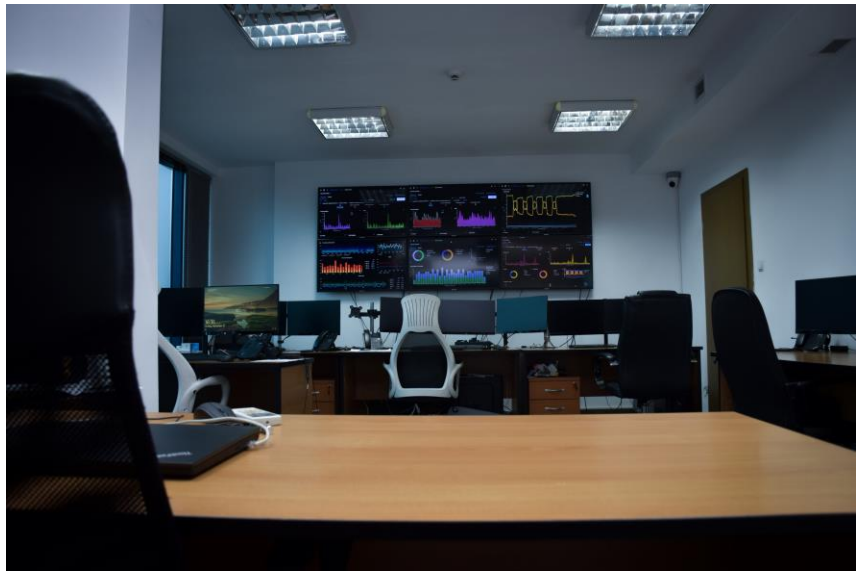
CYBER ONE

Cybersecurity Solutions

More information about us

CYBERONE is a company founded by Israeli and Bulgarian cybersecurity specialists in 2018. The company provide Israeli know-how and variety of technological solutions related to cybersecurity and information technology. The main priority of the company is the successful and effective provision of cybersecurity solutions to businesses in Europe.

Since 2019 the company established their own advanced Security Operation Center in Sofia, Bulgaria. Together with our partners we strive to provide quality cybersecurity and IT services. In addition, we provide complete software and hardware solutions for Cybersecurity and data protection.



How can we protect you?

CYBER ONE

Passive protection

Implementation of mechanisms for passive control and protection of IT infrastructure

Proactive protection

Providing regular penetration tests and vulnerabilities scan

Monitoring

Implementation of innovative solutions for monitoring servers, workstations and networks

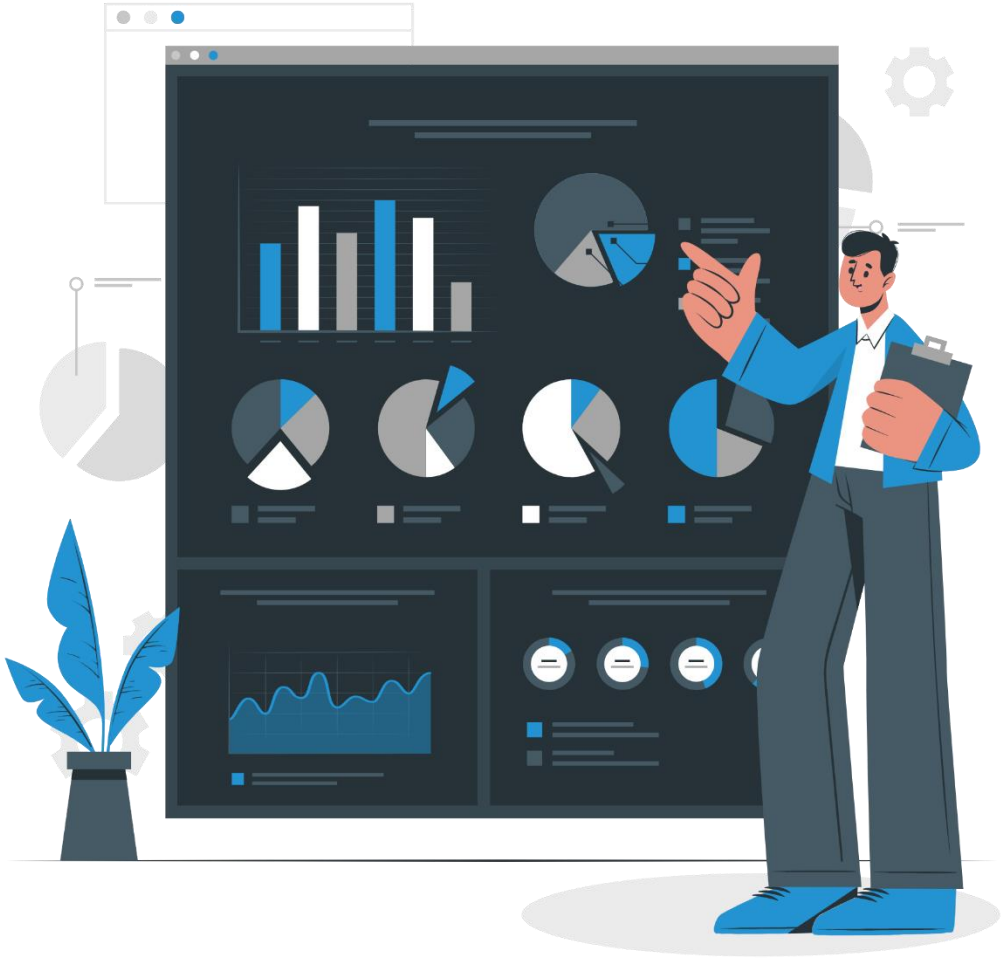
What is SIEM?

CYBER ONE

Security Information and Event Management (SIEM) is a combined security solution containing software products and services that allow real-time monitoring of various rule-based cybersecurity logs directed to data from multiple variety of IT systems and integrated into incidents that can be correlated and handled.

SIEM solutions that we can offer are one of the most popular and with proven success in detecting and preventing attacks.

These type of solutions also help to prevent malicious actions by company employees as the administrator has complete information about what actions and operations they perform.



Why do you need a SIEM?

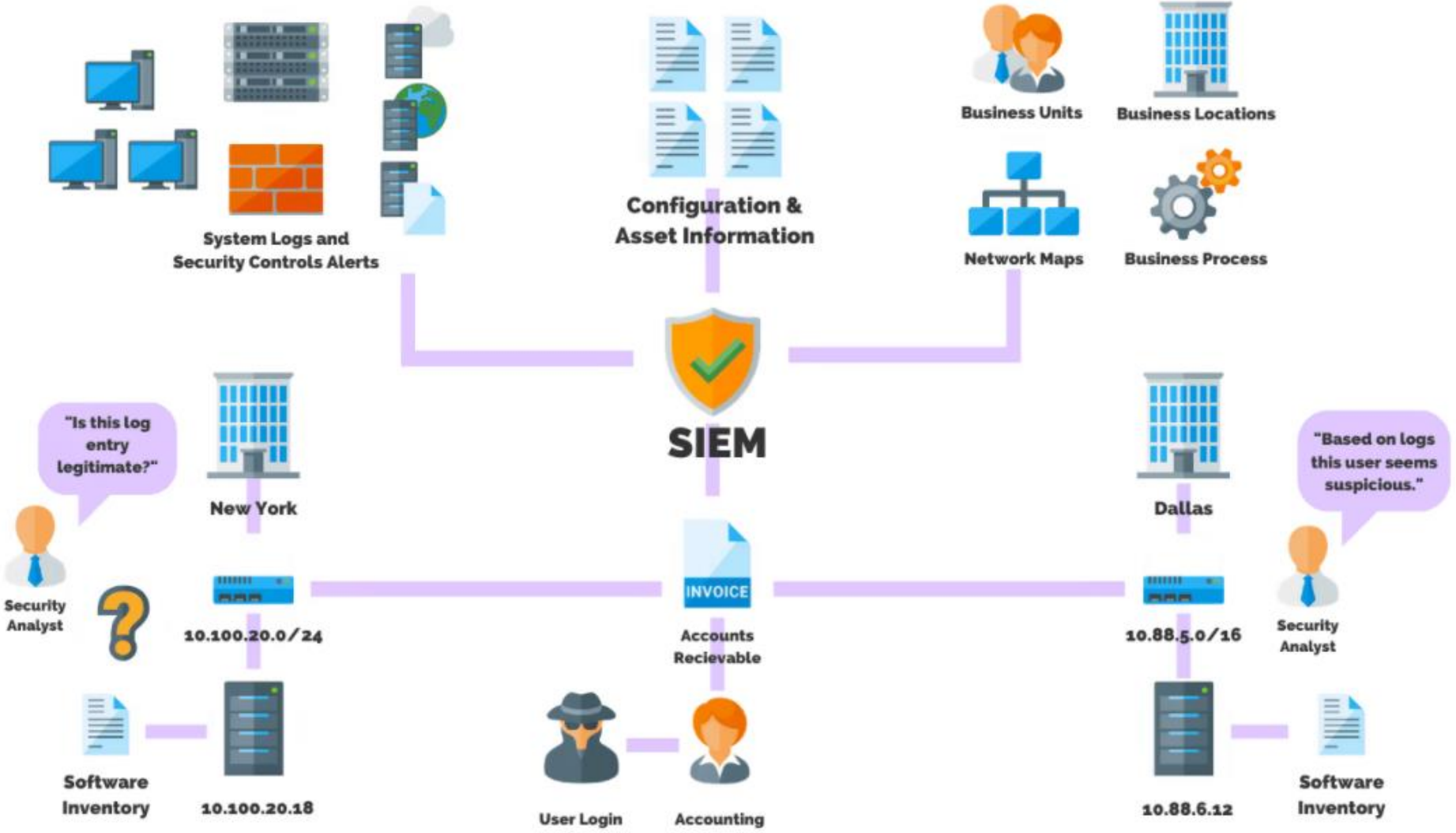
CYBER ONE

The reason an organization needs a SIEM solution to monitor the systems and report suspicious activities is that the amount of data an average organization generates nowadays is too much to handle manually. Log management sits at the core of SIEM functions; as the more diversified types of logs from more disparate sources feed the SIEM system, the more it generates actionable reports. This capability allows SIEM to correlate relevant events by cross-referencing logs from different sources against correlation rules.

Most enterprises own a lot of servers or cloud services and usually cannot handle neither the monitoring nor the security at a scale. By using a SIEM your company can provision security and monitoring more easily. Our software will allow you to generate reports in a matter of seconds for hundreds or even thousands of servers.

How does our solution works?

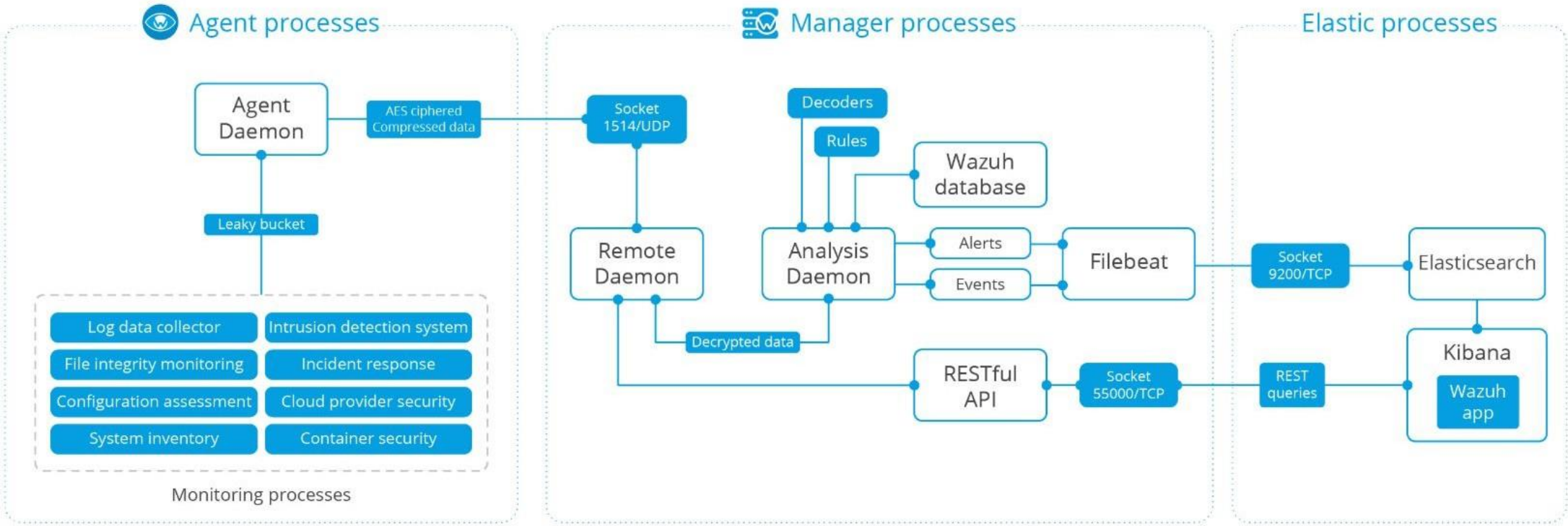
CYBER ONE



Cloud SIEM infrastructure

CYBER ONE

The cloud server node is in charge of analyzing the data received from the agents, processing events through decoders and rules, and using threat intelligence to look for well-known IOCs (Indicators Of Compromise). A single node can analyze data from hundreds or thousands of agents, and scale horizontally when set up in cluster mode.
The server is also used to manage the agents, configuring and upgrading them remotely when necessary. Additionally the server is capable of sending orders to the agents, for example to trigger a response when a threat is detected.



Features and capabilities

CYBER ONE

- Security Analytics
- Intrusion Detection
- Log Data Analysis
- File Integrity Monitoring
- Vulnerability Detection
- Configuration Assessment
- Incident Response
- Regulatory Compliance
- Cloud Security
- Containers Security

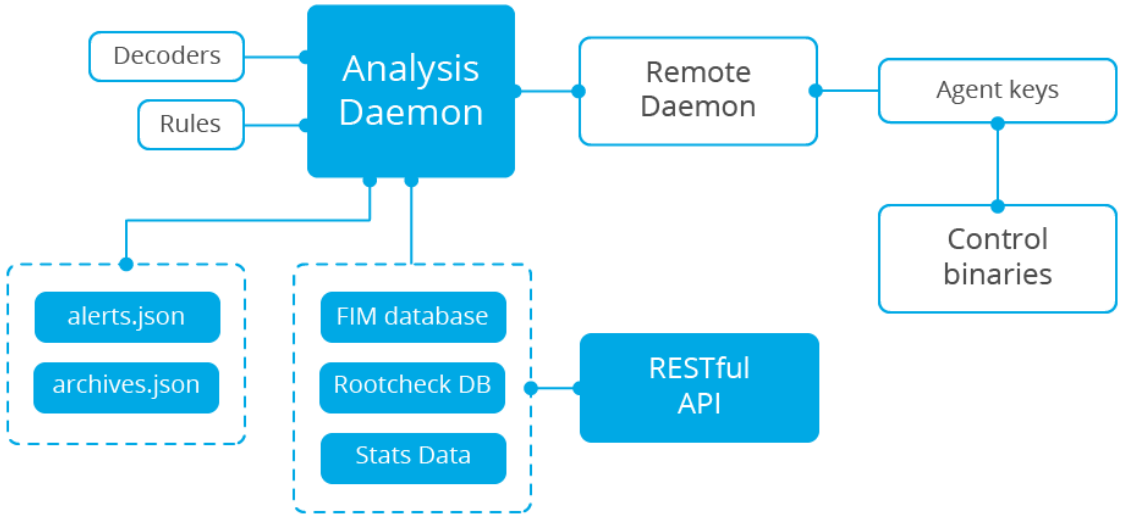
Host-based Intrusion Detection System (HIDS)

Compliance & Security Management

Monitoring and security for AWS and GCP

Custom ruleset and rules customization

Monitoring for custom or proprietary software



Real-time cybersecurity

CYBERONE

CYBERONE SIEM performs real-time analysis of security alerts generated by computers, network devices, servers and applications.

- Correlation of security events
- Security analysis
- Data collection and categorization
- Risk Assessment
- Incident investigation
- Proactive attack response
- Automation workflows
- Compliance with regulatory requirements

Monitoring

Applications | User behavior | File integrity | Containers & Cloud

Detection

Intrusion attempts | Vulnerabilities | Malware activity | Policy violations

Response

Prevention | Forensics | Telemetry | Workflows

Advantages of our solution

CYBER ONE

Advantages compared to other SIEM software

- ✓ The agent is compatible with many operating systems: Linux, Windows, Mac, Solaris, AIX and HP-UX.
- ✓ We have a unified security monitoring platform that analyzes real-time security events.
- ✓ Created for management and compliance with the policies of PCI, HIPAA, GDPR, NIST, GPG13.
- ✓ There is a possibility for scaling, thanks to the structure of our cluster infrastructure (1 + 3 +?).
- ✓ Infrastructure monitoring:
  - ✓ Clouds and cloud services: AWS, Azure, Google.
  - ✓ Monitoring of virtual containers: Docker, Kubernetes.
  - ✓ Virtual and physical (on premise) infrastructure

Advantages compared to other SIEM software

- ✓ Possibility to integrate with 3rd party threat intelligence feeds.
- ✓ Very flexible framework for both blacklist and whitelist list
- ✓ Predefined alerts as well as capabilities for custom alerting
- ✓ Alerting by email, REST API, Telegram, Slack, Teams etc.

Benefits for your company

CYBER ONE

Detecting Incidents

A SIEM solution detects incidents that otherwise can go unnoticed. This technology analyzes the log entries to detect indicators of malicious activity. Moreover, since it gathers events from all sources across the network, the system can reconstruct the attack timeline to help determine its nature and impact. The platform communicates recommendations to security controls –for example, directing a firewall to block the malicious content.

Improved efficiency

SIEM tools can significantly improve your efficiency when it comes to understanding and handling events in your IT environment. With SIEM tools, you can view the security log data from the many different hosts in your system from a single interface. This expedites the incident handling process in several ways. First, the ability to easily see log data from the hosts in your environment allows your IT team to quickly identify an attack's route through your business. Second, the centralized data lets you easily identify the hosts that were affected by an attack.

Compliance with Regulations

Companies use SIEM to meet compliance requirements by generating reports that address all logged security events among these sources. Without a SIEM, an organization need to manually retrieve log data and compile the reports.

Incident Management

A SIEM improves incident management by allowing the security team to identify an attack's route across the network, identifying the compromised sources and providing the automated mechanisms to stop the attacks in progress.

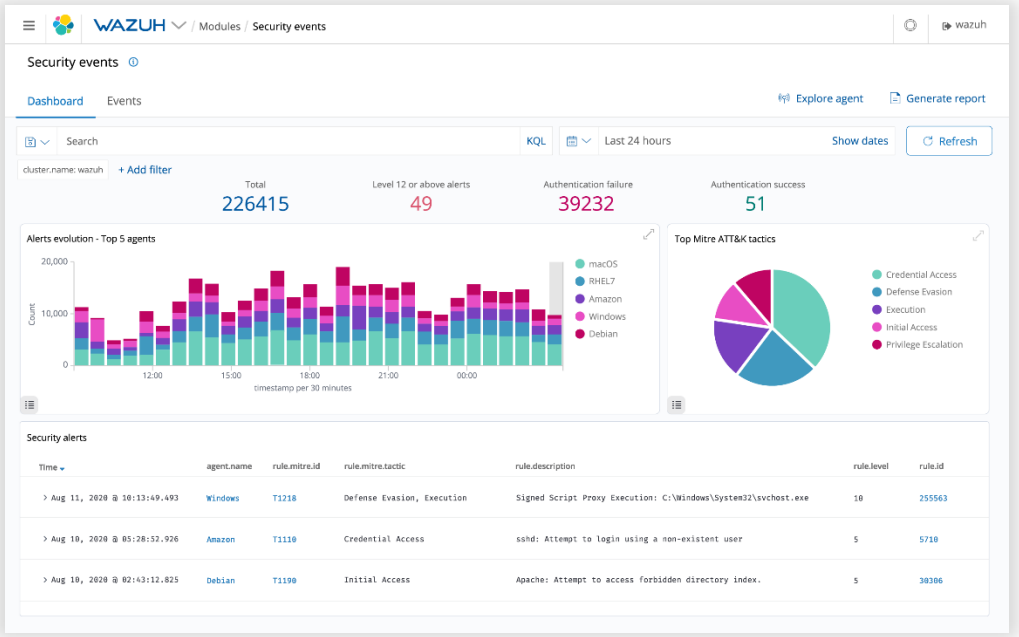
Use cases for your company

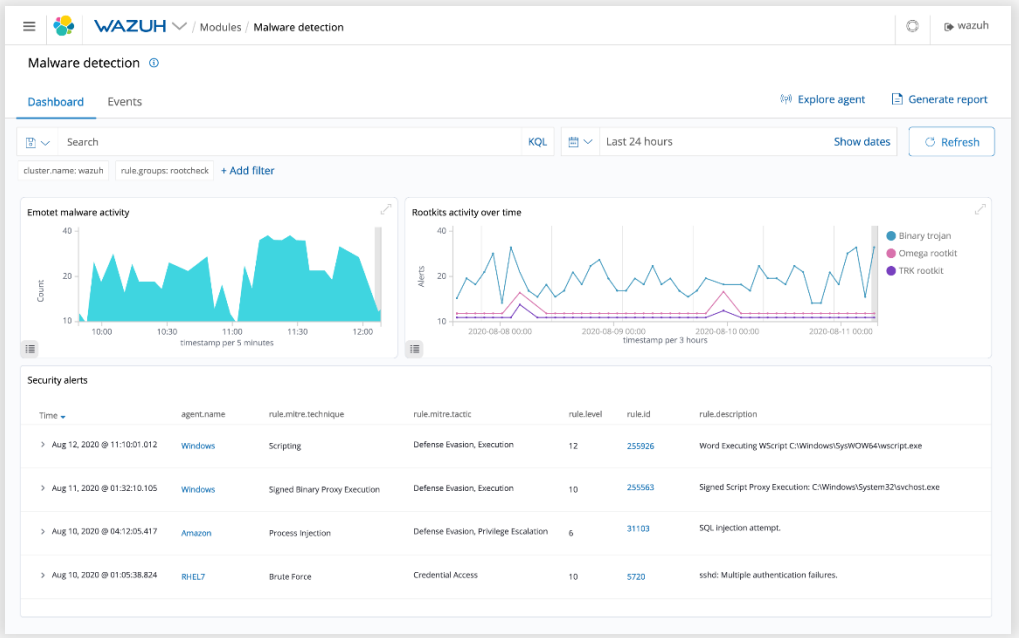
CYBER ONE

Security Analytics

SIEM is used to collect, aggregate, index and analyze security data, helping organizations detect intrusions, threats and behavioral anomalies.

As cyber threats are becoming more sophisticated, real-time monitoring and security analysis are needed for fast threat detection and remediation. That is why our light-weight agent provides the necessary monitoring and response capabilities, while our server component provides the security intelligence and performs data analysis.





Intrusion Detection

The agents scan the monitored systems looking for malware, rootkits and suspicious anomalies. They can detect hidden files, cloaked processes or unregistered network listeners, as well as inconsistencies in system call responses.

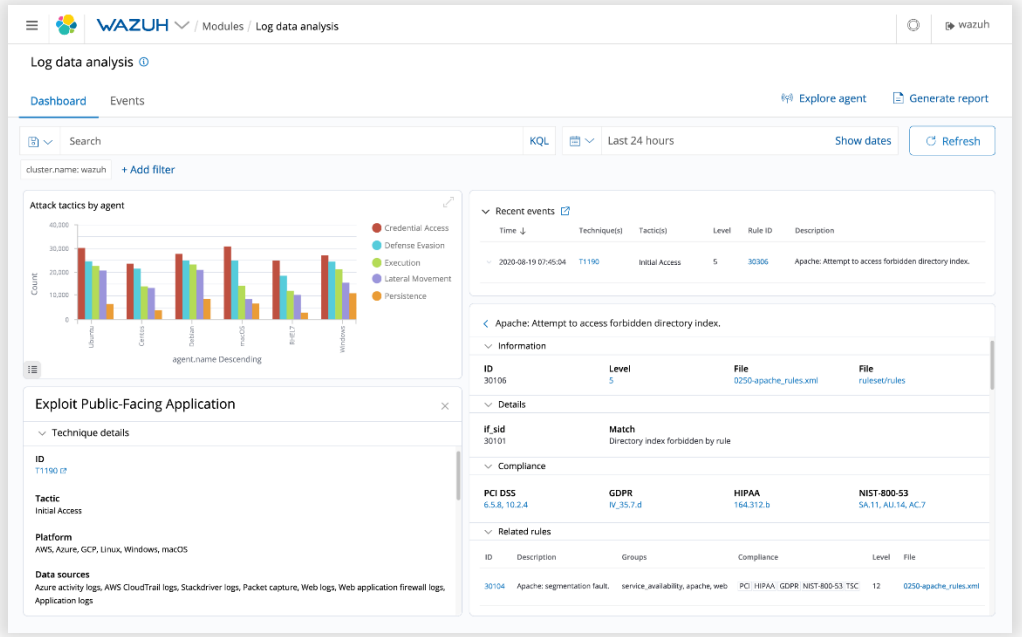
In addition to agent capabilities, the server component uses a signature-based approach to intrusion detection, using its regular expression engine to analyze collected log data and look for indicators of compromise.

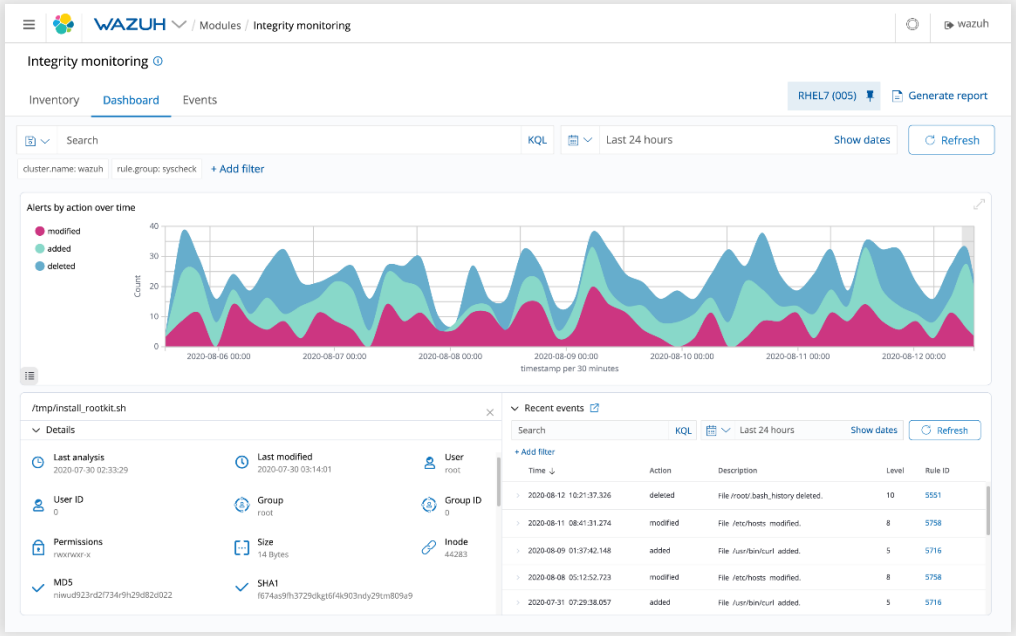
Use cases for your company

Log Data Analysis

The agents can read operating system and application logs, and securely forward them to a central manager for rule-based analysis and storage.

The rules help make you aware of application or system errors, misconfigurations, attempted and/or successful malicious activities, policy violations and a variety of other security and operational issues.





File Integrity Monitoring

The SIEM monitors the file system, identifying changes in content, permissions, ownership, and attributes of files that you need to keep an eye on. In addition, it natively identifies users and applications used to create or modify files.

File integrity monitoring capabilities can be used in combination with threat intelligence to identify threats or compromised hosts. In addition, several regulatory compliance standards, such as PCI DSS, require it.

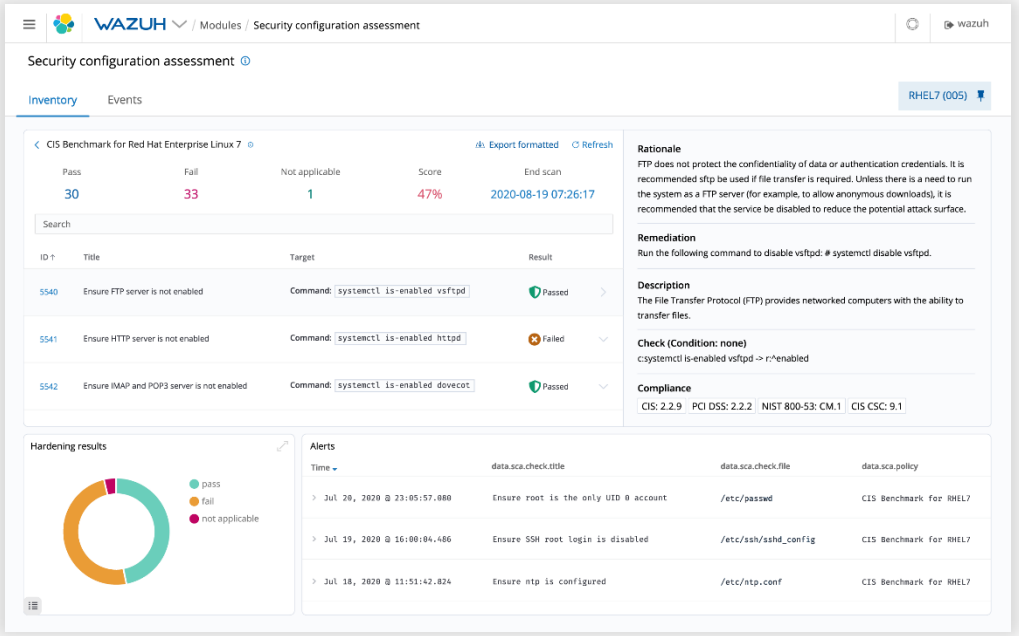
Use cases for your company

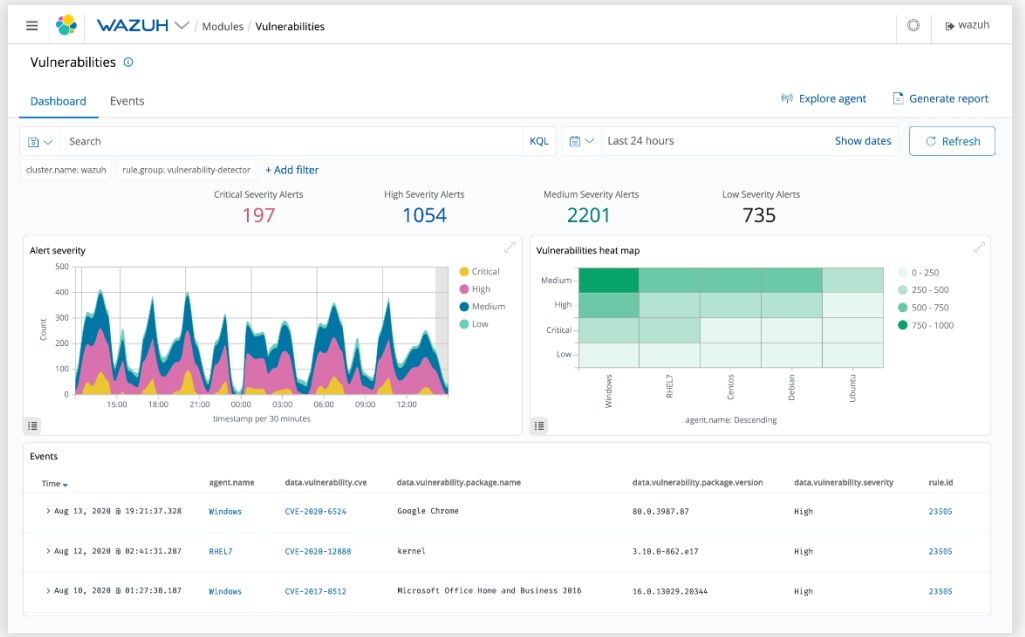
CYBER ONE

Vulnerability Detection

SIEM agents pull software inventory data and send this information to the server, where it is correlated with continuously updated CVE (Common Vulnerabilities and Exposure) databases, in order to identify well-known vulnerable software.

Automated vulnerability assessment helps you find the weak spots in your critical assets and take corrective action before attackers exploit them to sabotage your business or steal confidential data.





Configuration Assessment

The SIEM monitors system and application configuration settings to ensure they are compliant with your security policies, standards and/or hardening guides. Agents perform periodic scans to detect applications that are known to be vulnerable, unpatched, or insecurely configured.
Additionally, configuration checks can be customized, tailoring them to properly align with your organization. Alerts include recommendations for better configuration, references and mapping with regulatory compliance.

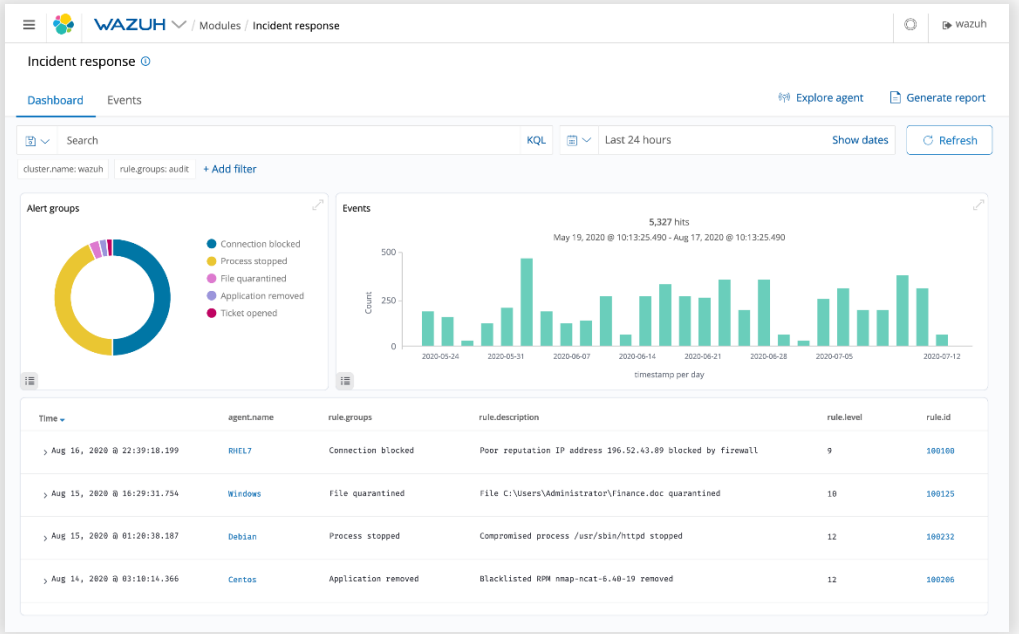
Use cases for your company

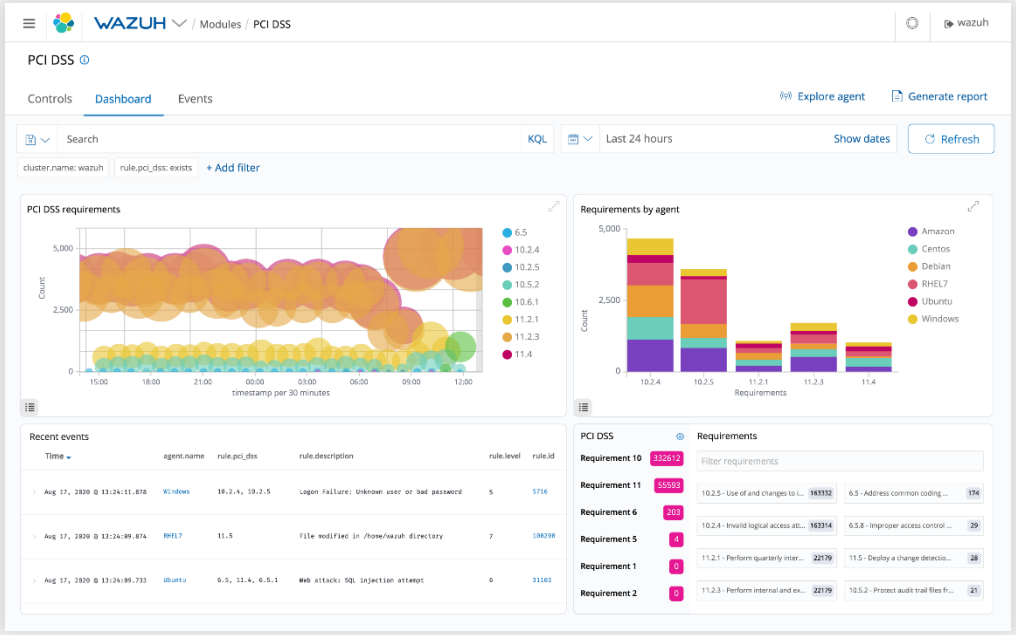
CYBERONE

Incident Response

The software provides out-of-the-box active responses to perform various countermeasures to address active threats, such as blocking access to a system from the threat source when certain criteria are met.

In addition, the SIEM can be used to remotely run commands or system queries, identifying indicators of compromise (IOCs) and helping perform other live forensics or incident response tasks.





Regulatory Compliance

Wazuh provides some of the necessary security controls to become compliant with industry standards and regulations. These features, combined with its scalability and multi-platform support help organizations meet technical compliance requirements.

Wazuh is widely used by payment processing companies and financial institutions to meet PCI DSS (Payment Card Industry Data Security Standard) requirements. Its web user interface provides reports and dashboards that can help with this and other regulations (e.g. GPG13 or GDPR).

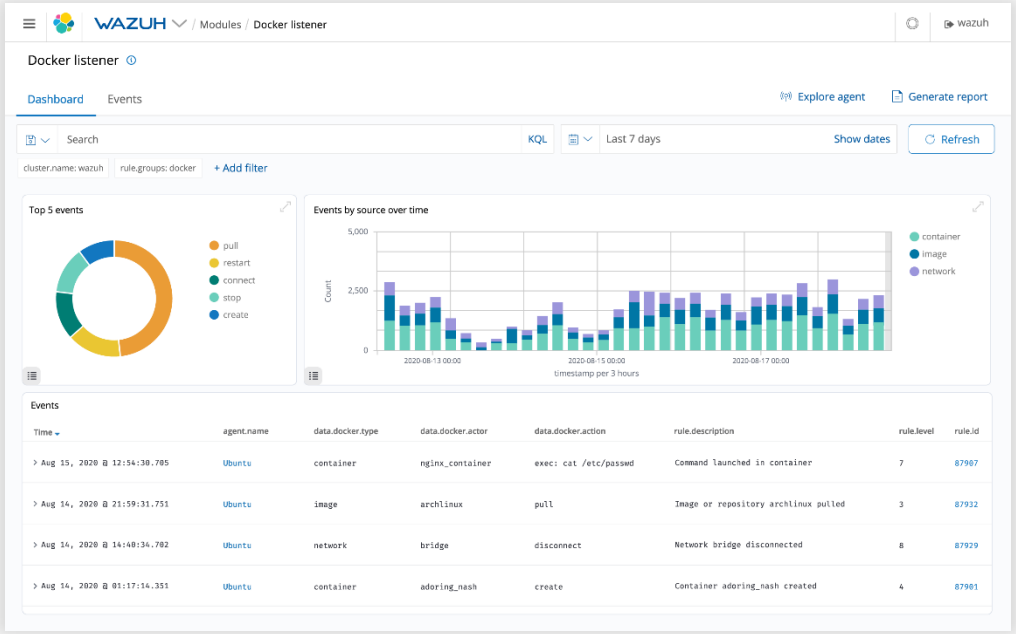
Use cases for your company

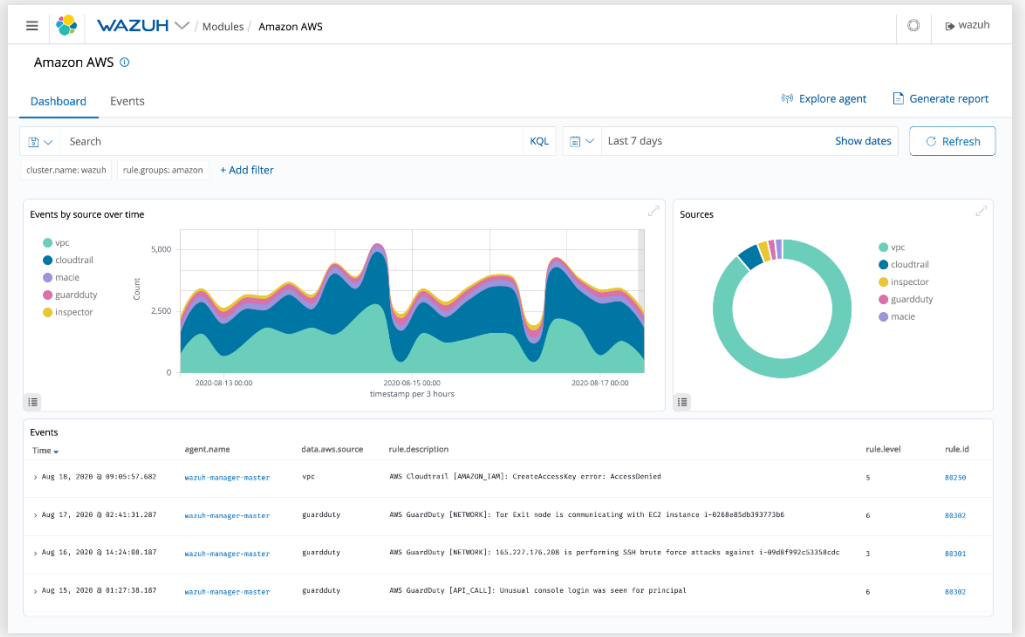
CYBER ONE

Cloud Security

SIEM helps monitoring cloud infrastructure at an API level, using integration modules that are able to pull security data from well known cloud providers, such as Amazon AWS, Azure or Google Cloud. In addition, it provides rules to assess the configuration of your cloud environment, easily spotting weaknesses.

In addition, the SIEM light-weight and multi-platform agents are commonly used to monitor cloud environments at the instance level.





Containers Security

Wazuh provides security visibility into your Docker hosts and containers, monitoring their behavior and detecting threats, vulnerabilities and anomalies. The Wazuh agent has native integration with the Docker engine allowing users to monitor images, volumes, network settings, and running containers.

Wazuh continuously collects and analyzes detailed runtime information. For example, alerting for containers running in privileged mode, vulnerable applications, a shell running in a container etc.

CYBER ONE

Contact us:

www.cyberone.bg
office@cyberone.bg

+359 88 260 0493

51D “Cherni Vrah” blvd.
Sofia, Bulgaria