Application of the MITRE ATT&CK Framework in the Context of University Networks

Mirka Miladinović[1[/]] and Savo Tomović[1[0000-0002-9388-7784]]

[1] University of Montenegro, Podgorica, Montenegro

miladinovicmirka@gmail.com

savot@ucg.ac.me

Abstract. In today's digital environment, university networks are constantly exposed to threats from cyber attacks due to the wide range of users and the open nature of university networks. Maintaining the security of these networks requires constant monitoring, detection of vulnerabilities and definition of proactive prevention strategies. The MITRE ATT&CK framework represents a knowledge base that documents the tactics, techniques and procedures (TTP) used by advanced threats (APT - Advanced Persistent Threat) in order to compromise various information systems. As a comprehensive threat analysis tool, this framework has become indispensable in the field of cyber security. University networks are potentially vulnerable environments due to their openness and complexity. Therefore, the goal of this project is to investigate the possibility of successfully applying the MITRE ATT&CK framework in the domain of university networks in order to improve their security. The Academic Network of the University of Montenegro will serve as a case study.

Keywords: MITRE ATT&CK, Caldera, Wazuh, university networks security.

1 Initiation of the Analysis

The assessment process was initiated through the distribution of a structured questionnaire to a technical staff member employed at the University's Center for Information Systems (CIS). The questionnaire was designed to collect detailed information regarding the organization's IT infrastructure, operating systems, network architecture, virtualization environment, key assets, and implemented security controls.

The technical representative from CIS completed the questionnaire, providing comprehensive insights into the current operational setup, configurations, and security practices in place. Based on the responses received, the analysis team conducted a systematic review and evaluation of the existing environment, identifying strengths, potential vulnerabilities, and areas requiring improvement. This information served as the foundational input for the subsequent phases of the assessment, including threat identification, risk evaluation, and prioritization of security measures.

1.1 Short Summary of the Current State

Operating Systems: Windows and Linux - Windows hosts are likely used for workstations, servers, and applications dependent on the Microsoft environment, while Linux OS supports infrastructural and application components such as web and

Research Paper
DOI: https://doi.org/10.46793/BISEC25.172M
Part of ISBN: 978-86-89755-40-4

database services. The existence of multiple Oss, even just two in this case, requires a harmonized policy for patching, hardening, and logging across both OSs and all system components.

Cloud: Not in use - This means the entire system, and therefore all data, is located on the organization's on-premise infrastructure. This setup simplifies control over physical and network security, reducing the attack surface and dependency on cloud vendors' security policies. On the other hand, it increases the organization's (i.e., CIS's) responsibility for backup, availability, and scalability.

Network: The network is segmented, which is a good practice to reduce the blast radius and control access between zones (e.g., internal and development environments). However, there are public services (mail server, database, e-learning platform, e-index) that increase the risk of initial compromise since these services are accessible via the internet.

Virtualization: The infrastructure is based on the VMware platform. Virtualization enables flexible management and resource consolidation but requires proper hypervisor configuration, segmentation of the management network, and protection of VMs, as well as ensuring backup and restore processes aligned with security policies.

Key Assets: Database - containing sensitive data, Mail server - communication channel and phishing vector, E-learning platform - publicly exposed web service, E-index - contains potentially sensitive student data, Financial applications - critical for operations, LDAP - central authentication and authorization service

Security Devices: Primary network protection is implemented through FortiGate firewall devices, with additional host-based firewalls present. It is essential to ensure that firewall policies are properly defined (minimization of open ports, segmented data flow) and that devices are under continuous monitoring.

Authentication/Access: Implementing MFA and LDAP for access management represents a good practice in access control. However, LDAP/AD infrastructures are often targeted due to their central role in credential and privilege management. Therefore, additional protective measures and monitoring of activity in these systems are necessary.

Limitations: The listed services (mail, database, e-learning, LDAP) must not be taken offline during testing. This means that tests must be planned and executed non-disruptively — for example, focusing on passive assessments, authorized scanning with limited scope, and testing patches and configurations without shutting down services.

Publicly exposed systems (mail server, e-learning platform, databases) are the most common entry points for attackers. They target vulnerabilities and misconfigurations in applications and services exposed on the internet to gain initial access through brute-force attacks or web exploits. Weak points can include software bugs, temporary glitches, or incorrect configurations — leading to remote code execution, privilege escalation, or system access. For web applications and databases, these threats often manifest through vulnerabilities such as SQL Injection or Remote Code Execution. **Required controls:** regular patching, WAF policies, strict access control, and continuous vulnerability scanning.

Phishing refers to targeted or mass messages aiming to trick recipients into performing unwanted actions such as opening malicious attachments/emails, clicking compromised links, or providing login credentials redirected to malicious sites or fake

authentication steps. While MFA significantly reduces successful attacks, it doesn't eliminate all scenarios (e.g., token reuse, push fatigue, compromised devices). **Required actions:** strengthen user awareness, conduct phishing simulations, and monitor login attempts.

Once an attacker gains privileged access to a system, they often use techniques for credential theft and command execution to expand network access and gain additional privileges. Upon compromising Windows/Linux systems with appropriate privileges, attackers frequently use credential dumping and script/command execution (PowerShell, cmd) for privilege escalation and lateral movement. **Required controls:** detect PowerShell activity, monitor logs, enforce least-privilege and zero-trust principles, and ensure regular password rotation.

1.2 Evaluation of Detection and Visibility Coverage with the MITRE DeTTECT and Navigator

We used DeTTECT, to quantitatively assess how well system and data sources in university network enable detection, visibility, and coverage of MITRE ATT&CK techniques. DeTTECT allowed us to perform the analysis in two distinct operational modes, detection mode and visibility mode, each serving different phases of the security evaluation. Detection mode focuses on analyzing rules, analytical queries, and correlation mechanisms that actively identify malicious activity. In contrast, visibility mode evaluates how well data sources provide visibility into system activities, regardless of whether a detection rule exists. Visibility determines if an event can be observed, while detection assesses whether it can be recognized as malicious, making visibility a prerequisite for detection and detection a higher level of analytical maturity. The results were visualized using the MITRE ATT&CK Navigator.

Fig. 1. The image shows a MITRE ATT&CK Navigator view in which techniques are organized into color-coded columns according to their evaluated visibility scores derived from the DeTT&CT framework.

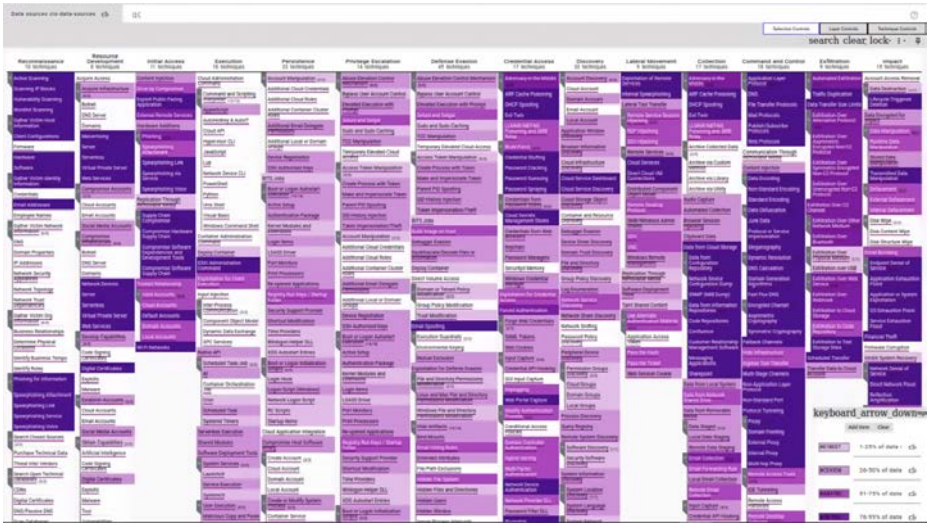

Fig. 2. The image presents a MITRE ATT&CK Navigator view in which techniques are displayed in varying shades of purple to represent their detection coverage based on DeTT&CT evaluations. This visualization offers a structured, comparative overview of how effectively different ATT&CK techniques are detectable across the full range of adversary tactics.

2 Simulation with Caldera and Wazuh agents

MITRE Caldera is a cybersecurity platform for automated adversary emulation, red-team exercise support, and incident response automation, built on the MITRE ATT&CK framework and developed as a research project. The system consists of a core component (an asynchronous C2 server, a REST API, and a web interface) and extensions that expand functionality (agents, TTP collections, reporting). Caldera emulates adversary tactics, techniques, and procedures to assess a network's detection and response capabilities, enables automated execution of red-team tests, simulates C2 infrastructure, and generates analytical reports. Its advantages include open-source code and the ability to integrate with other tools.

Our initial map of data sources and associated ratings (device completeness, data field completeness, timeliness, consistency, retention), derived according to the Navigator/DeTTECT classification, provides the baseline against which Caldera activities should be observable.

The objectives of the initial tests were therefore twofold: first, to use Caldera operation sets to reproduce typical MITRE ATT&CK techniques (discovery, execution, lateral movement, beaconing, etc.); and second, to correlate Caldera's generated records with central logs — in our case using the Wazuh SIEM.

All operations were executed via the "wavuty" agent on the host, which runs on a Linux platform under the user with standard user privileges. The operations followed

various tactics such as Discovery, Collection, Credential Access, Defense Evasion, and Exfiltration.

2.1 Operation 1: AGENT WORM

This operation simulates a malicious worm that targets unsecured SSH configurations and command-line history in order to obtain credentials.

Tactics (Fig. 3.): Collection; Credential Access;
Discovery Techniques: Data from Local System (T1005); Unsecured Credentials: Bash History (T1552.003); Remote System Discovery (T1018).

Table 1. Agent Worm.

Tactics	Techniques	Abilities
Collection	T1005: Data from Local System	Client worm, Parse SSH config
Credential Access	T1552.003: Unsecured Credentials - Bash History	Client worm, Dump history
Discovery	T1018: Remote System Discovery	Client worm, Collect ARP details

Example commands:

- Dump the Bash command-line history: `cat .bash_history`
- Attempt to parse the SSH configuration using the `stormssh` tool (unsuccessful).

Results:

- Successful extraction of the Bash history.
- Collection of network ARP details using arp -a failed.

This operation indicates attempts to obtain user credentials and to map the network environment. The observed failure to collect ARP data suggests a degree of resilience in the network configuration.

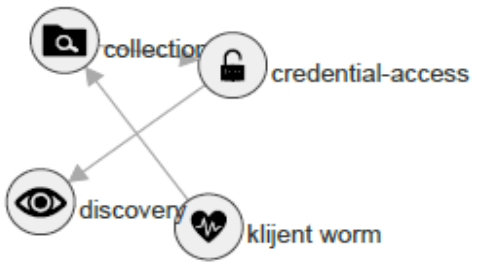

Fig. 3. Tactics leveraged by the Worm agent. The arrows illustrate the directional relationships between these adversarial behaviors

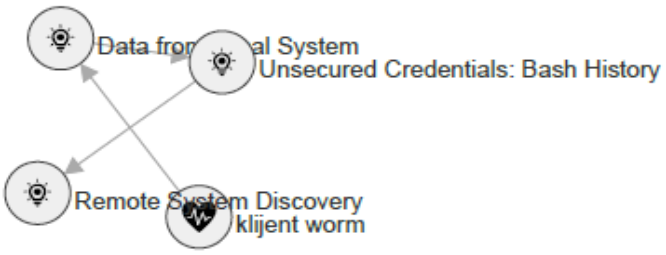

Fig. 4. Techniques used by the Worm agent - a small diagram illustrating links between specific MITRE ATT&CK techniques and harmful entity named “klijent worm”. The arrows represent relationships indicating how the worm engages in both credential-related data collection and discovery activities during its operational lifecycle.

2.2 Operation 2: COLLECTION AGENT

The purpose was the systematic collection of files with specified extensions and their preparation for exfiltration.

Tactics: Collection
Techniques: Data from Local System (T1005), Local Data Staging (T1074.001)

Table 2. Collection Agent.

Tactics	Techniques	Abilities
Collection	T1005: Data from Local System T1074.001: Local Data Staging	Collection Client Find files Create staging directory

Example of commands:

- Search and staging of files: `find -name .png -type f -not -path . -size -500k 2>/dev/null | head -5`
- Copying the located files into the same staging folder, preparing them for exfiltration.

Results: Identification and preparation of a significant number of files according to predefined criteria for further processing.

This operation demonstrates aspects of the data-collection process that are critical to system integrity. Monitoring file-system access and detecting the creation of staging areas are recommended.

2.3 Operation 3: DEFENSE EVASION AGENT

The objective of the operation was the implementation of techniques for concealment and detection disruption, including log deletion, file hiding, and disabling the firewall.

Tactics: Defense Evasion.
Techniques: Indicator Removal on Host (T1070), Impair Defenses (T1562), Hide Artifacts (T1564.001), Obfuscated Files or Information (T1027), Timestomp (T1070.006).

Table 3. Defense Evasion Agent.

Tactics	Techniques	Abilities
Defense evasion	T1070.003: Indicator Removal on Host: Clear Command History T1562.004: Impair Defenses: Disable or Modify System Firewall T1070.002: Indicator Removal on Host: Clear FreeBSD, Linux or Mac System Logs T1562.001: Impair Defenses: Disable or Modify Tools T1562.003: Impair Defenses: Impair Command History Logging T1564.001: Hide Artifacts: Hidden Files and Directories T1027: Obfuscated Files or Information T1140: Deobfuscate/Decode Files or Information T1070.006: Indicator Removal on Host: Time stamp T1027.001: Obfuscated Files or Information: Binary Padding	Defense EvasionClient Avoid logs Stop/Start UFW firewall Edit UFW firewall sysctl.conf file Edit UFW firewall ufw.conf file Overwrite Linux Mail Spool Clear Paging Cache Clear Bash History (truncate) Setting the HISTFILE environment variable Use Space Before Command to Avoid Logging to History Create a hidden file in a hidden directory Decode base64 data into Script Linux base64 Encoded Shebang in CLI Base64 decoding with shell utilities Set a file's creation timestamp Pad binary to change hash using truncate command – Linux/MacOS `rm -rf`

Example commands:

- Deleting the bash history with the effective command: `truncate -s 0 .bash_history`
- Setting HISTFILE to null to prevent logging: `unset HISTFILE`
- Creating hidden files: `mkdir -p /var/tmp/.hidden-directory; echo "T1564.001" > /var/tmp/.hidden-directory/.hidden-file`
- Base64-decoding a script directly into bash: `echo IyEvYmluL2Jhc2gK... | base64 -d | bash`
- Manipulating a file's modification date to conceal activity: `touch -t 010100001971 tmpT1070.006-creation.txt`.

Results:

- Preservation of concealment through log deletion and encoding
- Innovative methods for masking files and metadata, thereby accelerating the stealth of operations.

The operation clearly demonstrates advanced concealment techniques employed by adversaries to evade detection. It is recommended to employ advanced analytical tools for file and log analysis with a focus on unauthorized modifications.

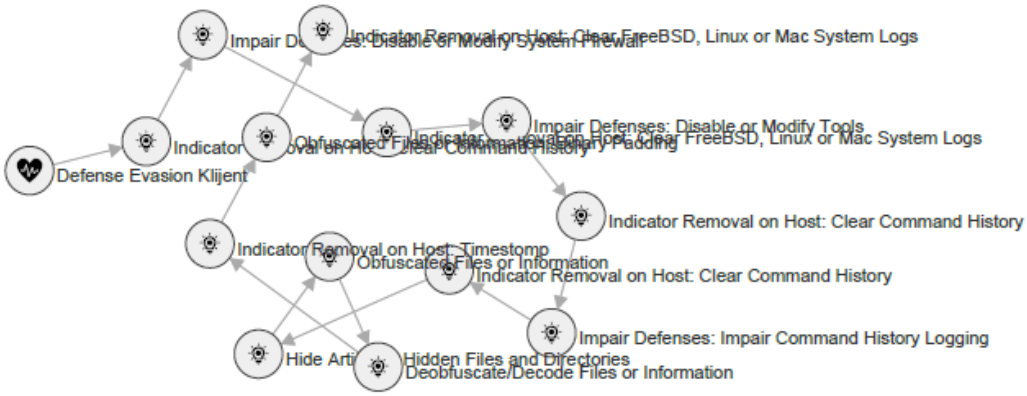

Fig. 5. Techniques used by the Defense Evasion agent - The image presents an interconnected diagram illustrating a cluster of MITRE ATT&CK defense-evasion techniques linked to an entity labeled "Defense Evasion Klijent." Multiple nodes of various log-impairment and command-history-clearing techniques form a network that conceptually maps how the client worm employs layered evasion strategies to hinder detection and analysis.

2.4 Operation 4: DISCOVERY AGENT

The scope of tactical activities was directed at a detailed analysis of users, processes, and permissions on the targeted system.

Tactics: Discovery.
Techniques: System Owner/User Discovery (T1033), Account Discovery - Local Account (T1087.001), Process Discovery (T1057), Permission Groups Discovery - Local Groups (T1069.001).

Table 4. Discovery Agent.

Tactics	Techniques	Abilities
Discovery	T1033: System Owner/User Discovery T1087.001: Account Discovery: Local Account T1057: Process Discovery T1069.001: Permission Groups Discovery: Local Groups	Caldera2 Client Identify active users Find local users Find user processes

Example commands:

- Identification of the active user: `whoami`
- Search for all local users: `cut -d: -f1 /etc/passwd | grep -v grep`
- Collection of processes by key names: `ps aux | grep nx`
- Investigation of user groups: `groups`.

Results:

- Precise mapping of user and process configurations, with identification of accounts of interest, and potential service and system accounts.

The operation provides a comprehensive view of the structure of user and service accounts, which is critical for assessing access vulnerabilities and privileges on the system. Strengthening access controls and monitoring the activity of highly privileged accounts is recommended.

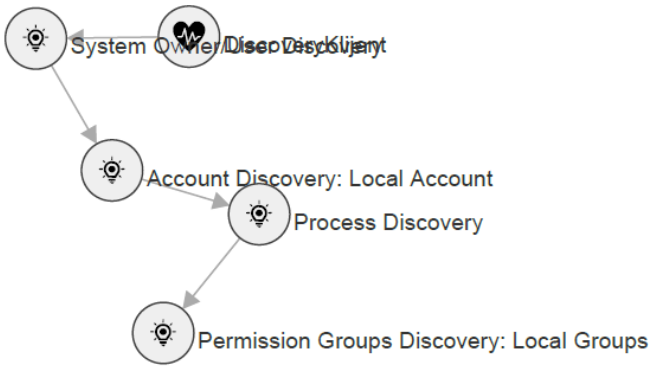

Fig. 5. Techniques used by the Discovery agent - The image illustrates a small chain of discovery techniques associated with the entity labeled “Discovery Klijent.” It traces how the client worm successively queries system ownership details, enumerates local accounts and running processes, and ultimately identifies local permission groups as part of its reconnaissance behavior.

3 Conclusion

The system was exposed to a broad spectrum of sophisticated techniques for data collection, manipulation, and exfiltration, accompanied by activities to discover and map user accounts, active processes, and associated system groups.

The Fig 6. illustrates the relationship between the Caldera operation *Klijent CALDERA2* (represented by the heart icon in the center) and the set of facts discovered by the deployed agent during the emulation exercise. Each star icon represents a

specific fact or data artifact collected throughout the simulated adversary activities, such as user account names, file extensions, or URLs.

The connections between nodes indicate which facts were gathered as part of the same operation. The legend on the right shows the number and types of discovered facts, including user accounts identified on the host, sensitive file extensions detected, potentially malicious URLs and additional contextual data.

This visualization provides insight into the information an attacker (simulated adversary) could obtain during reconnaissance and collection phases. It also supports the evaluation of visibility and detection coverage within the monitored environment.

Technical challenges were encountered in fully disabling defensive measures, as well as in obtaining key network information such as ARP tables which were partially inaccessible.

Advanced concealment efforts were executed, including multi-layered deletion of command-line history, the use of base64 encoding to obscure executable scripts, and manipulation of file-system metadata (timestomping) to blur digital traces. Numerous files with critical extensions (.yml, .png, .wav) were identified and systematically collected, then organized into staging directories, archived, and exfiltrated via HTTP requests (curl).

The synchronized coordination of operational steps and command-and-control communication between the agent and the command server clearly reflects a high degree of sophistication and deliberate integration within the adversary campaign.

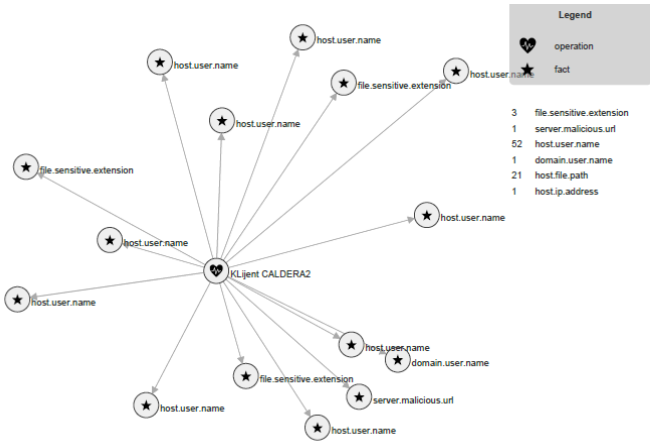

Fig. 6. Visualization of Facts Collected During the “Klijent CALDERA2” Operation

The Fig. 7 also helps estimate the complexity and scope of the simulated campaign (number of techniques, branching paths, and chained behaviors), useful for prioritizing detection and monitoring improvements.

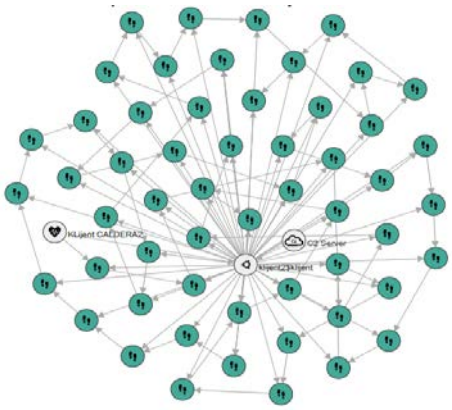

Fig. 7. Caldera Operation Flow

The Caldera was utilized for automated simulation of attack techniques aimed at credential collection, privilege escalation, data exfiltration, and trace concealment. The SIEM instance visualized the dynamics and frequency of detections, categorization of tactics, and log modifications of system resources through MITRE ATT&CK rules.

The analysis encompassed: collection and visualization of alerts over a time series. classification of the most dominant MITRE tactics and attack rules and decomposition of detected activities by attack types and specific commands.

Graphical representations from Wazuh SIEM indicate a sharp increase in the number of alerts coinciding with the activation of Caldera agents-based attack scenarios. The visualization titled "Alerts evolution over time" in Fig. 8. shows a steady increase in the number of alerts as the simulated attack progressed, indicating continuous detection of Caldera activities and clearly demonstrates that most detections occurred during automated phases of mass command execution, implying high activity levels of credential access and brute force attacks.

The pie chart labeled "Top tactics" (Fig. 8.) identifies credential access (e.g., brute force and password guessing) and lateral movement as the most prominent techniques detected on the SIEM instance, while defense evasion, persistence, impact, and privilege escalation constitute minor segments. This scenario aligns with Caldera attack simulations, with rules related to password access attempts, SSH sessions, and manipulation of valid user accounts being the most strongly detected.

The graph on the right of Fig. 9, labeled “Alerts” similarly shows the number of detected alerts over time. The colored markers represent different severity levels or alert categories, emphasizing the escalation of security events during that short period.

In the lower section, several summary charts provide additional insights. The chart titled “Top 5 alerts” displays that the majority of the events are related to SSHD login attempts. Other, less frequent alerts involve integrity checksum changes, brute-force detections, and PAM session openings or closings. This clearly suggests that SSH authentication issues are the dominant source of security alerts.

The final chart on the right, “Top 5 PCI DSS Requirements,” connects these alerts to specific PCI DSS compliance requirements. Most of the alerts correspond to

requirements 10.2.5 and 10.2.4, which deal with monitoring privileged user access and tracking failed login attempts. There are also entries for requirements 10.1 and 11.5, which relate to maintaining log integrity and detecting unauthorized modifications. The correlation suggests that the system is experiencing multiple failed access attempts involving privileged accounts, which poses a security concern.

In conclusion, the Wazuh SIEM demonstrated a solid baseline for threat detection, especially in identifying credential-related and brute-force activities. Correlation depth and detection accuracy can be further improved through the enrichment of event data with contextual metadata such as host and process identifiers, the implementation of additional detection rules aligned with underrepresented MITRE ATT&CK techniques, and continuous fine-tuning based on feedback from adversary simulation results (e.g., Caldera). Future improvements should focus on expanding visibility across less frequently detected tactics and increasing analytic depth to enhance detection coverage, precision, and response readiness against advanced adversarial techniques.

Fig. 8. Wazuh MITRE ATT&CK Dashboard - Detection Overview

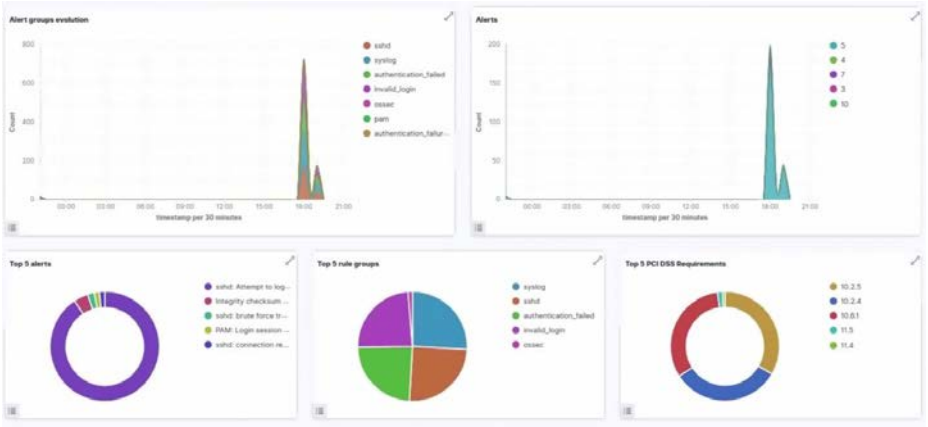

Fig. 9. Wazuh dashboard showing alert distribution and authentication anomalies.

4 Future Work

The performed analysis shows that the ATT&CK framework, thanks to tools such as Navigator, DeTT&CT, Caldera, and Wazuh, can be applied in practice to other kinds of organizations besides those in an enterprise environment, such as public-sector institutions like universities. It extends this framework to show that even complex, open, and heterogeneous academic networks will benefit enormously from structured threat-informed defense methodologies. Another major advantage is derived from the open-source nature of the tools, which makes it possible for institutions with limited budgets to systematically assess the current security posture and build realistic, automated, and controlled training environments for technical staff and students.

Future research is needed to investigate how these platforms can be used for the continuous development of security maturity within academic institutions. The integration of simulated adversary exercises into university curricula can facilitate hands-on education in cyber defense with real-world attack models. Further, expanding SIEM and logging capabilities would vastly improve visibility and detection across underrepresented ATT&CK techniques revealed by this study, especially with endpoint telemetry correlation, process-level monitoring, and anomaly detection models.

Another promising avenue is automating the red/blue team feedback loops. By connecting Caldera emulation outputs to detection engineering pipelines, universities can iteratively create, validate the performance of, and refine new detection rules to keep up with defensive coverage. In addition, assessments in the future might include cloud-based academic services, distance learning platforms, and hybrid infrastructures to represent the evolving digital ecosystem of modern universities.

Finally, there is an important opportunity for collaboration across institutions. Universities could share anonymized detection data, defensive playbooks, and ATT&CK-mapped analyses to establish a collective knowledge base specific to higher education. By doing so, a sector-wide understanding of threats targeting academic environments would take shape, thereby contributing to improved resilience and fostering a unified approach toward threat-informed defense.

Acknowledgments. Agreement on research funding between the University of Montenegro and the company "Sport Vision".

References

1. **MITRE Corporation.** *MITRE ATT&CK®: A Framework for Cyber Threat Intelligence and Defense.* Available at: https://attack.mitre.org/ (accessed: November 2025).
2. **MITRE Corporation.** *Caldera: Automated Adversary Emulation Platform.* Available at: https://github.com/mitre/caldera (accessed: November 2025).
3. **Wazuh, Inc.** *Wazuh: Open Source Security Platform for Threat Detection, Visibility, and Compliance.* Available at: https://wazuh.com/ (accessed: November 2025).
4. **Center for Threat-Informed Defense (CTID).** *DeTTECT: Detection and Visibility Mapping Framework.* MITRE Engenuity, 2023. Available at: https://github.com/center-for-threat-informed-defense/detect (accessed: November 2025).