverse, real-world scenarios that could compromise an organization's security. This gap in training and preparedness emphasizes the need for a practical, scalable solution that enables thorough testing, threat detection, and response strategies in dynamic, real-world-like environments.

Objectives

Create a virtual lab that emulates realistic attacks such as port scanning, brute force, SQL injection, reverse shells, and privilege escalation within a controlled, isolated virtual network using tools like Nmap, Hydra, and Metasploit..

Provide a virtualized Security Operations Center (SOC) setup where learners can interact with tools like Wazuh and Suricata to monitor, detect, and analyze cyber threats in real-time.

DOI: 10.48175/IJARSCT-25058

To demonstrate the functionality of SIEM and endpoint detection systems, helping users analyze logs, detect anomalies, and understand system behavior during cyber events.

To promote cyber hygiene and awareness, reinforcing the need for proper configuration, timely patching, and continuous monitoring through practical lab exercises.

To use attack emulation techniques, including port scanning and basic exploitation attempts from Kali Linux, to assess and improve system security posture.

III. LITERATURE REVIEW

Table 1: Literature Survey Table

Sr. No	Title	Methodology	Disadvantages
[1]	"The Impact of Virtual Laboratories on Active Learning and Engagement in Cybersecurity Distance Education," Victor R. Kebande,(Apr-2024)	Utilized a three-fold methodology combining purposive sampling, face validation by cybersecurity experts, and performance assessment of students using V Labs to analyze engagement and learning outcomes.	Virtual labs, while controlled and scalable, may lack the full complexity and unpredictability of real-world cyber threat landscapes, potentially limiting exposure to dynamic attack behaviors.
[2]	"Navigating Cybersecurity Training: A Comprehensive Review," Saif Al-Dean Qawasmeh, Ali Abdullah S. AlQahtani, (Jan-2024)	Conducts an extensive thematic review of cybersecurity training techniques across academic and industrial domains, primarily focusing on simulation-based methods, gamified learning, and online training platforms without deeply integrating real-time lab environments or offensive-defensive dual-role capabilities.	The surveyed methods often lack adaptability, suffer from limited realism in simulated attack scenarios, and do not provide integrated environments where learners can practice both offensive and defensive techniques in enterprise-like network architectures.
[3]	"Hands-On Labs: The Key to Effective Cybersecurity Education," INE Security Research Team, (Sept- 2024)	Incorporates virtual labs, capture-the-flag (CTF) events, and certification-aligned practical environments to offer students hands-on exposure. Encourages industry collaboration, project-based learning, and internship programs to simulate real-world scenarios in a secure setting.	Limited support for advanced adversarial simulations and lacks deep customization for enterprise-level red teaming.
[4]	"Building resilience in cybersecurity: An artificial lab approach," Kerstin Awiszus1, Yannick Bell, Jan Lüttringhaus, Gregor Svindland, Alexander Voß, Stefan Weber, (Aug-2023)	Developed an artificial lab framework using experimental economics to simulate cyberattacks and observe how firms invest in resilience, using Markovian SIR models and network graph simulations.	Limitations include the difficulty in scaling the lab model for diverse organizations and the inability to fully replicate real-world dynamic cyber threat environments.
[5]	"RNNIDS: Enhancing Network Intrusion Detection Systems through Deep Learning,"SOROUSH M. SOHI,	Introduced RNN-based intrusion detection, trained on benchmark datasets (NSL-KDD), comparing its performance to classical machine	Model performance is dataset-dependent and may suffer from reduced effectiveness in detecting zero-day or evolving attacks

	JEAN-PIERRE SEIFERT, FATEMEH GANJI, (Dec-2020)	learning models for anomaly detection.	without frequent retraining.
[6]	"Cyber Security Teaching and Learning Laboratories: A Survey," Luke TOPHAM, Kashif KIFAYAT, Younis A. YOUNIS, Qi SHI, Bob ASKWITH, (2016)	Conducted a comprehensive literature survey of cybersecurity lab models in academic institutions, reviewing design types, pedagogical alignment, and lab accessibility features.	Survey found inconsistent standards in lab implementations and challenges in replicating real-world scenarios, especially in basic static labs.
[7]	"CLaaS: Cybersecurity Lab as a Service," Cihan Tunc, Salim Hariri, (Nov-2015)	Proposed a cloud-based virtual lab platform (CLaaS) using dynamic VM provisioning to deliver cybersecurity training remotely, with emphasis on scalability, elasticity, and ease of access.	The model requires robust infrastructure and internet connectivity, making it less viable in low-resource or offline environments..

As shown in Table 1, prior virtual lab platforms demonstrate limitations including a lack of real-world adversarial simulation depth, minimal red-teaming support, constrained customization of attack scenarios, and limited integration of offensive tooling and network pivoting capabilities.

IV. METHODOLOGY

As shown in figure 1, Cybercrescendo follows a structured approach:

Virtual Environment Setup:

A simulated enterprise-grade IT infrastructure was constructed using VirtualBox, incorporating segmented LANs, domain controllers, DNS servers, and Linux-based monitoring nodes. This design mirrors a realistic organizational cybersecurity environment to enhance scenario fidelity.

Security Tool Configuration:

Security tools like OPNsense firewall, Suricata IDS/IPS, and Wazuh SIEM are configured for network defense. Offensive tools such as Kali Linux, Metasploit, and Nmap are used for simulating penetration testing, vulnerability scanning, and red team operations.

Attack Simulation and Response:

Realistic attack scenarios are launched, including brute force, SQL injection, phishing, and privilege escalation. Blue Team participants are trained to detect, analyze, and mitigate these threats in real-time using integrated dashboards and alerts.

Threat Intelligence Automation:

Tools like MISP, TheHive, and Cortex were integrated to mimic real-world threat intelligence workflows. They enriched attack data, facilitated incident triage, and automated response actions to help users understand full-cycle SOC operations

.

Hands-on Training Exercises:

Learners were guided through modular labs featuring practical challenges like malware analysis, insider threat detection, and SIEM rule tuning. Each module included stepwise goals, hints, and real-time feedback to reinforce concepts through active learning.

DOI: 10.48175/IJARSCT-25058

Performance Monitoring and Feedback Loop:

Using Wazuh, all user actions were logged. Performance metrics such as detection time, number of false positives, and response accuracy were collected. These reports helped learners understand their weaknesses and focus areas for improvement.

V. SYSTEM DESIGN

The architecture of Cybercrescendo includes:

Network Topology

Segmented networks include DMZ (web services), Internal (AD, DNS), and Security Ops (SIEM, IDS/IPS).

System Setup

Windows Server (AD, DNS, DHCP), Ubuntu servers with Wazuh, Suricata, and ELK stack.

Red Team Tools

Kali Linux with Nmap, Metasploit, Hydra; simulates brute-force, phishing, CVE exploitation.

Blue Team Tools

Wazuh, TheHive, ELK for alerting, log analysis, and real-time threat detection.

Threat Intel

MISP integrates with Cortex and Wazuh for enriched alerts and ecosystem simulation.

Attack Scenarios

Covers SQLi, XSS, privilege escalation, insider threats, and zero-day simulations.

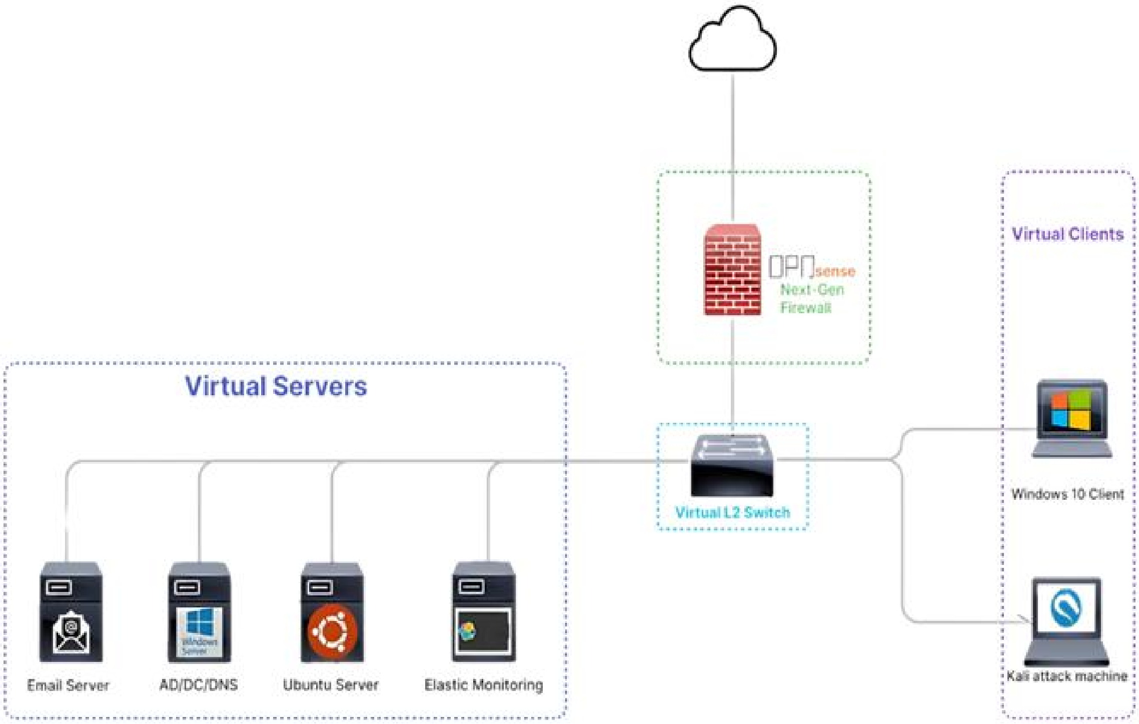
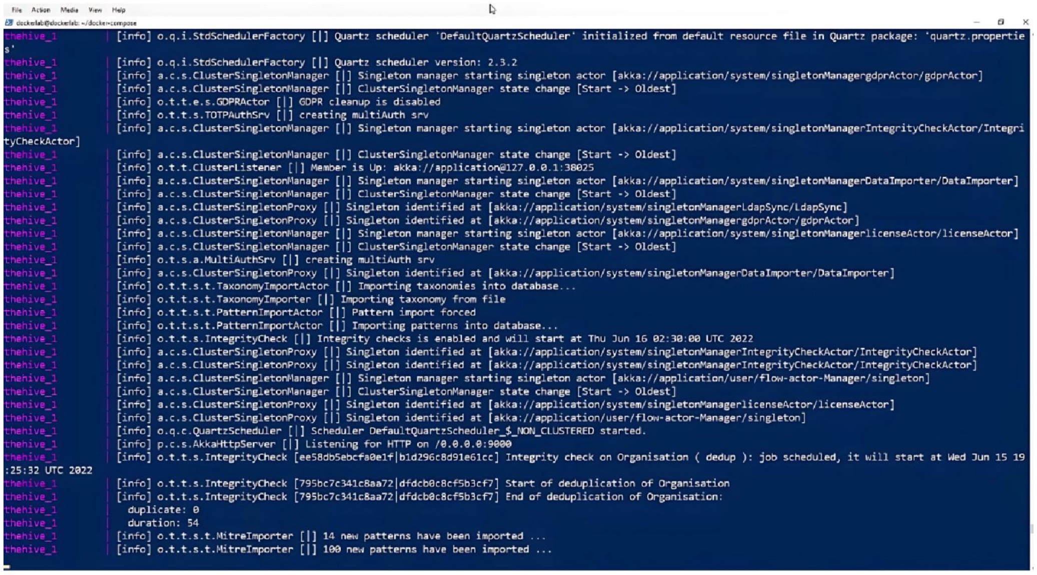


Fig. 1. Architecture Diagram

VI. RESULTS AND ANALYSIS



```
thehive_1       | [info] o.q.i.StdSchedulerFactory [|] Quartz scheduler 'DefaultQuartzScheduler' initialized from default resource file in Quartz package: 'quartz.propertie
s'
thehive_1       | [info] o.q.i.StdSchedulerFactory [|] Quartz scheduler version: 2.3.2
thehive_1       | [info] a.c.s.ClusterSingletonManager [|] Singleton manager starting singleton actor [akka://application/system/singletonManagergdprActor/gdprActor]
thehive_1       | [info] a.c.s.ClusterSingletonManager [|] ClusterSingletonManager state change [Start -> Oldest]
thehive_1       | [info] o.t.t.e.s.GDPRActor [|] GDPR cleanup is disabled
thehive_1       | [info] o.t.t.s.TOTPAuthSrv [|] creating multiAuth srv
thehive_1       | [info] a.c.s.ClusterSingletonManager [|] Singleton manager starting singleton actor [akka://application/system/singletonManagerIntegrityCheckActor/Integri
tyCheckActor]
thehive_1       | [info] a.c.s.ClusterSingletonManager [|] ClusterSingletonManager state change [Start -> Oldest]
thehive_1       | [info] o.t.t.ClusterListener [|] Member is Up: akka://application@127.0.0.1:38025
thehive_1       | [info] a.c.s.ClusterSingletonManager [|] Singleton manager starting singleton actor [akka://application/system/singletonManagerDataImporter/DataImporter]
thehive_1       | [info] a.c.s.ClusterSingletonManager [|] ClusterSingletonManager state change [Start -> Oldest]
thehive_1       | [info] a.c.s.ClusterSingletonProxy [|] Singleton identified at [akka://application/system/singletonManagerLdapSync/LdapSync]
thehive_1       | [info] a.c.s.ClusterSingletonProxy [|] Singleton identified at [akka://application/system/singletonManagergdprActor/gdprActor]
thehive_1       | [info] a.c.s.ClusterSingletonManager [|] Singleton manager starting singleton actor [akka://application/system/singletonManagerlicenseActor/licenseActor]
thehive_1       | [info] a.c.s.ClusterSingletonManager [|] ClusterSingletonManager state change [Start -> Oldest]
thehive_1       | [info] o.t.s.a.MultiAuthSrv [|] creating multiAuth srv
thehive_1       | [info] a.c.s.ClusterSingletonProxy [|] Singleton identified at [akka://application/system/singletonManagerDataImporter/DataImporter]
thehive_1       | [info] o.t.t.s.t.TaxonomyImportActor [|] Importing taxonomies into database...
thehive_1       | [info] o.t.t.s.t.TaxonomyImporter [|] Importing taxonomy from file
thehive_1       | [info] o.t.t.s.t.PatternImportActor [|] Pattern import forced
thehive_1       | [info] o.t.t.s.t.PatternImportActor [|] Importing patterns into database...
thehive_1       | [info] o.t.t.s.IntegrityCheck [|] Integrity checks is enabled and will start at Thu Jun 16 02:30:00 UTC 2022
thehive_1       | [info] a.c.s.ClusterSingletonProxy [|] Singleton identified at [akka://application/system/singletonManagerIntegrityCheckActor/IntegrityCheckActor]
thehive_1       | [info] a.c.s.ClusterSingletonProxy [|] Singleton identified at [akka://application/system/singletonManagerIntegrityCheckActor/IntegrityCheckActor]
thehive_1       | [info] a.c.s.ClusterSingletonManager [|] Singleton manager starting singleton actor [akka://application/user/flow-actor-Manager/singleton]
thehive_1       | [info] a.c.s.ClusterSingletonManager [|] ClusterSingletonManager state change [Start -> Oldest]
thehive_1       | [info] a.c.s.ClusterSingletonProxy [|] Singleton identified at [akka://application/system/singletonManagerlicenseActor/licenseActor]
thehive_1       | [info] a.c.s.ClusterSingletonProxy [|] Singleton identified at [akka://application/user/flow-actor-Manager/singleton]
thehive_1       | [info] o.q.c.QuartzScheduler [|] Scheduler DefaultQuartzScheduler_$_NON_CLUSTERED started.
thehive_1       | [info] p.c.s.AkkaHttpServer [|] Listening for HTTP on /0.0.0.0:9000
thehive_1       | [info] o.t.t.s.IntegrityCheck [ee58db5ebcfa0e1f|b1d296c8d91e61cc] Integrity check on Organisation ( dedup ): job scheduled, it will start at Wed Jun 15 19
:25:32 UTC 2022
thehive_1       | [info] o.t.t.s.IntegrityCheck [795bc7c341c8aa72|dfdcb0c8cf5b3cf7] Start of deduplication of Organisation
thehive_1       | [info] o.t.t.s.IntegrityCheck [795bc7c341c8aa72|dfdcb0c8cf5b3cf7] End of deduplication of Organisation:
thehive_1       |   duplicate: 0
thehive_1       |   duration: 54
thehive_1       | [info] o.t.t.s.t.MitreImporter [|] 14 new patterns have been imported ...
thehive_1       | [info] o.t.t.s.t.MitreImporter [|] 100 new patterns have been imported ...
```

Fig. 2. TheHive Initialization via Docker in CyberCrescendo Lab

As shown in Fig. 2, the terminal output represents the backend initialization process of TheHive—a Security Incident Response Platform (SIRP)—within a Dockerized environment in CyberCrescendo's virtual lab. Several essential services such as user authentication (MultiAuthSrv), pattern and taxonomy importers, integrity checks, and GDPR compliance modules are activated. These log messages confirm that the platform's key functions like incident correlation, data validation, and threat intelligence integration are successfully up and running. This setup reflects a realistic deployment scenario where all components work together to simulate enterprise-level threat detection and response.

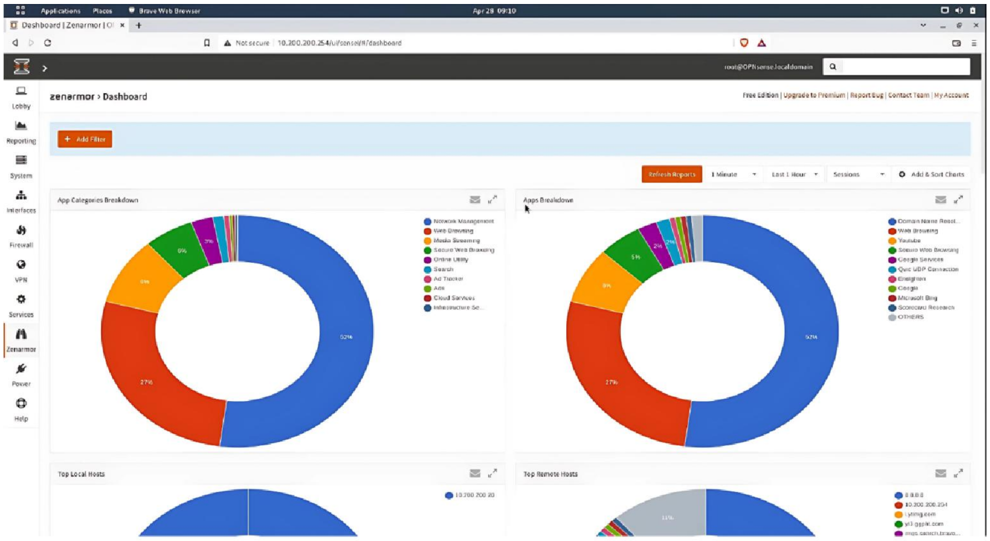
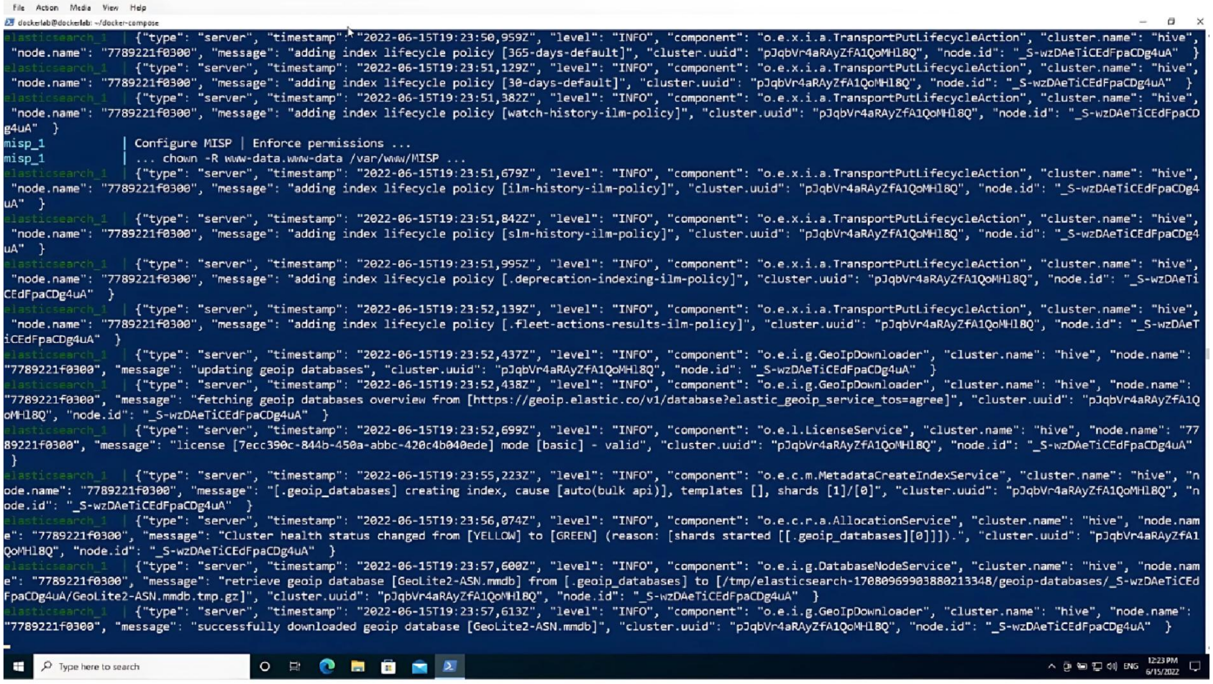


Fig. 3. Zenarmor Application Traffic Categorization Dashboard

As shown in Fig. 3, the Zenarmor interface provides a detailed breakdown of network traffic by application categories and individual apps. This allows administrators to visualize which types of applications are being accessed (e.g., productivity, streaming, social media), along with specific app usage volumes. Such granularity helps in identifying bandwidth-heavy or potentially risky applications, enhancing visibility and enabling precise policy enforcement. For learners, this view helps build a practical understanding of traffic monitoring and how cybersecurity tools categorize and manage network behavior in real-time


File Action Media View Help
dockerlab@dockerlab: ~/docker-compose
Type here to search
ENG
12:23 PM
6/15/2022

```
elasticsearch_1  | {"type": "server", "timestamp": "2022-06-15T19:23:50,959Z", "level": "INFO", "component": "o.e.x.i.a.TransportPutLifecycleAction", "cluster.name": "hive",
 "node.name": "7789221f0300", "message": "adding index lifecycle policy [365-days-default]", "cluster.uuid": "pJqbVr4aRAyZfA1QoMHl8Q", "node.id": "_S-wzDAeTiCEdFpaCDg4uA"  }
elasticsearch_1  | {"type": "server", "timestamp": "2022-06-15T19:23:51,129Z", "level": "INFO", "component": "o.e.x.i.a.TransportPutLifecycleAction", "cluster.name": "hive",
 "node.name": "7789221f0300", "message": "adding index lifecycle policy [30-days-default]", "cluster.uuid": "pJqbVr4aRAyZfA1QoMHl8Q", "node.id": "_S-wzDAeTiCEdFpaCDg4uA"  }
elasticsearch_1  | {"type": "server", "timestamp": "2022-06-15T19:23:51,382Z", "level": "INFO", "component": "o.e.x.i.a.TransportPutLifecycleAction", "cluster.name": "hive",
 "node.name": "7789221f0300", "message": "adding index lifecycle policy [watch-history-ilm-policy]", "cluster.uuid": "pJqbVr4aRAyZfA1QoMHl8Q", "node.id": "_S-wzDAeTiCEdFpaCD
g4uA"  }
misp_1           | Configure MISP | Enforce permissions ...
misp_1           | ... chown -R www-data.www-data /var/www/MISP ...
elasticsearch_1  | {"type": "server", "timestamp": "2022-06-15T19:23:51,679Z", "level": "INFO", "component": "o.e.x.i.a.TransportPutLifecycleAction", "cluster.name": "hive",
 "node.name": "7789221f0300", "message": "adding index lifecycle policy [ilm-history-ilm-policy]", "cluster.uuid": "pJqbVr4aRAyZfA1QoMHl8Q", "node.id": "_S-wzDAeTiCEdFpaCDg4
uA"  }
elasticsearch_1  | {"type": "server", "timestamp": "2022-06-15T19:23:51,842Z", "level": "INFO", "component": "o.e.x.i.a.TransportPutLifecycleAction", "cluster.name": "hive",
 "node.name": "7789221f0300", "message": "adding index lifecycle policy [slm-history-ilm-policy]", "cluster.uuid": "pJqbVr4aRAyZfA1QoMHl8Q", "node.id": "_S-wzDAeTiCEdFpaCDg4
uA"  }
elasticsearch_1  | {"type": "server", "timestamp": "2022-06-15T19:23:51,995Z", "level": "INFO", "component": "o.e.x.i.a.TransportPutLifecycleAction", "cluster.name": "hive",
 "node.name": "7789221f0300", "message": "adding index lifecycle policy [.deprecation-indexing-ilm-policy]", "cluster.uuid": "pJqbVr4aRAyZfA1QoMHl8Q", "node.id": "_S-wzDAeTi
CEdFpaCDg4uA"  }
elasticsearch_1  | {"type": "server", "timestamp": "2022-06-15T19:23:52,139Z", "level": "INFO", "component": "o.e.x.i.a.TransportPutLifecycleAction", "cluster.name": "hive",
 "node.name": "7789221f0300", "message": "adding index lifecycle policy [.fleet-actions-results-ilm-policy]", "cluster.uuid": "pJqbVr4aRAyZfA1QoMHl8Q", "node.id": "_S-wzDAeT
iCEdFpaCDg4uA"  }
elasticsearch_1  | {"type": "server", "timestamp": "2022-06-15T19:23:52,437Z", "level": "INFO", "component": "o.e.i.g.GeoIpDownloader", "cluster.name": "hive", "node.name":
"7789221f0300", "message": "updating geoip databases", "cluster.uuid": "pJqbVr4aRAyZfA1QoMHl8Q", "node.id": "_S-wzDAeTiCEdFpaCDg4uA"  }
elasticsearch_1  | {"type": "server", "timestamp": "2022-06-15T19:23:52,438Z", "level": "INFO", "component": "o.e.i.g.GeoIpDownloader", "cluster.name": "hive", "node.name":
"7789221f0300", "message": "fetching geoip databases overview from [https://geoip.elastic.co/v1/database?elastic_geoip_service_tos=agree]", "cluster.uuid": "pJqbVr4aRAyZfA1Q
oMHl8Q", "node.id": "_S-wzDAeTiCEdFpaCDg4uA"  }
elasticsearch_1  | {"type": "server", "timestamp": "2022-06-15T19:23:52,699Z", "level": "INFO", "component": "o.e.l.LicenseService", "cluster.name": "hive", "node.name": "77
89221f0300", "message": "license [7ecc390c-844b-450a-abbc-420c4b040ede] mode [basic] - valid", "cluster.uuid": "pJqbVr4aRAyZfA1QoMHl8Q", "node.id": "_S-wzDAeTiCEdFpaCDg4uA"
 }
elasticsearch_1  | {"type": "server", "timestamp": "2022-06-15T19:23:55,223Z", "level": "INFO", "component": "o.e.c.m.MetadataCreateIndexService", "cluster.name": "hive", "n
ode.name": "7789221f0300", "message": "[.geoip_databases] creating index, cause [auto(bulk api)], templates [], shards [1]/[0]", "cluster.uuid": "pJqbVr4aRAyZfA1QoMHl8Q", "n
ode.id": "_S-wzDAeTiCEdFpaCDg4uA"  }
elasticsearch_1  | {"type": "server", "timestamp": "2022-06-15T19:23:56,074Z", "level": "INFO", "component": "o.e.c.r.a.AllocationService", "cluster.name": "hive", "node.nam
e": "7789221f0300", "message": "Cluster health status changed from [YELLOW] to [GREEN] (reason: [shards started [[.geoip_databases][0]]]).", "cluster.uuid": "pJqbVr4aRAyZfA1
QoMHl8Q", "node.id": "_S-wzDAeTiCEdFpaCDg4uA"  }
elasticsearch_1  | {"type": "server", "timestamp": "2022-06-15T19:23:57,600Z", "level": "INFO", "component": "o.e.i.g.DatabaseNodeService", "cluster.name": "hive", "node.nam
e": "7789221f0300", "message": "retrieve geoip database [GeoLite2-ASN.mmdb] from [.geoip_databases] to [/tmp/elasticsearch-17080969903880213348/geoip-databases/_S-wzDAeTiCEd
FpaCDg4uA/GeoLite2-ASN.mmdb.tmp.gz]", "cluster.uuid": "pJqbVr4aRAyZfA1QoMHl8Q", "node.id": "_S-wzDAeTiCEdFpaCDg4uA"  }
elasticsearch_1  | {"type": "server", "timestamp": "2022-06-15T19:23:57,613Z", "level": "INFO", "component": "o.e.i.g.GeoIpDownloader", "cluster.name": "hive", "node.name":
"7789221f0300", "message": "successfully downloaded geoip database [GeoLite2-ASN.mmdb]", "cluster.uuid": "pJqbVr4aRAyZfA1QoMHl8Q", "node.id": "_S-wzDAeTiCEdFpaCDg4uA"  }
```

Fig. 4. System Log: Elasticsearch Index Policies &GeoIP Setup

As shown in Fig. 4, the system logs reveal that Elasticsearch is actively initializing several Index Lifecycle Management (ILM) policies, such as 365-days-default, watch-history-ilm-policy, and .fleet-actions-results-ilm-policy, among others. These policies automate data retention and index management tasks, helping to optimize storage and performance.

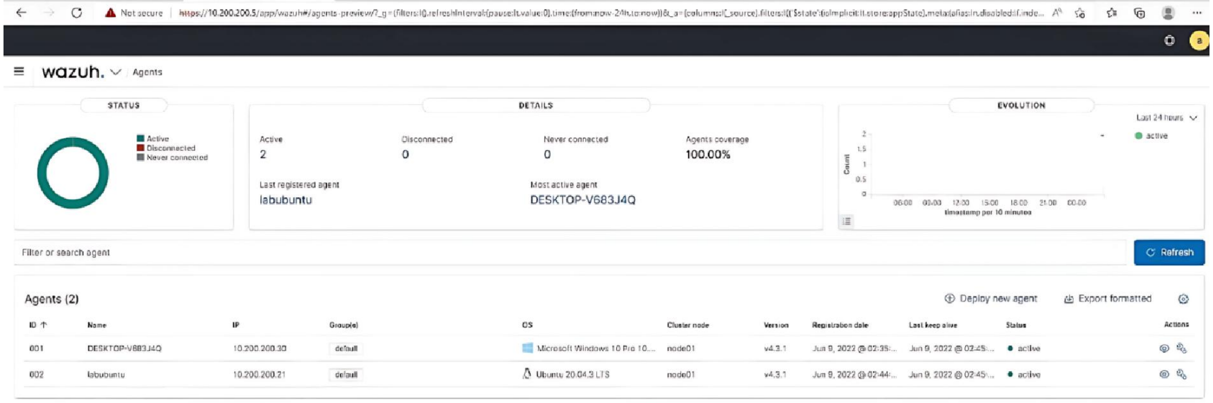
Additionally, the logs indicate that the GeoIP database (GeoLite2-ASN.mmdb) was successfully fetched and deployed, enabling geographic IP mapping for traffic analysis. CyberCrescendo's integration of such logging through Dockerized services (e.g., MISP, Elasticsearch) ensures transparency and auditability, helping learners and administrators track service setup and monitor backend configurations effectively.

As shown in Fig. 5 demonstrates the deployment and operational integrity of endpoint agents within the Cybercrescendo virtual lab environment. Using the Wazuh SIEM platform, agents were successfully installed and monitored across both Windows and Ubuntu systems. The dashboard displays two fully active agents: one on a Windows 10 host (DESKTOP-V683J40) and the other on an Ubuntu 20.04 LTS node (labubuntu). Both show regular heartbeat signals, confirming stable connections to the central SIEM.

The results affirm 100% coverage across simulated endpoints, enabling real-time data collection, log analysis, and behavioral monitoring. This level of integration is critical for achieving practical Blue Team training objectives, such as log triage, alert validation, and endpoint visibility. The success of agent synchronization indicates that Cybercrescendo

DOI: 10.48175/IJARSCT-25058

effectively supports enterprise-like system monitoring, crucial for teaching incident detection and endpoint telemetry management.


Not secure
https://10.200.200.5/app/wazuh#/agents-preview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(columns:!(_source),filters:!(('$state':(isImplicit:!t,store:appState),meta:(alias:!n,disabled:!f,inde...
wazuh.
Agents
STATUS
Active
Disconnected
Never connected
DETAILS
EVOLUTION
Last 24 hours
active
Count
2
1.5
1
0.5
0
06:00
09:00
12:00
15:00
18:00
21:00
00:00
timestamp per 10 minutes
Filter or search agent
Refresh
Deploy new agent
Export formatted

Active 2 | Disconnected 0 | Never connected 0 | Agents coverage 100.00%

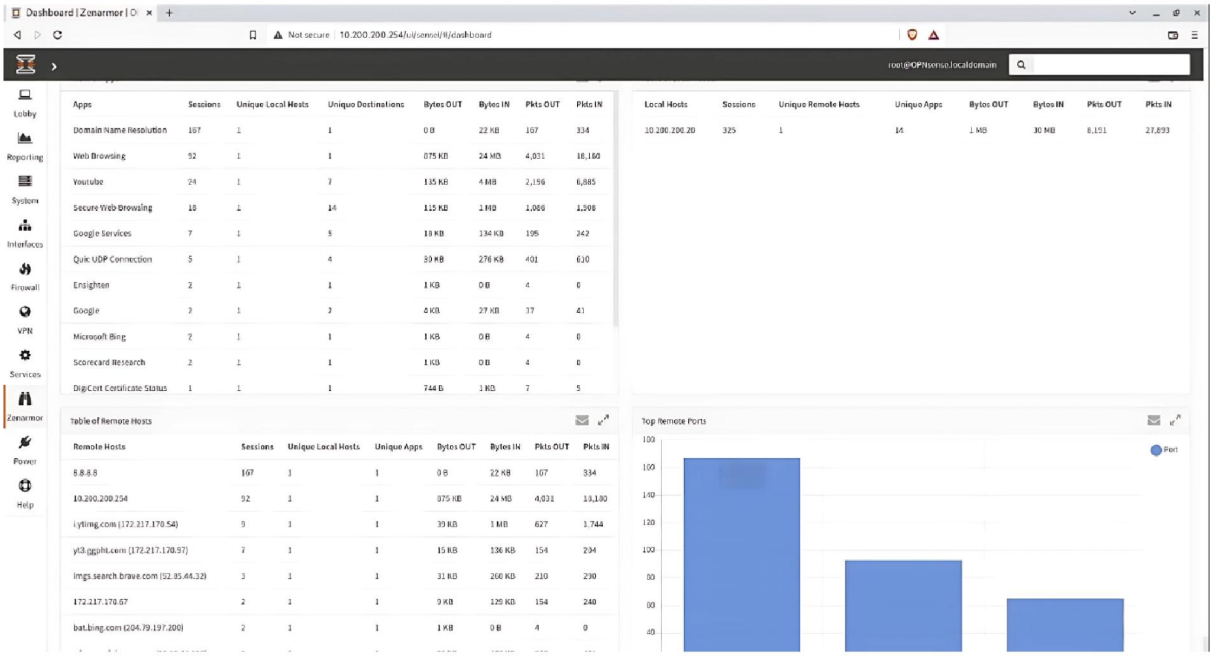
Last registered agent labubuntu

Most active agent DESKTOP-V683J4Q

Agents (2)

ID ↑	Name	IP	Group(s)	OS	Cluster node	Version	Registration date	Last keep alive	Status	Actions
001	DESKTOP-V683J4Q	10.200.200.30	default	Microsoft Windows 10 Pro 10...	node01	v4.3.1	Jun 9, 2022 @ 02:35:...	Jun 9, 2022 @ 02:45:...	● active	
002	labubuntu	10.200.200.21	default	Ubuntu 20.04.3 LTS	node01	v4.3.1	Jun 9, 2022 @ 02:44:...	Jun 9, 2022 @ 02:45:...	● active	

Fig. 5. Wazuh Agent Monitoring Results



Apps	Sessions	Unique Local Hosts	Unique Destinations	Bytes OUT	Bytes IN	Pkts OUT	Pkts IN
Domain Name Resolution	167	1	1	0 B	22 KB	167	334
Web Browsing	92	1	1	875 KB	24 MB	4,031	18,180
Youtube	24	1	7	135 KB	4 MB	2,196	6,885
Secure Web Browsing	18	1	14	115 KB	1 MB	1,086	1,508
Google Services	7	1	5	18 KB	134 KB	195	242
Quic UDP Connection	5	1	4	30 KB	276 KB	401	610
Ensighten	2	1	1	1 KB	0 B	4	0
Google	2	1	2	4 KB	27 KB	37	41
Microsoft Bing	2	1	1	1 KB	0 B	4	0
Scorecard Research	2	1	1	1 KB	0 B	4	0
DigiCert Certificate Status	1	1	1	744 B	1 KB	7	5

Local Hosts	Sessions	Unique Remote Hosts	Unique Apps	Bytes OUT	Bytes IN	Pkts OUT	Pkts IN
10.200.200.20	325	1	14	1 MB	30 MB	8,151	27,893

Table of Remote Hosts

Remote Hosts	Sessions	Unique Local Hosts	Unique Apps	Bytes OUT	Bytes IN	Pkts OUT	Pkts IN
8.8.8.8	167	1	1	0 B	22 KB	167	334
10.200.200.254	92	1	1	875 KB	24 MB	4,031	18,180
i.ytimg.com (172.217.170.54)	9	1	1	39 KB	1 MB	627	1,744
yt3.ggpht.com (172.217.170.97)	7	1	1	15 KB	136 KB	154	204
imgs.search.brave.com (52.85.44.32)	3	1	1	31 KB	260 KB	210	290
172.217.170.67	2	1	1	9 KB	129 KB	154	240
bat.bing.com (204.79.197.200)	2	1	1	1 KB	0 B	4	0

Fig. 6. Application-Level Traffic Visibility

As shown in Fig. 6 presents real-time application-layer traffic metrics, including session counts, data volumes, domain queries, and protocol types. The traffic profile spans secure web browsing, streaming, certificate validations, and encrypted tunneling.

These insights confirm CyberCrescendo's ability to replicate diverse, realistic network behaviors—empowering learners to analyze encrypted flows, detect risk-prone applications, and gain hands-on exposure to deep packet inspection and behavioralmonitoring

DOI: 10.48175/IJARSCT-25058

VII. CONCLUSION AND FUTURE SCOPE

CyberCrescendo reimagines cybersecurity education by offering a rich, interactive lab environment where users actively engage with real-world attack simulations. By combining offensive tactics, defensive strategies, and data-driven performance tracking, it fosters hands-on learning experiences that strengthen skills in threat mitigation, incident analysis, and system resilience—all within a secure, enterprise-like setup.

In the future, the platform will expand its scope by simulating complex threats such as fileless malware and cloud-based intrusions while introducing support for containerized and scalable cloud infrastructure. Planned updates include collaborative scenarios for team-based training, game-based progression features to boost motivation, and integration with academic certifications to align with industry needs. These enhancements are designed to deepen realism, widen accessibility, and drive meaningful engagement in both classroom and corporate settings.

REFERENCES

[1] Victor R. Kebande, “The Impact of Virtual Laboratories on Active Learning and Engagement in Cybersecurity Distance Education,” arXiv:2404.04952v1 [cs.CY], Apr. 2024.

[2] Saif Al-Dean Qawasmeh, Ali Abdullah S. AlQahtani, “Navigating Cybersecurity Training: A Comprehensive Review,” arXiv:2401.11326 [cs.CR], Jan. 2024.

[3] INE Security Research Team, “Hands-On Labs: The Key to Effective Cybersecurity Education,”Sept 2024.

[4] Kerstin Awiszus1, Yannick Bell, Jan Lüttringhaus, Gregor Svindland, Alexander Voß, Stefan Weber, “Building resilience in cybersecurity: An artificial lab approach,” DOI: 10.1111/jori.12450, Aug 2023

[5] SOROUSH M. SOHI, JEAN-PIERRE SEIFERT, and FATEMEH GANJI, “RNNIDS: Enhancing Network Intrusion Detection Systems through Deep Learning,” arXiv:1807.03212 [cs.CR], Nov 2020

[6] Luke TOPHAM, Kashif KIFAYAT, Younis A. YOUNIS, Qi SHI, and Bob ASKWITH “Cyber Security Teaching and Learning Laboratories: A Survey,” Information & Security: An International Journal, Volume 35, Issue 1, p.51-80, 2016.

[7] Cihan Tunc and Salim Hariri, "CLaaS: Cybersecurity Lab as a Service,"The University of Arizona, Tucson, Arizona 85721 USA, Nov 2015.

DOI: 10.48175/IJARSCT-25058