DEPARTMENT OF SOFTWARE ENGINEERING

BACHELORS IN SOFTWARE ENGINEERING

Course Code: CT-460

Course Title: Network & Information Security

Complex Engineering Problem

BE Batch 2021, Fall Semester 2024

Course Learning Outcome

CLO3: Be able to understand, Analyze and compare network and IS security data to formulate issues and problems (C4-PLO4)

Complex problem-solving attributes (CPA) covered (as per PEC - OBA manual – 2019)

- **CPA-1 Depth of analysis required:** These problems do not have readily apparent solutions and demand abstract thinking and innovative analysis to develop appropriate models.

- **CPA-2 Level of interaction:** Necessitate the resolution of substantial challenges resulting from the interplay of diverse or conflicting technical, engineering, or other factors.

- **CPA-3 Familiarity:** Can go beyond prior experiences through the application of principle-driven methodologies.

Problem Statement

Students are required to work on one of the assigned open-source tools in the domain of Malware Analysis, Blockchain auditing, Penetration Testing, Digital Forensics, Web Security, SIEM, IDS, and Container Security etc. They must first properly install and configure the tool and implement working scenarios. The next task is to launch one of the assigned attack vectors like DDoS, Malware, Viruses, SQL Injections etc. on the implemented work. Afterwards, appropriate protection mechanism should be implemented to counter the attack. The students need to perform analysis of the implemented security mechanism and its quantification. The students are required to submit a detailed report.

Minimum Required Features:

1. Security Mechanism implementation: Analysis of the implemented security mechanism and its quantification.

2. Documentation: The report should contain Abstract, Introduction, Related Work, Comparative Analysis, Methodology, Result and Analysis and Conclusion. The report should follow IEEE format.

Instructions and Guidelines:

1. Software Selection: Choose the software that is publicly available and free to use. Ensure it is not proprietary.

2. Security Mechanism Analysis:

- Implementation of the threat vector for the given topic.
- A detailed analysis of the implemented security mechanism and its quantification.

3. Documentation:

- Create comprehensive documentation summarizing your findings. Include diagrams, flowcharts, and pseudocode where necessary to clarify your analysis. The sections of Report are Abstract, Introduction, Related Work, Methodology, Results and Findings and Conclusion.
- Explanation of how the proposed mechanism cater the given security threat. (As discussed in class)

Deliverables:

1. A detailed report on your security mechanism analysis. This report should include the following:

-Abstract Section: Summary of report.

- Introduction Section: highlighting the scope of problem and your contributions.
- Related Work: Description of the previous work that have addressed this problem.
- Methodology adapted for solving the given threat vector or security issue
- Results and finding: Important findings during the work. Documentation of identified data structures, algorithms, and design patterns used.
- Any interesting findings or insights about the given security operations.
- Conclusion: Summary of wok and findings

2. Any code snippets, pseudocode, or diagrams that help illustrate your analysis.

Please note that this problem is for educational and research purposes only, and you should adhere to all relevant legal and ethical guidelines.

You are required to bring the hardcopy of the report for final assessment that will be conducted in week 13. You are also required to submit the soft copy of report and work on the Google classroom.

While compiling the report, keep the following in mind:

- **Attach the provided rubric on top of your report, with names and roll numbers filled in.**
- **Title page, along with rubric sheet.**
- **Use font size of 12 and/or 14 for headings, and 11 for regular text.**
- **Font style should be Times New Roman.**

DEPARTMENT OF SOFTWARE ENGINEERING
BACHELORS IN SOFTWARE ENGINEERING
Course Code: CT-460
Course Title: Network & Information Security
Complex Engineering Problem
BE Batch 2021, Fall Semester 2024
Grading Rubric

Group Members:

Student No.	Name	Roll No.
S1		
S2		
S3		
S4		

CRITERIA AND SCALES				**Marks Obtained**			
				S1	**S2**	**S3**	**S4**
Criterion 1: To what extent the student understood the assigned security domain?							
0	1	2	3				
The student did not understand the assigned security domain.	The student understood the assigned security domain partially.	The student understood the assigned security domain satisfactorily.	The student understood the assigned security domain exceptionally well.				
Criterion 2: To what extent the student implemented the attack vector? (CPA-1, CPA-3)							
0	1	2	3				
The student did not implement the attack vector.	The student implemented the attack vector partially.	The student implemented the attack vector satisfactorily.	The student implemented the attack vector exceptionally well.				
Criterion 3: To what extent the student implemented the defense mechanism against given attack vector? (CPA-1, CPA-3)							
0	1	2	3				
The student did not implement the defense mechanism against given attack vector.	The student implemented the defense mechanism against given attack vector partially.	The student implemented the defense mechanism against given attack vector satisfactorily.	The student implemented the defense mechanism against given attack vector exceptionally well.				
Criterion 4: To what extent the student has performed the analysis of the security mechanism? (CPA-2, CPA-3)							
0	1	2	3				
The student did not perform any analysis	The student worked on the assigned task, and performed analysis partially	The student worked on the assigned task, and accomplished analysis satisfactorily.	The student worked on the assigned task, and accomplished analysis exceptionally well.				
Criterion 5: Does the report adhere to the given format and requirements?							
0	1	2	3				
The report does not contain the required information and is formatted poorly.	The report contains the required information only partially but is formatted well.	The report contains all the required information but is formatted poorly.	The report contains all the required information and completely adheres to the given format.				
			Total Marks:				

Teacher's Signature

Network & Information Security
CT-460

Complex Engineering Problem

“Extended Detection and Response (XDR): Implementation Analysis Using Wazuh”

Group Id: 01

Group Members:

Khushbakht Khan	SE-21009
Sarah Sami	SE-21026
Syed Aun Muhammad	SE-21036
Moiz Naveed	SE-21048

Department of Software Engineering ,Neduet

Extended Detection and Response (XDR): Implementation Analysis Using Wazuh

Khushbakht Khan
Dept of Software Engineering
NED University
Karachi, Pakistan
khushbakhtkhan1@gmail.com

Sarah Sami
Dept of Software Engineering
NED University
Karachi, Pakistan
sarahsk002@gmail.com

Syed Aun Muhammad
Dept of Software Engineering
NED University
Karachi, Pakistan
auna7472@gmail.com

Moiz Naveed
Dept of Software Engineering
NED University)
Karachi, Pakistan
naveedmoiz928@gmail.com

Abstract—**In today's rapidly evolving technological landscape, As companies have adopted modern tools to meet their business requirements, cybercriminals have managed to improve their attack vector as well. The current security architecture comprises a multitude of security controls. However, these measures have proven ineffective. According to a report from the clip solution, over 90% of respondents had experienced a multi-layered security breach. This is primarily due to the limitations of traditional Security Information and Event Management (SIEM) which pioneered the approach of log storage and correlation. The majority of SIEM solutions offer very weak security analytics. Countering the SIEM practice was Extended Detection Response which arose as a new standard [1]. XDR makes better use of existing security products by bridging together disparate tools into a single cohesive unit to curtail invasions. It also enhances automated responses and detection capabilities thus overcoming many of the drawbacks that were faced with traditional approaches. Acknowledging these points this paper aims to highlight the significance of XDR, its primary functions, various deployments, and notably its ability to enhance efficiency levels where human intervention is heavily utilized. The effectiveness of Wazuh as a XDR solution extends to its illustration of the architecture, mechanisms of operation, and in particular, the components that are crucial within any organization that seeks to offer protection. However, the focus of Wazuh is to offer flexibility as XDR networks would find this vital in the adoption of such networks, which may not be provided in many other XDR configurations. Weaknesses pertaining to limited sphere of awareness, the price factor and the necessity of trained staff are also included. The paper ends with a description of Wazuh's architecture and experimental conditions, emphasizing its function in the improvement of security operations.**

Index Terms—**Extended Detection and Response (XDR), Security Information and Event Management (SIEM), Cybersecurity, Threat Detection, Wazuh, Automation, Orchestration, Endpoint Security, Network Security, Threat Intelligence, Security Operations Center (SOC), Machine Learning, Integration, Open-Source Security Platform.**

I. Introduction

Today's society is more reliant on technology and this means that businesses are under more complex cyberattacks. Such attacks seek to bypass several lines of defense security. They look for weaknesses in various solutions and worm their way in. Such assaults occur quite frequently and display a high degree proficiency in circumventing conventional defenses. For this reason, organizations are constantly on the lookout for ways to secure their critical assets and keep their operations running. Most of the time, standard security techniques do the trick for a limited period of time. But they also cause certain issues. Among them is that they create data silos making it difficult to perform operations. A typical example of a security discipline used for the purpose of monitoring the activity logs and the compliance of the standards is the Security Information and Event Management (SIEM) system [2]. They attempt to process a vast amount of data of many different sources using raw data that is highly unorganized as the most common practice. This kind of manual link can result into delay in detection of threat which is caused by too much notifications. A considerable portion of these alerts are false positives. This describes the situation where security personnel become frustrated with the constant barrage of alerts, making it difficult for him or her to detect actual dangers and respond accurately to them. A promising solution to these issues has been offered by Extended Detection and Response (XDR). It is another step forward in the development of security technologies [5].

Why Do We Need XDR?

XDR tackles most of the drawbacks that arise in traditional SIEM systems by going beyond log-level analysis and incorporating a more integrated and automated model-based security approach. Contrary to SIEM, which depends immensely on the manual correlation of large datasets, XDR pulls data directly from integrated sources of plenty security events across diverse layers and aligns them in real time. With the integrating features of XDR, security teams are also proven to detect and respond to threats much faster and more efficiently. This is especially the case when dealing with the more advanced multi-stage attacks that seem to be more common nowadays [1]. Although SIEM systems continue to be relevant in log management and regulatory compliance purposes, they are usually inadequate when it comes to complicated threats that need quick and seamless action. XDR may be viewed as a shift toward integrated detection and response strategy which focuses on effective defense mechanisms against modern cyber threats. Quite simply, as threats to organizations continue to become more complex, XDR becomes critical in the improvement of organizations' detection and response to threats [3].

A. Comparison of Security Solutions

*1) **Network Detection and Response (NDR):*** NDR or Network Detection and Response is a security practice that involves active monitoring and analysis of network traffic to identify abnormalities and threats, which tend to be at the network level. The growth of cybercrimes at the network level and their sophistication brought about the need for NDR to operate primarily on network packets as its data source and utilize anomaly detection methods to identify unusual network activities. Certain functions, like automating the blocking of harmful traffic to thwart risks, are also part of the package. As for NDR, it works with a low integration level with network tools and has provided visibility into traffic events in the network environment. So the ond lean to the other - network focused one, and yet deployment complexity and operational burden are medium sped so it is easy for most of the organizations. Accordingly, NDR systems are generally available at a mid-range budget ready to respond to the situational needs that are needed for the network focused security needs.

*2) **Extended Detection and Response (XDR):*** Extended Detection and Response (XDR) takes a holistic approach to security by extending detection across endpoints, networks, and cloud environments. By aggregating data from diverse sources such as servers, endpoints, and cloud platforms, XDR provides comprehensive threat visibility. It employs advanced analytics and correlation across vectors to detect sophisticated, multi-stage threats. XDR automates responses across multiple layers, ensuring seamless workflows between endpoints and networks. Although XDR requires significant deployment effort and entails higher operational overhead, its advanced integration and analytics capabilities justify its higher cost, making it suitable for organizations seeking comprehensive protection [4].

*3) **Endpoint Detection and Response (EDR):*** Endpoint Detection and Response (EDR) targets endpoint-level threats, offering detailed insights into device activities. It uses endpoint logs as its primary data source and employs a combination of signature-based and behavior-based detection techniques to identify threats. EDR also automates responses, such as isolating compromised endpoints to prevent threat propagation. While EDR integrates moderately with other security tools, its focus remains on endpoint security. The deployment complexity is low to moderate, with manageable operational overhead, and its moderate cost makes it accessible to a wide range of organizations.

*4) **Security Orchestration, Automation, and Response (SOAR):*** Security Orchestration, Automation, and Response (SOAR) focuses onaggregating alerts from various tools and coordinating responses rather than direct detection. SOAR combines data from multiple security sources, relying on predefined workflows and playbooks to streamline detection and response activities. Its automation capabilities enhance response efficiency, and its integration level is high, enabling seamless coordination across diverse security platforms [20]. SOAR provides a unified view of threats detected by integrated tools, though its deployment and operational overhead are significant. This, coupled with its high cost, reflects its advanced orchestration and automation functionalities.

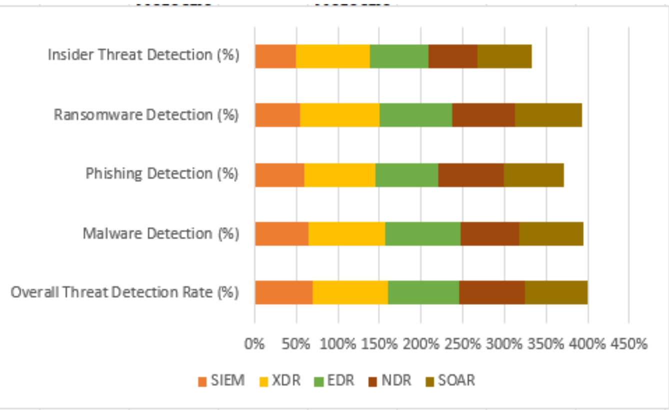


Fig. 1: Analysis between alternative of XDR

II. Related Work

As much as there is an advancement in technology, so does the corresponding increase in threats eeking to exploit these technological solutions and systems. Back in the day, technology such as Security Information and Event Management (SIEM) and Endpoint Detection and Response (EDR) were reliable as well as fundamental technologies in any organization that required cybersecurity measures. These solutions often, if not always, meet dissatisfaction in their intended purpose when it comes to addressing the intricate patterns typical of many modern multi-vector attacks targeting endpoints, networks, and cloud infrastructures in unison. Extended Detection and Response (XDR) now claims to address some this issues.

There is a paradigm shift in the landscape of security operations with XDR. By providing integration, automation, and visibility across security layers, it improves how security operations are conducted. Earlier assessments have also reported its potential to bring together multiple security tools and processes as a constructive shift against older practices. In this segment, however, the focus will be on advanced components of XDR such as integration, responsiveness and threat hunting while positioning it against existing tools and methodologies. Also, the ability of XDR to help alleviate skill gap in the cybersecurity teams and its ability to utilize efficient machine learning and be improved on even further strengthen.

A. Key Features of XDR

- **Stronger Building Blocks for Security Operations Centers:** XDR integrates security measures at various levels—endpoints, networks, cloud systems, and applications—into a unified system. This integration facilitates easier and more comprehensive data coordination, enabling security managers to pinpoint attacks that use multiple approaches [2].
- **Automatic Response Features:** XDR automates response measures based on predefined rules

and machine learning. Key automated responses include:

  - Isolating impacted systems,
  - Blocking malicious IP addresses,
  - Initiating pre-planned incident response procedures.

- **Professional Threat Hunt:** Enhanced analytics and machine learning capabilities enable XDR to:
  - Move beyond reactive defense strategies,
  - Identify patterns and anomalies suggesting a breach,
  - Assist security analysts in detecting blind spots within the environment.
- **Sophisticated Alerting Framework to Counter Alert Overload Problem:** XDR uses advanced correlation algorithms to:
  - Isolate distractions,
  - Categorize alerts based on risk levels.

  This aids security personnel in focusing resources on high-priority threats, reducing operational strain, and improving response times.
- **Improved Perspective Over All Other Environments:** XDR provides comprehensive visibility across multiple security layers, including:
  - Endpoints,
  - Network ,
  - Cloud environments .

  This visibility is critical for understanding the full impact of security breaches and conducting thorough post-incident analyses.

B. Drawbacks of XDR

While XDR is an advanced solution for enhancing security operations, there are certain challenges that organizations must be aware of before deploying it. These challenges may influence its overall effectiveness and suitability, depending on factors such as infrastructure complexity, available expertise, and organizational objectives.

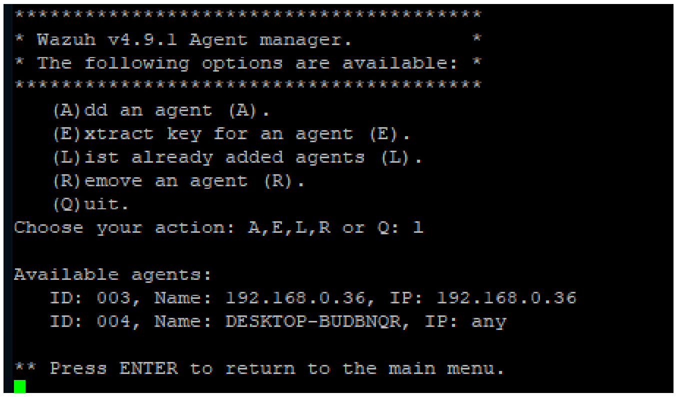
- **Limited Coverage Across Domains:** XDR solutions often excel in specific areas, like endpoint or network security, but they can face challenges in addressing broader environments such as hybrid or multi-cloud systems. This limitation arises from dependencies on proprietary technologies, such as endpoint agents, which may hinder the platform's ability to cover all threat vectors comprehensively[16]. Organizations should critically evaluate whether their chosen XDR platform aligns with their unique security needs.
- **Additional Costs and Investments:** Although XDR centralizes many security functionalities, implementing it can incur extra costs for additional tools and integrations, such as automation frameworks, SIEM systems, and threat intelligence feeds. These extra expenses can raise the overall cost of ownership, making XDR a resource-heavy investment for some organizations. Furthermore, differences in features across various providers can add complexity to the decision-making process, often requiring compromises [3].
- **Demand for Skilled Security Personnel:** Effective use of XDR systems relies heavily on skilled personnel. While the platform automates detection and response to a degree, human intervention is frequently needed to analyze alerts, investigate incidents, and refine operational workflows. For organizations lacking an established Security Operations Center (SOC), implementing XDR may place a significant strain on resources, necessitating further investment in training or hiring [4].
- **Limited Flexibility Beyond Predefined Use Cases:** Many XDR platforms include pre-configured playbooks, reports, and workflows tailored to common scenarios. While these features are beneficial for fast deployment, they may limit customization [21]. Organizations with specific or complex requirements might find extending the platform's capabilities challenging without advanced technical expertise.
- **Vendor Lock-In Risks:** A significant challenge with many XDR solutions is their tight integration with their own proprietary ecosystems. While this can simplify initial deployment, it also creates dependencies on the vendor's framework. This vendor lock-in can complicate transitions to alternative providers or integrating third-party tools, limiting flexibility and potentially hindering future innovation.

III. Methodology

The implementation of Wazuh as an open-source platform for security monitoring and extended detection and response (XDR) involves integrating several key components: Wazuh Manager, Wazuh Indexer, Wazuh Dashboard, and Wazuh Agents. Each of these components plays a critical role in creating a cohesive and robust security solution. This section describes the functionality and interaction of these components, while elaborating on the system's implementation process and features. Wazuh's application as an XDR solution enables the platform to detect and respond to security threats across a wide variety of data sources, combining endpoint security, network security, and threat intelligence into a unified system.

A. Key Components of Wazuh as XDR

*1) **Wazuh Manager**:* The Wazuh Manager serves as the heart of the platform. It collects, analyzes, and processes security data from endpoints where Wazuh Agents are installed, leveraging advanced rule-based event correlation engines to identify potential threats and policy violations. As an XDR solution, the Manager doesn't just focus on isolated security events but integrates threat intelligence, offering comprehensive detection capabilities across multiple data sources (e.g., network traffic, endpoint logs, and cloud environments). It generates alerts, enforces compliance measures, and facilitates incident response workflows by integrating with other security tools in the ecosystem, ensuring proactive threat mitigation.

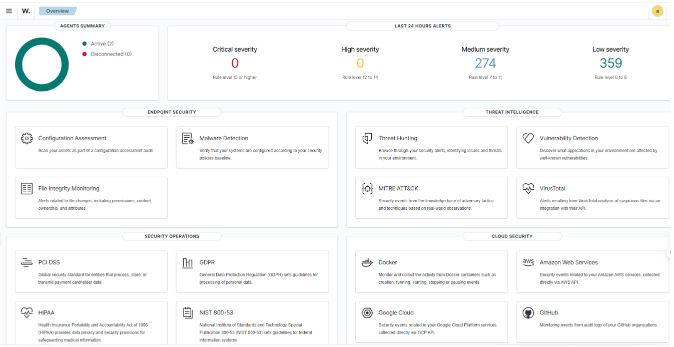


```
****************************************
* Wazuh v4.9.1 Agent manager.          *
* The following options are available: *
****************************************
   (A)dd an agent (A).
   (E)xtract key for an agent (E).
   (L)ist already added agents (L).
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R or Q: l

Available agents:
   ID: 003, Name: 192.168.0.36, IP: 192.168.0.36
   ID: 004, Name: DESKTOP-BUDBNQR, IP: any

** Press ENTER to return to the main menu.
```

Fig. 2: Agent Manager

*2) **Wazuh Indexer**:* Complementing the Manager is the Wazuh Indexer, a data storage and search engine powered by OpenSearch. The Indexer stores processed security logs and alerts received from the Manager, enabling efficient querying and retrieval of data. With Wazuh's XDR capabilities, the Indexer supports the aggregation of security data across diverse environments, ensuring that historical data and real-time event data are readily available for in-depth analysis. Its scalable architecture ensures that it can handle the large volumes of security telemetry required for effective XDR implementation, providing insights into attack trends and long-term security patterns.

*3) **Wazuh Dashboard**:* The **Wazuh Dashboard**, built on Kibana, provides a visual interface for monitoring, analyzing, and managing security events. As part of the XDR architecture, the Dashboard serves as a comprehensive visualization layer, offering real-time and historical insights into the organization's security posture. It allows security teams to correlate data from multiple sources and easily track the status of alerts, investigations, and responses. The customizable dashboards allow security teams to tailor visualizations to meet specific needs, making Wazuh's threat detection and incident response processes intuitive, actionable, and efficient.



AGENTS SUMMARY

Active (2)
Disconnected (0)

LAST 24 HOURS ALERTS

Critical severity 0 Rule level 15 or higher

High severity 0 Rule level 12 to 14

Medium severity 274 Rule level 7 to 11

Low severity 359 Rule level 0 to 6

ENDPOINT SECURITY

Configuration Assessment
Scan your assets as part of a configuration assessment audit.

Malware Detection
Verify that your systems are configured according to your security policies baseline.

File Integrity Monitoring
Alerts related to file changes, including permissions, content, ownership, and attributes.

THREAT INTELLIGENCE

Threat Hunting
Browse through your security alerts, identifying issues and threats in your environment.

Vulnerability Detection
Discover what applications in your environment are affected by well-known vulnerabilities.

MITRE ATT&CK
Security events from the knowledge base of adversary tactics and techniques based on real-world observations.

VirusTotal
Alerts resulting from VirusTotal analysis of suspicious files via an integration with their API.

SECURITY OPERATIONS

PCI DSS
Global security standard for entities that process, store, or transmit payment cardholder data.

GDPR
General Data Protection Regulation (GDPR) sets guidelines for processing of personal data.

HIPAA
Health Insurance Portability and Accountability Act of 1996 (HIPAA) provides data privacy and security provisions for safeguarding medical information.

NIST 800-53
National Institute of Standards and Technology Special Publication 800-53 (NIST 800-53) sets guidelines for federal information systems.

CLOUD SECURITY

Docker
Monitor and collect the activity from Docker containers such as creation, running, starting, stopping or pausing events.

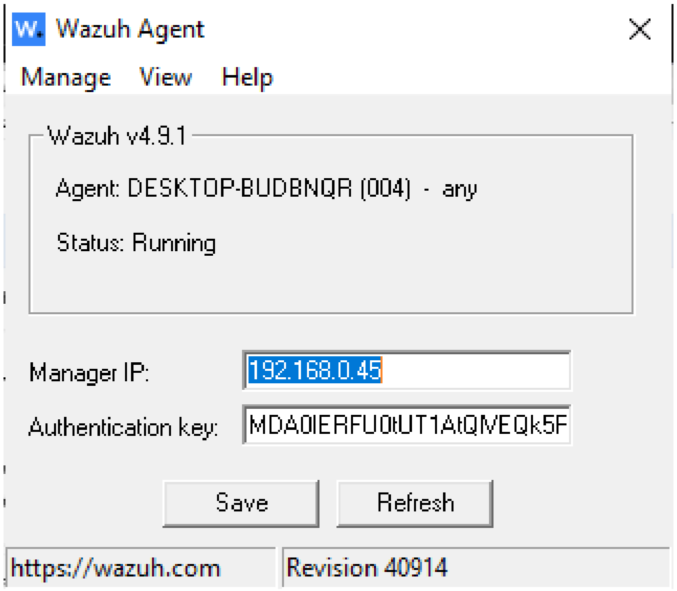
Amazon Web Services
Security events related to your Amazon AWS services, collected directly via AWS API.

Google Cloud
Security events related to your Google Cloud Platform services, collected directly via GCP API.

GitHub
Monitoring events from audit logs of your GitHub organizations.

Fig. 3: Wazuh Dashboard

*4) **Wazuh Agent**:* The Wazuh Agent, deployed on endpoints such as servers, desktops, and containers, acts as the primary data collector. This lightweight software monitors logs, tracks file integrity, evaluates configurations, and detects rootkits. In the context of Wazuh as an XDR solution, the Agent extends its monitoring capabilities to cover both endpoint and network activity, offering deeper visibility into the attack surface. Despite its comprehensive monitoring features, the Agent maintains a minimal resource footprint, ensuring that its presence does not significantly impact endpoint performance.



Wazuh v4.9.1

Agent: DESKTOP-BUDBNQR (004) - any

Status: Running

Manager IP: 192.168.0.45

Authentication key: MDA0IERFU0tUT1AtQlVEQk5F

https://wazuh.com

Revision 40914

Fig. 4: Wazuh Agent Setup

B. Communication Flow

The Wazuh platform operates with a strong emphasis on secure and streamlined communication among its various components. The data, collected by Wazuh Agents, undergoes encryption via Transport Layer Security (TLS) before transmission to the Wazuh Manager. Once received, the Manager analyzes the data using pre-configured security rules and generates alerts as necessary. These alerts, along with the processed logs, are then sent to the Indexer for efficient storage and retrieval. The Wazuh Dashboard subsequently interacts with the Indexer, allowing security teams to access and visualize both real-time insights and historical data trends.

This seamless data flow ensures that all components work in harmony, forming a cohesive security solution. By consolidating endpoint monitoring, network analysis, and threat intelligence, Wazuh creates a centralized platform for detecting and addressing security threats. As an XDR (Extended Detection and Response) solution, this architecture enhances an organization's ability to identify and mitigate risks across its entire infrastructure, ensuring a robust and proactive security posture.

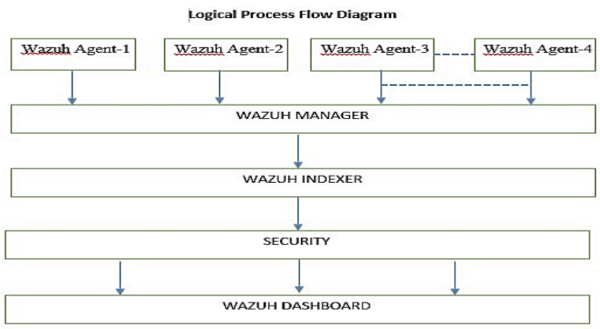


Fig. 5: Architecture flow of XDR

C. Feature Supporting Security Goals

Wazuh's robust feature set addresses critical aspects of organizational security, including security operations, endpoint security, and threat intelligence, all of which are key to effective XDR deployment.

- **Security Operations:** Wazuh consolidates logs from various sources (e.g., endpoints, network devices, applications) and applies sophisticated correlation rules to detect complex attack patterns. Its Intrusion Detection System (IDS) analyzes logs and behavior for known signatures of attacks, ensuring timely mitigation. As an XDR platform, Wazuh correlates data from across the infrastructure to detect multi-stage attacks and lateral movements, enhancing the ability to identify threats that span across endpoints, networks, and cloud environments [17]. Wazuh also supports compliance reporting for standards like GDPR, HIPAA, and PCI DSS, significantly reducing the administrative burden of regulatory adherence.

- **Endpoint Security:** Wazuh monitors file integrity, detecting unauthorized changes to critical files and directories. Its rootkit detection capabilities uncover hidden malicious processes, while configuration assessments ensure that endpoints meet industry-standard security benchmarks [13]. As an XDR solution, Wazuh leverages these endpoint security features to offer comprehensive threat detection and response capabilities, proactively defending against a wide range of endpoint-based attacks.

- **Threat Intelligence:** Wazuh integrates with external threat intelligence feeds to stay updated on emerging vulnerabilities and exploits. Its anomaly detection identifies behavioral deviations that may signal unknown threats, providing early detection for threats that evade traditional signature-based methods [18]. In an XDR context, Wazuh combines external threat intelligence, endpoint activity, and network behavior to offer a more holistic view of the security landscape, enabling precise and timely responses to ncidents.

D. Implementation Process

The deployment of Wazuh as an XDR solution can be effectively achieved through a series of structured steps. Below is a detailed outline of the implementation process, ensuring both clarity and functionality:

1) **Setting up the Virtual Environment:** To begin, a virtual machine is configured to host the key Wazuh components: the Wazuh Manager, Wazuh Indexer, and Wazuh Dashboard. Tools such as Oracle VirtualBox are used to create this environment. The virtual machine is provisioned with sufficient resources to ensure seamless operation of these integrated components. Each component plays a critical role—data collection and analysis by the Manager, efficient data storage and querying by the Indexer, and real-time visualization by the Dashboard.
2) **Deploying Wazuh Agents:** Wazuh Agents are installed on endpoint devices, including servers and workstations. These lightweight agents are configured to securely communicate with the Wazuh Manager, collecting relevant system logs, application logs, and other critical data. Secure communication protocols such as Transport Layer Security (TLS) are employed to ensure the data remains encrypted and protected.
3) **Customizing the System:** After deployment, the system is tailored to meet organizational security requirements. This involves editing configuration files to define the type of data collected, setting detection rules, and determining alert thresholds. Additionally, automated responses are configured to address specific scenarios, such as sending alerts, isolating affected endpoints, or blocking suspicious activities.
4) **Operationalizing the Dashboard:** Once validated, the Wazuh Dashboard becomes the central interface for security teams. It enables monitoring of live events, management of alerts, and generation of compliance reports. This provides teams with actionable insights and comprehensive visibility across endpoints, networks, and cloud environments.
5) **Ongoing Maintenance and Updates:** To ensure the system remains effective against evolving threats, regular updates and maintenance are conducted. This includes integrating the latest threat intelligence, refining detection methods, and adapting configurations to meet new security challenges.

By following these steps, Wazuh delivers a robust and scalable XDR platform. It empowers organizations to proactively identify and respond to cyber threats.

TABLE I: Comparison of Different XDR Platforms

Feature	**Wazuh (Open Source)**	**CrowdStrike Falcon (Cloud-based)**	**Microsoft Defender XDR (Integrated)**	**Palo Alto Networks Cortex XDR (Hybrid)**	**SentinelOne Singularity XDR (AI-driven)**
Deployment Model	Flexible deployment on-premises or in the cloud. Ideal for businesses with diverse infrastructures[7].	Fully cloud-based, enabling scalability and accessibility from anywhere [9].	Fully integrated with Microsoft 365 for organizations already in its ecosystem.	Hybrid approach supporting cloud and on-prem environments for maximum versatility.	Cloud-first with optional on-premises agents, offering adaptability for various setups.
Integration	Supports a wide array of third-party tools for enhanced compatibility with existing ecosystems[8].	Seamlessly integrates with the Falcon platform for unified threat management [9].	Works natively with other Microsoft services, creating a cohesive experience.	Extensive compatibility with third-party tools, enhancing overall functionality.	Designed for easy API integration with third-party tools and enterprise platforms.
Data Sources	Collects data from endpoints, servers, and cloud environments for a broad security perspective.	Focuses on endpoint and network data, emphasizing real-time detection.	Monitors endpoints, emails, and networks for comprehensive coverage.	Integrates data from endpoints, networks, and cloud environments for deep visibility.	Analyzes endpoint, network, and application telemetry for holistic security insights.
Threat Detection	Relies on behavioral analytics to identify unusual patterns and potential risks.	Uses advanced machine learning to proactively detect and respond to threats.	Employs AI and ML for proactive and intelligent threat identification.	Uses analytics to uncover sophisticated attack methods across environments.	Powered by AI to autonomously detect and contain threats in real-time.
Response Capabilities	Automates remediation to address issues quickly and efficiently.	Offers a mix of automated and manual options for flexible responses.	Automates incident response with predefined playbooks for rapid action.	Provides both automated and manual options for customizable responses.	Fully autonomous responses with optional manual intervention when required.
User Interface	Simple and user-friendly dashboard for managing security events.	Intuitive interface designed to streamline operations and reduce complexity.	Integrated dashboard within Microsoft Security Center for ease of use.	Customizable dashboards tailored to user preferences for better navigation.	Modern interface focused on simplicity and efficiency in security management.
Pricing	Free and open-source, accessible to organizations with budget constraints.	Subscription-based model, scalable for growing businesses but may be costly for small setups.	Subscription aligned with Microsoft 365, making it cost-effective for existing customers.	Tiered subscription plans offering flexibility based on organizational needs [11].	Subscription pricing tailored to feature sets and enterprise scalability.
Scalability	Highly scalable for organizations of all sizes, from startups to large enterprises.	Cloud-native design ensures scalability for enterprises with expanding needs.	Scales effortlessly alongside Microsoft 365 infrastructure.	Adapts to varying business sizes, supporting hybrid architectures.	Scalable architecture supports dynamic environments and future growth[23].

IV. Results

The research paper explores the implementation and effectiveness of Extended Detection and Response (XDR) using Wazuh, an open-source security platform. XDR enhances cybersecurity by integrating security measures across various environments—endpoints, networks, and cloud platforms—addressing limitations in traditional Security Information and Event Management (SIEM) systems. The paper outlines Wazuh's architecture, which includes components like the Wazuh Manager, Indexer, Dashboard, and Agents, all of which work together to provide robust threat detection, compliance management, and real-time insights via an intuitive dashboard.

The study highlights several benefits of XDR with Wazuh, including automated responses, better threat visibility, and reduced alert fatigue through advanced correlation algorithms. Wazuh's integration with external threat intelligence and machine learning boosts its ability to detect complex threats. However, the paper also identifies challenges such as high implementation costs, reliance on skilled personnel, and potential limitations in coverage. Other concerns include vendor lock-in and limited customization beyond predefined scenarios. Despite these hurdles, the study concludes that XDR, as demonstrated by Wazuh, represents a significant advancement in cybersecurity, offering a proactive, integrated approach that suits various organizational needs when implemented with proper planning and resources.

V. Conclusion

When looking closer at Wazuh as an example of Extended Detection and Response (XDR) systems, it is clear that progress in cybersecurity practice has been made. Within traditional Security Information and Event Management (SIEM) systems manual data correlation and alert management is most tedious and therefore causes lags in threat detection and response. Those issues are solved in XDR, where several security products are combined, response is automated and visibility is provided across different environments.

As an open-source XDR platform, Wazuh provides a cost-effective solution that is easy to customize to suit the requirements of different organizations. The structure of a Wazuh system which consists of Wazuh Manager, Wazuh Indexer, Wazuh Dashboard, and Wazuh Agents is very efficient in data collection, processing, and visualization. Such integration improves the processes of detecting threats and processing incidents.

However, going for an XDR solution like Wazuh is not without possible challenges. Such challenges include the ability to provide an appropriate level of security across all domains, higher costs associated with additional tools that may be necessary, and the absence of qualified staff for the effective operation of the system.

In conclusion, those efforts can be crowned with success as definitely, such approaches are already represented by working systems which are XDR solutions such as Wazuh, XDR is a big leap in the evolution of different cybersecurity approaches. They provide better threat detection

References

[1] M. Nicholls, ”MDR vs MSSP vs SIEM: A Guide to Threat Detection,” *Redscan*, Aug. 22, 2023. [Online]. Available: https://www.redscan.com/news/mdr-vs-mssp-vs-siem-guide/.

[2] Zenarmor, ”What is Extended Detection and Response (XDR)? Benefits, Components, and Best Practices,” *Zenarmor Documentation*. [Online]. Available: https://www.zenarmor.com/docs/network-security-tutorials/whatis-extended-detection-and-response-xdr.

[3] Heimdal Security, ”SIEM vs XDR: A Comparison of Two Advanced Detection and Response Solutions,” *Heimdal Security Blog*, Apr. 20, 2023. [Online]. Available: https://heimdalsecurity.com/blog/siem-vs-xdr-a-comparison-of-twoadvanced-detection-and-response-solutions/.

[4] Check Point Software, ”XDR Security - What is Extended Detection and Response?” *Check Point Software*. [Online]. Available: https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-xdr-extendeddetection-and-response/.

[5] Check Point Software, ”XDR vs. SIEM,” *Check Point Software*. [Online]. Available: https://www.checkpoint.com/cyberhub/threat-prevention/what-is-xdr-extended-detection-and-response/xdr-vs-siem/.

[6] F. Mulyadi, L. A. Annam, R. Promya, and C. Charnsripinyo, ”Implementing Dockerized Elastic Stack for Security Information and Event Management,” in *5th International Conference on Information Technology*, 2020, pp. 1–7. doi: 10.1109/InCIT50588.2020.9310950.

[7] S. Moiz, A. Majid, A. Basit, M. Ebrahim, A. A. Abro, and M. Naeem, ”Security and Threat Detection through Cloud-Based Wazuh Deployment,” in *2024 IEEE 1st Karachi Section Humanitarian Technology Conference (KHI-HTC)*, Tandojam, Pakistan, 2024, pp. 1–5. doi: 10.1109/KHI-HTC60760.2024.10482206.

[8] J. Brown, ”Understanding Open-Source Security Solutions: Wazuh and Its Applications,” *International Journal of Cybersecurity Research*, vol. 15, no. 3, pp. 45–57, 2023.

[9] T. Davis, ”CrowdStrike Falcon: Leading Cloud-Based Threat Protection,” *Cyber Defense Insights*, vol. 11, no. 2, pp. 22–34, 2022.

[10] M. Green, ”Microsoft Defender XDR: Enhancing Security Through Integration,” *Enterprise Security Journal*, vol. 8, no. 1, pp. 18–27, 2023.

[11] K. Johnson, ”Hybrid XDR Solutions: An Analysis of Cortex XDR,” *IT Security Quarterly*, vol. 10, no. 4, pp. 30–42, 2023.

[12] S. Carter, ”The Rise of AI-Powered XDR: A Deep Dive into SentinelOne Singularity,” *Security Today*, vol. 14, no. 2, pp. 40–52, 2023.

[13] R. Johnson, ”XDR and the SOC: Skills Gap Analysis,” *Security Today*, vol. 15, no. 1, pp. 10–21, 2023.

[14] J. Smith, ”Challenges in XDR Implementation,” *Cybersecurity Journal*, vol. 12, no. 4, pp. 34–47, 2022.

[15] M. Davis, ”Evaluating XDR Flexibility,” *Journal of Advanced Threat Detection*, vol. 9, no. 3, pp. 56–69, 2022.

[16] K. Green, ”Vendor Lock-in Risks in Cybersecurity,” *Enterprise Security Journal*, vol. 7, no. 2, pp. 50–61, 2023.

[17] P. Robinson, ”Emerging Trends in XDR and Threat Detection,” *Journal of Network Security*, vol. 19, no. 1, pp. 10–22, 2024.

[18] A. Lee, ”Integrating XDR with Legacy Security Systems: Opportunities and Challenges,” *Computers & Security Review*, vol. 40, no. 5, pp. 78–92, 2023.

[19] N. White, ”The Role of Machine Learning in XDR Platforms,” *AI in Cybersecurity Journal*, vol. 13, no. 3, pp. 45–58, 2023.

[20] G. Mitchell, ”Optimizing Security Operations with SOAR: A Comprehensive Guide,” *Journal of Cybersecurity Operations*, vol. 16, no. 4, pp. 45–60, 2023. [Online]. Available: https://www.cybersecurityjournal.com/soar-comprehensive-guide.

[21] A. S. George, A. S. H. George, T. Baskar, and D. Pandey, ”XDR: The Evolution of Endpoint Security Solutions - Superior Extensibility and Analytics to Satisfy the Organizational Needs of the Future,” *Masters IT Solutions, Chennai, Tamil Nadu, India*, vol. 5.731, pp. 1-4, 2023.