The 13th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications
4-6 September, 2025, Gliwice, Poland

A Testbed for Cyber Attack Emulation and AI-Driven Anomaly Detection in Industrial IoT- and OT-Networks

Jaafer Rahmani[1] , Kai Oliver Detken[2] , Axel Sikora[3]
[1,3] ivESK, Offenburg University, Offenburg, Germany, jaafer.rahmani@hs-offenburg.de, axel.sikora@hs-offenburg.de
[2] DECOIT GmbH & Co. KG, Bremen, Germany, detken@decoit.de

Abstract — **Legacy Industrial Control System protocols, such as Modbus, expose critical vulnerabilities in Industrial IoT environments, underscoring the urgent need for advanced security solutions. Our Operational Technology testbed is purpose-built to emulate realistic Industrial Control Network scenarios by integrating essential IT and OT components, including an Engineering Workstation and a Human-Machine Interface for supervisory control, along with Programmable Logic Controllers, an MQTT broker, and a smart switch for VLAN segmentation, in order to replicate the complexities of modern industrial networks. Together, these components form the core of our testbed, enabling not only the simulation of cyber-attack scenarios but also the generation of rich, high-fidelity datasets that are critical for training AI-based anomaly detection models. To our knowledge, this is the first generic cyber attack testbed for deep field buses, enabling systematic attacks and analyses. The collected data, which encompasses network traffic, telemetry, and host logs, is processed through a centralized Elastic Security Information and Event Management system augmented by local monitoring tools such as NetFlow, Auditd, and Zeek. This paper details the design, implementation, and evaluation of our testbed, demonstrating its adaptability to emulate various attack scenarios and its effectiveness in producing datasets that advance cybersecurity in Industrial Control networks.**

Keywords* — *OT, Industrial IoT, Industrial Control Networks, Modbus, Cyber-Attack Emulation, AI-Based Anomaly Detection, SIEM, Dataset Generation, Network Traffic Analysis.

I. Introduction

Industrial Control Systems (ICS) are essential components that support and manage the operations of critical infrastructure sectors, including but not limited to energy production, manufacturing processes, transportation systems, and water treatment facilities. These systems provide the necessary control and monitoring capabilities to ensure that industrial operations run smoothly and efficiently [1].

One of the challenges faced by ICS is their reliance on legacy communication protocols, such as Modbus/TCP (Modbus/Transmission Control Protocol) and PROFINET (Process Fieldbus Network). These protocols were initially developed with a focus on reliability and operational continuity in isolated environments, where the risk of external threats was minimal. As a result, they were not built with modern cybersecurity considerations in mind, such as encryption to secure data transmission and authentication mechanisms to verify the identity of users and devices interacting with the system [2].

In today's interconnected environment, where ICS components are increasingly networked and connected to the Internet through Industrial Internet of Things (IIoT) architectures, the vulnerabilities associated with these outdated protocols become more pronounced. Cybersecurity threats, including malware, hacking attempts, and other malicious activities, pose significant risks to the integrity and reliability of industrial operations [3]. While existing security research has produced valuable domain-specific testbeds, they often fail to address cross-industry threats and complex attack vectors characteristic of modern Advanced Persistent Threats (APTs). To address these limitations, we present a novel testbed that integrates both IT and OT components to create a high-fidelity representation of industrial control networks, enabling systematic attack emulation and the generation of comprehensive datasets critical for developing effective AI-based anomaly detection systems.

II. State of the Art

Modern industrial cybersecurity research has evolved through three generations of testbed architectures, each addressing different aspects of ICS protection:

A. Legacy Protocol Vulnerabilities

The security limitations of industrial protocols like Modbus/TCP are well-documented. Mamun and Rahman [4] demonstrated how these protocols remain vulnerable to denial-of-service attacks that can disrupt critical operations. As IIoT adoption increases, traditionally isolated Operational Technology (OT) networks now face

This work was executed in the project ”KISTE - AI-powered SIEM System for Highly Reliable Industrial IoT Networks and Fieldbuses”, supported by the German Federal Ministry for Economic Affairs and Climate Action(BMWK), based on a decision of the German Bundestag under grant number ”KK5189606RG4”.

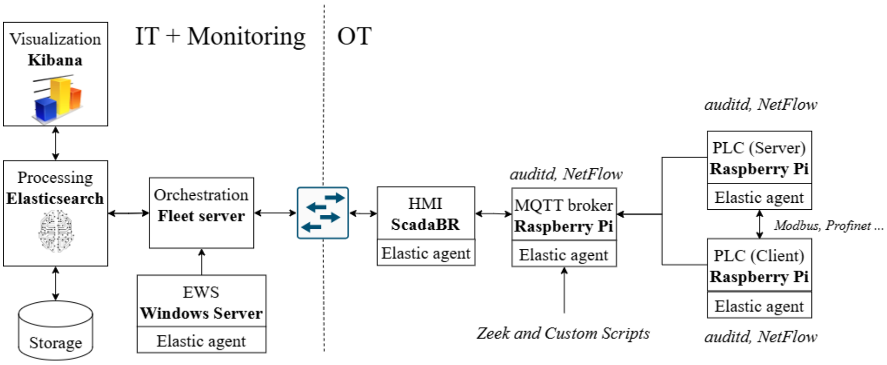


Figure 1. Testbed Architecture

sophisticated threats including ransomware [5] and botnet attacks [6]. The distributed nature of modern botnets presents particular challenges for industrial environments, as demonstrated by Savenko et al. [7], who showed that traditional centralized detection approaches fail to address the scalability and coordination requirements of distributed botnet detection in large-scale networked systems. Conventional security measures like firewalls and signature-based IDS struggle with IIoT's heterogeneous environments [8], creating demand for more adaptable solutions.

B. Domain-Specific Testbeds

Early research focused on vertical-specific platforms:

- Power systems: CPGrid-OT [9] for DNP3 protocol analysis
- Nuclear plants: Modbus-focused testbeds [10]
- Chemical processes: False data injection studies [11]

While valuable within their domains, these testbeds share common limitations:

- Single-protocol focus unable to analyze cross-industry threats
- Emphasis on simple attack vectors (e.g., DoS) rather than multi-stage APTs
- Lack of modern network segmentation features like VLANs

C. Cross-Domain Architectures

Foundational works like Hahn et al. [12] established cyber-physical co-simulation principles but predate today's converged IT/OT environments. More recent frameworks like ICSSIM [13] offer customization but require extensive configuration for complex attack scenarios. Protocol-aware monitoring solutions [14] have advanced anomaly detection but often neglect endpoint security data.

Contemporary approaches to intrusion detection have increasingly leveraged advanced machine learning techniques for improved threat identification. Hamolia et al. [15] demonstrated the effectiveness of latent space representation combined with machine learning algorithms for network intrusion detection, achieving enhanced detection capabilities through dimensional reduction and pattern recognition in high-dimensional network data. This approach addresses the challenge of processing complex, multi-dimensional network telemetry—a critical requirement for modern ICS environments where traditional signature-based detection methods prove insufficient against sophisticated attack vectors.

D. Research Gaps

Current testbed architectures grapple with two primary challenges that hinder their effectiveness in the evolving cybersecurity terrain:

- **Vertical Limitations**: Many specialized testbed designs, as exemplified by works such as [9], restrict their applicability across different industrial sectors, curtailing the potential for broader insights and learnings that could enhance overall cybersecurity frameworks.
- **Attack Complexity**: The majority of existing platforms fail to emulate the advanced tactics characteristic of modern APTs, such as lateral movement and process impairment [16], which are increasingly prevalent in sophisticated cyber attacks. Additionally, the distributed nature of contemporary threats, particularly botnets that can coordinate across multiple industrial networks, requires detection approaches that can operate effectively in distributed environments [7].

Our proposed testbed addresses these critical gaps in the current research landscape through innovative features designed to replicate and analyze complex attack scenarios:

- **Multi-level Monitoring**: Our system incorporates a consolidated approach to monitoring with specialized integrations, collecting network (Netflow), host (auditd), and protocol-based (Zeek) features simultaneously. This enables the generation of higher quality, feature-rich data critical for accurate threat analysis and incident response, supporting advanced machine

learning approaches that can benefit from latent space representations of complex network behaviors [15].
- **Multi-Stage APT Emulation**: We provide a comprehensive emulation environment that facilitates the replication of multi-stage attack sequences, such as credential compromise leading to VLAN hopping and succeeding in process impairment. This allows for a more nuanced understanding of the implications of layered attacks on ICS environments.

III. Methodology

Our methodology is organized into three interdependent components that ensure our testbed, shown in Fig. 2, is adaptable for emulating various attack scenarios and generating high-quality datasets for anomaly detection:

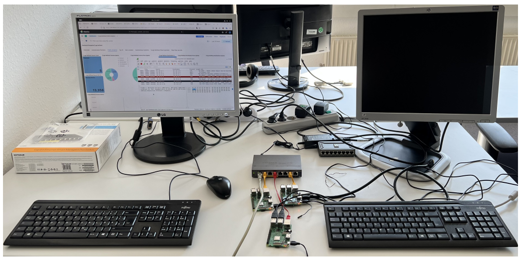


Figure 2. Testbed Setup

1) **Operational Environment Setup:** This component focuses on replicating the complexities of real-world ICS networks. By integrating both IT and OT elements—including the EWS for administrative control, the HMI for supervisory control, Raspberry Pis as PLCs, an MQTT broker, and a smart switch for VLAN segmentation—the testbed ensures a realistic simulation environment.
   Comparison with Existing Testbeds: Our approach addresses different requirements compared to established frameworks:
   - **vs. CPGrid-OT [9]:** While CPGrid-OT specializes in power grid SCADA simulations, our testbed targets broader industrial environments with multi-protocol support (Modbus, MQTT) and integrated SIEM capabilities.
   - **vs. ICSSIM [13]:** ICSSIM provides comprehensive virtualized industrial process simulation, whereas our hybrid approach combines physical edge devices with virtualized components to capture realistic network characteristics.

   The centralized ELK SIEM, combined with monitoring integrations (NetFlow, Auditd, and Zeek), captures a diverse, multi-layered dataset that serves as the baseline for anomaly detection. The concept of integrating data from multiple abstraction layers is directly applicable here. In our testbed, collecting data from the network, host, and protocol layers provides a holistic view of ICS operations, enabling detection of subtle deviations that may indicate sophisticated cyberattacks.
2) **Cyber-Attack Emulation Capability:** This component is designed to emulate cyber-attack scenarios, with current implementation focusing on proof-of-concept development:
   - **Modbus-based Attacks:** We have developed initial proof-of-concept implementations targeting Modbus/TCP packets and register manipulation. These scenarios are structured into phases (Initial Access, Privilege Escalation, Discovery, Lateral Movement, and Execution) following established attack methodologies. The complete implementation and validation results are planned to be expanded and published in IEEE ICEST 2025.
   - **Multi-stage Attack Chains:** Framework design supports progression from HMI compromise through network reconnaissance to PLC manipulation, with implementation ongoing.
3) **Dataset Generation for Anomaly Detection:** By capturing and correlating data from both normal and attack conditions, our testbed generates comprehensive datasets that include network traffic, sensor telemetry, and host logs. The multi-layer monitoring approach enables collection of correlated events across network, protocol, and host levels:
   - **Multi-Layer Coverage:** Network flows (NetFlow), protocol transactions (Zeek), and host events (Auditd) are captured simultaneously.
   - **Attack Scenario Labeling:** Attack scenarios are systematically labeled according to MITRE ATT&CK for ICS framework.
   - **Temporal Synchronization:** All monitoring systems are time-synchronized to enable cross-layer event correlation analysis.

   This integrated dataset approach is designed to support training and validation of AI-based anomaly detection models. Advanced techniques, including federated learning, are planned for future implementation following completion of the attack emulation capabilities and empirical validation.

Together, these components form a cohesive methodology that addresses the security evaluation of ICS networks through systematic attack emulation and comprehensive data collection.

IV. Lab Setup and Architecture

Our testbed emulates a realistic ICS network environment by integrating distinct IT and OT components, along with network expansion and segmentation, to mirror modern industrial architectures, as shown in Fig. 1.

A. *IT Setup*

- **Central ELK SIEM:** The ELK stack comprises Elasticsearch for log storage, Logstash for processing, and Kibana for visualization. **A Fleet server** ensures that deployed Elastic Agents across the IT and OT environments remain healthy and actively export log data. Comprehensive agent policies, including integrations for NetFlow, Auditd, Zeek and system logs, coupled with Wireshark captures, enable the collection and indexing of data from across the OT network. This approach, inspired by [8], is critical for generating high-quality datasets for machine learning applications.
- **Engineering Workstation (EWS):** Deployed as a Windows Server 2019 Virtual Machine, the EWS serves as the administrative hub for the testbed. It is responsible for IT systems' configuration and management, replicating some of the central command functions observed in real-world ICS deployments.

B. *OT Setup*

- **Raspberry Pis:** Serving as PLCs and Modbus server/clients, these devices run Elastic Agents with integrations for NetFlow, Auditd, and System monitoring. They capture detailed communication data over Modbus and PROFINET, with plans for future integration of TSN networks. This configuration is crucial for replicating the diverse communication patterns observed in ICS environments [8].
- **MQTT Broker:** The MQTT broker is equipped with Zeek and a custom telemetry collection script. It monitors both telemetry and network traffic, forwarding subtle protocol-level events to the central Elastic SIEM. This design ensures comprehensive data capture across multiple layers, which is essential for both forensic analysis and anomaly detection.
- **Human-Machine Interface (HMI):** Deployed as a SCADA system (via a ScadaBR Virtual Machine), the HMI provides real-time visualization and control of industrial processes. It displays key operational parameters, system statuses, and alarms, thereby enabling operators to monitor the ICS environment effectively. In our testbed, the HMI is essential for simulating supervisory control and for capturing dynamic operational data during both normal and attack scenarios.

C. *Network Expansion and VLAN Segmentation*

- **Netgear GS108PEv3 Smart Switch:** Implementing VLAN segmentation, this smart switch simulates segmented ICS environments, closely mirroring real-world industrial architectures. It enables the study of additional attack vectors, such as VLAN hopping and lateral movement, thereby enhancing the diversity and richness of the collected data.

V. Preliminary Results and Discussion

A. *Key Innovations*

Our testbed introduces three key innovations distinguishing it from existing ICS security platforms. First, unlike domain-specific platforms such as CPGrid-OT (power systems) or nuclear-focused testbeds, we provide the first multi-protocol cross-industry testbed simultaneously supporting Modbus, MQTT, and PROFINET. Second, we achieve the first real-time integration of NetFlow, Auditd, and Zeek within a unified SIEM framework for ICS environments, providing comprehensive three-layer monitoring. Third, our novel hybrid physical-virtual architecture combines physical edge devices with virtualized components to capture realistic industrial network characteristics while maintaining research flexibility.

B. *Multi-Layer Data Validation*

Our dashboard captures (Figs. 3, 4, 5) demonstrate successful comprehensive data collection across three critical layers. The network layer provides complete visibility of inter-device communications, protocol identification, and VLAN segmentation. The host layer captures process execution, file access, authentication events, and privilege changes across all monitored devices. The protocol layer delivers deep packet inspection of Modbus function codes, MQTT topics, and HTTP/HTTPS traffic patterns.

C. *Comparative Analysis*

Table I compares our testbed against CPGrid-OT and ICSSIM, based on their published capabilities. Our platform offers broader protocol support, unified three-layer monitoring, and integrated SIEM, which the others lack out-of-the-box.

The integration of NetFlow, Auditd, and Zeek enables unprecedented cross-layer event correlation and comprehensive forensic analysis capabilities not available in domain-specific systems. While CPGrid-OT [9] excels within power grid environments and ICSSIM [13] provides detailed process simulation, our approach uniquely combines enterprise-grade SIEM capabilities with multi-protocol ICS monitoring, enabling comprehensive threat detection across diverse industrial sectors with real-time correlation and standardized data export capabilities.

VI. Conclusion and Future Work

A. *Contributions*

This study delivers concrete contributions to ICS cybersecurity research through several technical innovations. We have developed the first cross-industry testbed supporting multiple industrial protocols simultaneously, achieved novel three-layer data integration (network, host, protocol) within enterprise SIEM infrastructure, and created a hybrid architecture combining physical devices with virtualized IT components. Our MITRE ATT&CK-based framework enables systematic attack scenario development and validation. These innovations establish

Table I. TESTBED CAPABILITY COMPARISON

Capability	Our Testbed	CPGrid-OT [9]	ICSSIM [13]
Protocol Support	**Modbus/TCP, MQTT, PROFINET**	DNP3 primary; IEC 61850 demonstrated	User-defined modules (e.g., Modbus/TCP)
Integrated Monitoring	**Unified: network + host + protocol**	Separate IT/OT network monitoring	Process simulation + network logging
SIEM Integration	**Embedded ELK (real-time)**	None	File-based logs (no native SIEM)
Cross-Layer Correlation	**Automated correlation scripted engine**	Manual event matching	None
Attack Framework	**MITRE ATT&CK ICS playbooks**	Scenario scripts (DoS, spoofing)	Process-level attack scripts
Data Export	**CSV, JSON, ES indices**	Standard power formats (CSV/JSON)	Proprietary format (CSV via scripts)
Edge Integration	**Agents on physical/virtual edges**	Centralized hardware	Centralized host

a new benchmark for multi-dimensional ICS security data collection, demonstrate the feasibility of cross-layer event correlation, and create a replicable methodology for comprehensive industrial network monitoring and AI-driven security solutions.

B. Limitations and Future Work

We acknowledge that Raspberry Pi devices cannot replicate sub-millisecond PLC response times required for real-time control validation, current attack scenarios focus primarily on Modbus with other protocols under development, and our testbed scale is suitable for research but requires expansion for full industrial validation. Our structured future work addresses these limitations through expansion of protocol support to OPC-UA among others, and deployment in industrial partner environments. Long-term goals include integration of federated learning for distributed anomaly detection, and establishment of industry standards for ICS security testbed evaluation.

DECLARATION ON GENERATIVE AI

During the preparation of this work, the author(s) used Grammarly in order to: Grammar and spelling check, Paraphrase and reword. After using this tool/service, the author(s) reviewed and edited the content as needed and take(s) full responsibility for the publication's content.

REFERENCES

[1] D. Bhamare, M. Zolanvari, A. Erbad, R. Jain, K. Khan, and N. Meskin, "Cybersecurity for industrial control systems: A survey," *Computers Security*, vol. 89, p. 101677, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404819302172

[2] M. K. Ferst, H. F. M. de Figueiredo, G. Denardin, and J. Lopes, "Implementation of secure communication with modbus and transport layer security protocols," in *2018 13th IEEE International Conference on Industry Applications (INDUSCON)*, 2018, pp. 155–162.

[3] B. Chen, N. Pattanaik, A. Goulart, K. L. Butler-purry, and D. Kundur, "Implementing attacks for modbus/tcp protocol in a real-time cyber physical system test bed," in *2015 IEEE International Workshop Technical Committee on Communications Quality and Reliability (CQR)*, 2015, pp. 1–6.

[4] M. A. A. Mamun and M. A. Rahman, "Launch of denial of service attacks on the modbus/tcp protocol and detection mechanisms," *Journal of Information Security and Applications*, vol. 54, p. 102554, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S187454822200052X

[5] D. Formby, S. Durbha, and R. Beyah, "Out of control: Ransomware for industrial control systems," in *RSA conference*, vol. 4, 2017, p. 8.

[6] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis *et al.*, "Understanding the mirai botnet," in *26th USENIX security symposium (USENIX Security 17)*, 2017, pp. 1093–1110.

[7] O. Savenko, A. Sachenko, S. Lysenko, G. Markowsky, and N. Vasylkiv, "Botnet detection approach based on the distributed systems," *International Journal of Computing*, vol. 19, no. 2, pp. 190–198, 2020.

[8] S. S. Sahoo and M. A. Rahman, "Testbeds and evaluation frameworks for anomaly detection within built environments: A review," *ACM Transactions on Cyber-Physical Systems*, vol. 6, no. 4, pp. 1–24, 2022. [Online]. Available: https://dl.acm.org/doi/pdf/10.1145/3722213

[9] H. M. Mustafa, S. Basumallik, A. Srivastava, and S. Kidder, "CPGrid-OT: Cyber-Power Data Generation Using Real-Time Reconfigurable Testbed for Resiliency." institute of electrical electronics engineers, May 2023, pp. 1–6.

[10] I. B. de Brito and R. T. de Sousa, "Development of an open-source testbed based on the modbus protocol for cybersecurity analysis of nuclear power plants," *Applied Sciences*, vol. 12, no. 15, 2022. [Online]. Available: https://www.mdpi.com/2076-3417/12/15/7942

[11] M. Noorizadeh, K. Khorasani, D. Unal, M. Shakerpour, and N. Meskin, "A Cyber-Security Methodology for a Cyber-Physical Industrial Control System Testbed," *IEEE Access*, vol. 9, pp. 16 239–16 253, Jan. 2021.

[12] A. Hahn, M. Govindarasu, A. Ashok, and S. Sridhar, "Cyber-Physical Security Testbeds: Architecture, Application, and Evaluation for Smart Grid," *IEEE Transactions on Smart Grid*, vol. 4, no. 2, pp. 847–855, Jun. 2013.

[13] A. Dehlaghi-Ghadim, A. Balador, M. H. Moghadam, H. Hansson, and M. Conti, "Icssim — a framework for building industrial control systems security testbeds," *Computers in Industry*, vol. 148, p. 103906, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0166361523000568

[14] A. T. Zahary, N. A. Al-shaibany, and A. Sikora, "A review of intrusion detection systems for the internet of things," in *Proceedings of the 1st International Conference on Emerging Technologies for Dependable Internet of Things (ICETI 2024)*, 2024, pp. 1–6.

[15] V. Hamolia, V. Melnyk, P. Zhezhnych, and A. Shilinh, "Intrusion detection in computer networks using latent space representation and machine learning," *International Journal of Computing*, vol. 19, no. 3, pp. 442–448, 2020.

[16] C. Zou, "Modbus-based industrial control system attack," 2021. [Online]. Available: https://cyberforensic.net/labs/modbus-attack.html

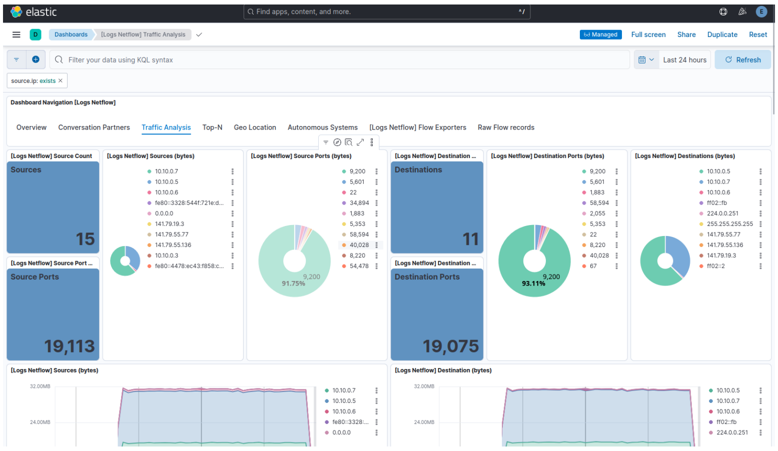
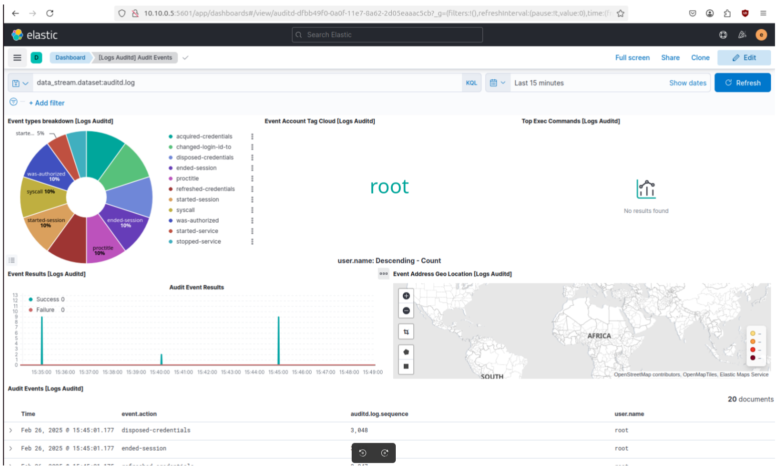


Figure 3. NetFlow Detailed Capture

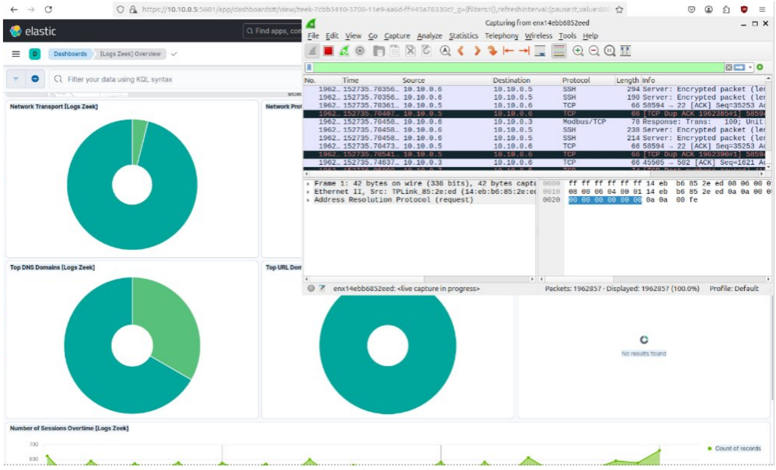


Audit Events [Logs Auditd]

20 documents

Time	event.action	auditd.log.sequence	user.name
Feb 26, 2025 @ 15:45:01.177	disposed-credentials	3,048	root
Feb 26, 2025 @ 15:45:01.177	ended-session		root

Figure 4. Auditd Detailed Capture


https://10.10.0.5:5601/app/dashboards#/view/zeek-7cbb5410-3700-11e9-aa6d-ff445a78330c?_g=(filters:!(),refreshInterval:(pause:!t,value:60
elastic
Find apps, con
Dashboards
[Logs Zeek] Overview
Filter your data using KQL syntax
Network Transport [Logs Zeek]
Network Prot
Top DNS Domains [Logs Zeek]
Top URL Dom
No results found
Number of Sessions Overtime [Logs Zeek]
700
600
Count of records
Capturing from enx14ebb6852eed
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help

```
No.    Time               Source       Destination  Protocol    Length Info
 1962… 152735.70356… 10.10.0.6    10.10.0.5    SSH            294 Server: Encrypted packet (ler
 1962… 152735.70356… 10.10.0.6    10.10.0.5    SSH            190 Server: Encrypted packet (ler
 1962… 152735.70361… 10.10.0.5    10.10.0.6    TCP             66 58594 → 22 [ACK] Seq=35253 Ac
 1962… 152735.70407… 10.10.0.5    10.10.0.6    TCP             66 [TCP Dup ACK 1962385#1] 5859
 1962… 152735.70458… 10.10.0.6    10.10.0.3    Modbus/TCP      78 Response: Trans:   100; Unit:
 1962… 152735.70458… 10.10.0.6    10.10.0.5    SSH            238 Server: Encrypted packet (ler
 1962… 152735.70458… 10.10.0.6    10.10.0.5    SSH            214 Server: Encrypted packet (ler
 1962… 152735.70473… 10.10.0.5    10.10.0.6    TCP             66 58594 → 22 [ACK] Seq=35253 Ac
 1962… 152735.70541… 10.10.0.5    10.10.0.6    TCP             66 [TCP Dup ACK 1962390#1] 5859
 1962… 152735.74637… 10.10.0.3    10.10.0.6    TCP             66 45505 → 502 [ACK] Seq=1621 Ac

› Frame 1: 42 bytes on wire (336 bits), 42 bytes captu    0000  ff ff ff ff ff ff 14 eb  b6 85 2e ed 08 06 00 0
› Ethernet II, Src: TPLink_85:2e:ed (14:eb:b6:85:2e:ed    0010  08 00 06 04 00 01 14 eb  b6 85 2e ed 0a 0a 00 0
› Address Resolution Protocol (request)                   0020  00 00 00 00 00 00 0a 0a  00 fe

enx14ebb6852eed: <live capture in progress>    Packets: 1962857 · Displayed: 1962857 (100.0%)    Profile: Default
```

Figure 5. Zeek and Wireshark Detailed Capture