konnektable

TECHNOLOGIES

Cyber Security Awareness in Critical Infrastructures

Presenter: Christos Angelidis

The next 20 minutes...

- Critical Infrastructures
- SIEM in Critical Infrastructures
- Architecture of the SIEM solution
- Software Components of SIEM
- Implementation and Development
- SIEM Capabilities
- Inputs from Agents
- MITRE Attack Framework
- Positioning SIEM in Critical Infrastructures

Critical Infrastructures

Critical Infrastructures are becoming targets of malicious behaviour. The reason is that this type of infrastructures are affecting a huge number of entities, from humans to whole cities and economies. If a malicious user obtains the control of this system, he/she could have the power to abuse whole cities. This is the reason why critical infrastructures must shield their environment with powerful cyber security countermeasures.

ENERGY

HEALTH

TRANSPORT

CHEMICAL AND NUCLEAR INDUSTRY

PUBLIC AND LEGAL ORDER AND SAFETY

FOOD

SIEM in Critical Infrastructures

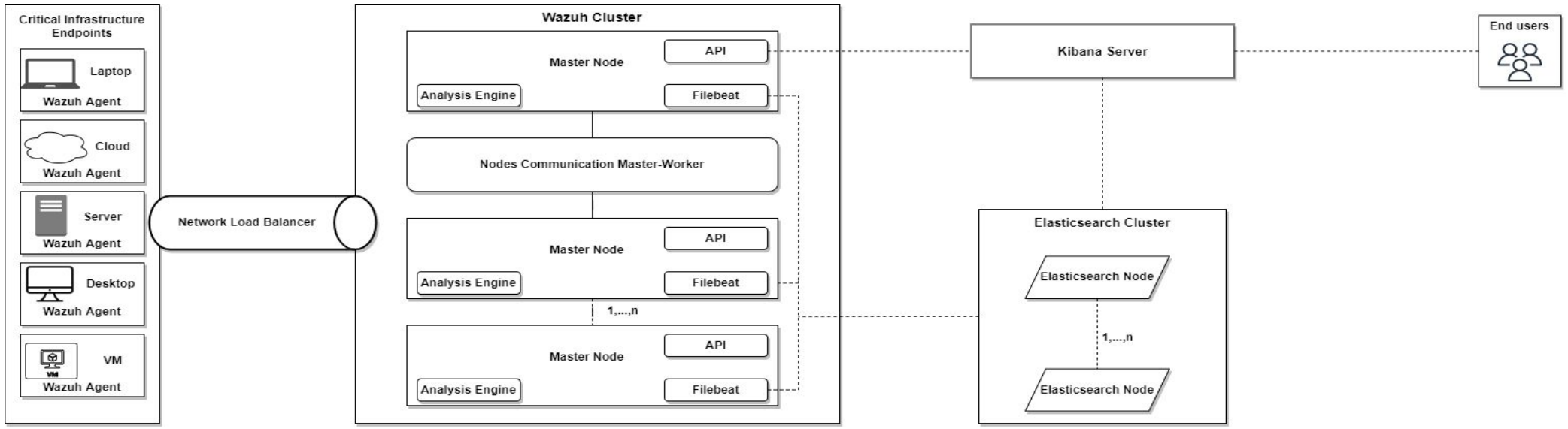
SIEM tool aims to combine the security information management (SIM) with the security event management (SEM), forming a single collaborative security management system. This system collects critical information from multiple sources and endpoints. These endpoints can be:

- Servers
- Virtual Machines
- Personal computers (laptops, desktops)

from the critical infrastructure that SIEM is assigned to monitor. SIEMs are widely used on a plethora of infrastructures, in order to detect any suspicious activity and inform the end-user of suspicious activities.

Architecture of the SIEM Solution

- **Wazuh Agents:** Installed on the monitored endpoints and forward security data to a central server
- **Wazuh Cluster:** A group of Wazuh managers that work together, divided by a master node and worker nodes
- **Elasticsearch Cluster:** A collection of one or more nodes that communicate with each other to perform read and write operations on indexes
- **Kibana Server:** A flexible and intuitive web interface for mining, analyzing, and visualizing data



Software Components of SIEM

Wazuh solution consists of:

- **Wazuh Agent:** an endpoint security agent, deployed to the monitored systems, and
- **Wazuh Server:** which collects and analyzes data gathered by the agents.
- **Filebeat:** which is the tool on the Wazuh server that securely forwards alerts and archived events to Elasticsearch.

Software Components of SIEM

ELK-STACK consists of:

- **Elasticsearch:** Elasticsearch is a distributed search and analytics engine based on Apache Lucene. Elasticsearch is a NoSQL database. After adding data, actions such as full-text searches, search by field, search multiple indices, aggregate results and more, can perform

- **Logstash:** Logstash, as a data pipeline, provides a broad array of input, filter, and output plugins for collecting, enriching, and transforming data from a variety of sources

- **Kibana:** Kibana is an open source data visualization dashboard for Elasticsearch, with a Wazuh UI, embedded as plugin. It provides visualization capabilities on top of the content indexed on an Elasticsearch cluster

- **Beats:** Beats are shippers that get and deliver data from distinct sources (e.g metricbeat)
  - **Metricbeat:** This agent comes with internal modules that collect metrics from services and statistics for every process running on the systems.
  - **Auditbeat:** This agent collects logs directly from the Linux and Unix Kernel, by using the auditd daemon. Can be easily expanded with rules a highly valuable information in a security context.

- **Suricata:** It is an endpoint agent which is installed to the monitored system and detect suspicious Network Activity

Implementation and Deployment

- Division in 2 Clusters
- Wazuh cluster
- Elasticsearch cluster
- Agent Configuration
- Creation of the necessary certificates
- Establishment of Communication between components through Logstash and Filebeat
- Installation and configuration of MetricBeat
- Installation and configuration of Suricata agents
- Installation and configuration of Kibana

SIEM Capabilities

The SIEM provides the following capabilities:

- **Log Data collection:** This feature is the real-time process of getting logs and events generated by the monitoring endpoints, where the agents are installed.
- **Distributed Data Storage:** SIEM provides a distributed data storage by using Elasticsearch. SIEM uses Elasticsearch to store the log data.
- **Integrity Monitoring:** The File Integrity Monitoring is located in the monitoring endpoint via the Wazuh agents, where periodic scans are running inside specified directories, in order to trigger alerts when these files are modified.
- **Secure Authorization:** SIEM uses Role-based access control (RBAC) in order to secure the system. Role-based access control (RBAC) refers to the idea of assigning permissions to users based on their role within an organization. It provides fine-grained control and offers a simple, manageable approach to access management that is less prone to error than assigning permissions to users individually.

SIEM Capabilities

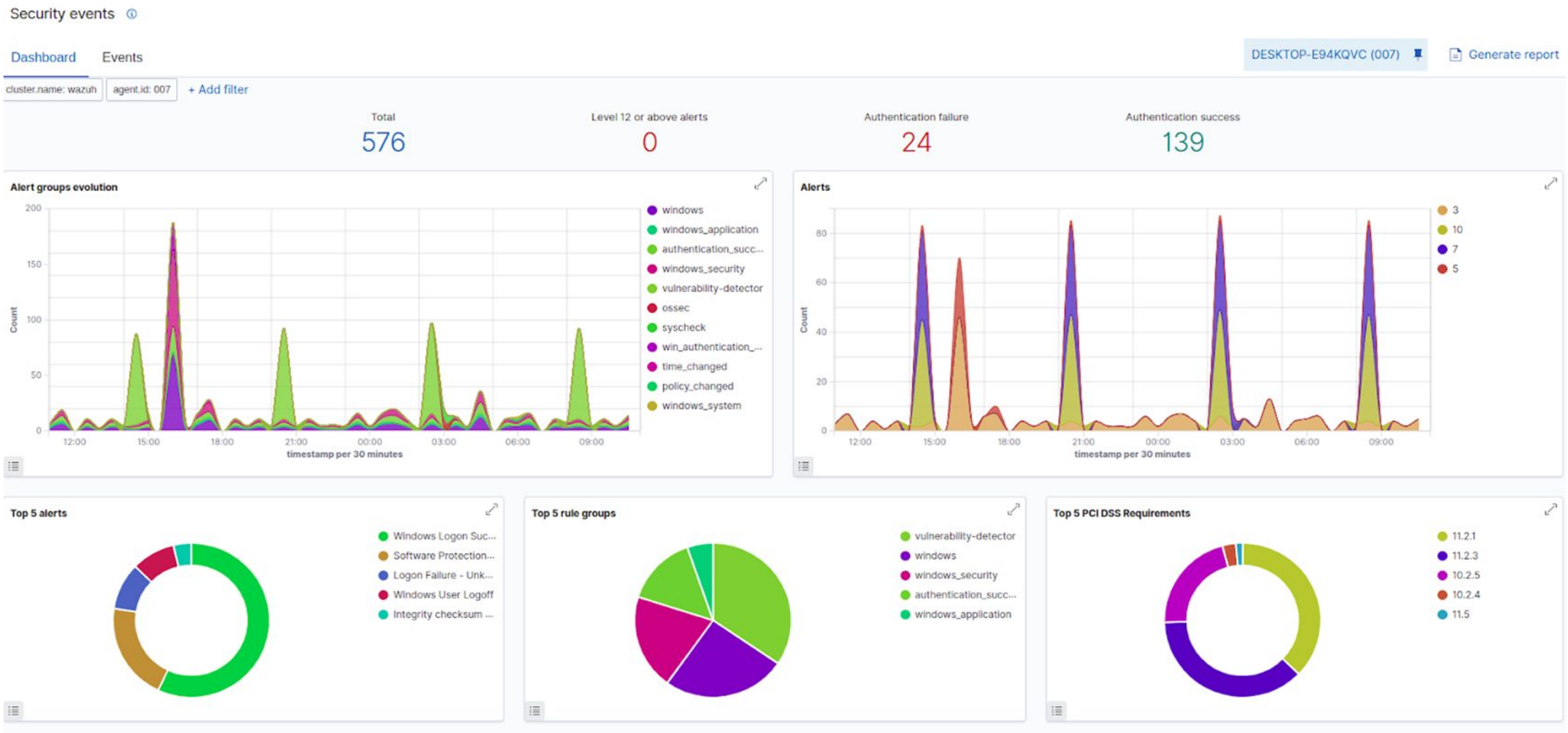
- **Vulnerability Detection:** SIEM is capable to detect vulnerabilities in the applications installed in agents using the Vulnerability Detector module. This software audit is performed through the integration of vulnerability feeds indexed by Canonical, Debian, Red Hat, and the National Vulnerability Database.

- **Incident Response (Countermeasures):** SIEM has enabled the Active Response to well-known attacks. Furthermore, the collected information on the incidents firing a rule triggers an Active Response (e.g., host-deny, firewall-drop, etc.).

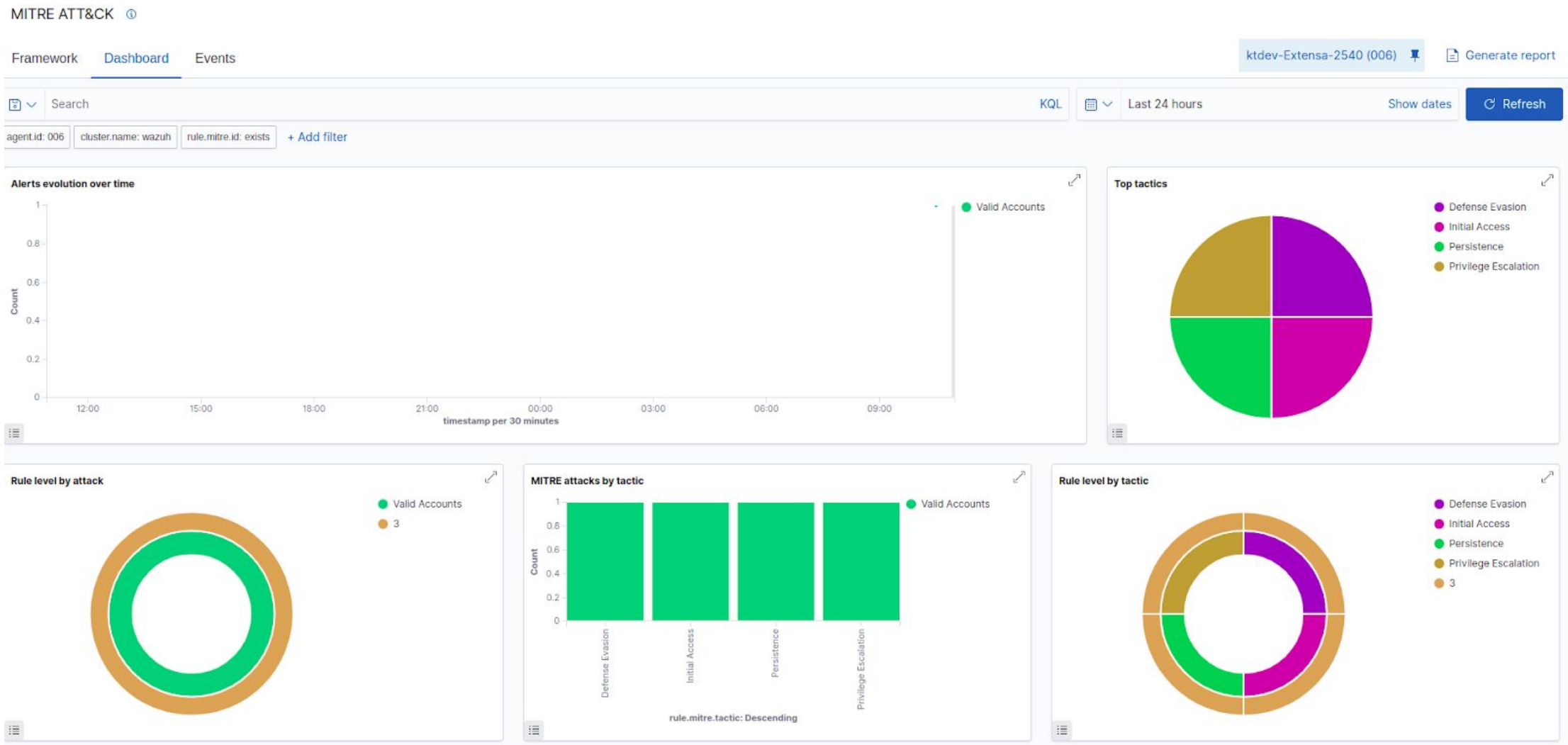
- **Alerting:** Alerting provides the capability to take action based on changes in the data.

- **Visualization:** The Visualization component of SIEM, based on Kibana, provides an advanced way to visualize and analyse SIEM alerts stored in Elasticsearch.

Inputs from the Agents



MITRE Attack Framework



Positioning SIEM in Critical Infrastructures

All the aforementioned features constitute an outcome of the SIEM solution. The SIEM tool could be a part of a cyber security solution in critical infrastructures, because **Critical Infrastructures** rely on distributed communication, which open various cybersecurity risks. As a result, the SIEM solution could be capable of addressing several and critical aspects of a critical infrastructure, using the presented components, their features, evolving depending on the new needs and finally delivering safety to each sector.

Conclusion

SIEM solution provides a **holistic and all-around** approach to alerting, monitoring, detecting, and actively responding to **cybersecurity** crime in critical infrastructure.

SIEM solution could be capable of addressing several critical aspects of **critical infrastructure**, providing valuable **defensive capabilities** on several essential services like Generation / Production, Transmission, Distribution, Management of the critical infrastructure, Storage facilities, etc.

Thank you!

Christos Angelidis
Data Scientist

konnektable TECHNOLOGIES

Our Contact

IRELAND

Marine Point (2nd Floor),
Belview Port, Waterford,
X91 W0XW, Ireland

+353 51349127

GREECE

Dervenion 30,
Metamorfosi, 14451,
Athens, Greece

+30 211 1138561

USA

829 Washington Street,
Apt 4, HOBOKEN,
NJ 07030, US

+1 7323209268

www.konnektable.com

info@konnektable.com