05. Markov(ProactiveXDR) Key Features

This chapter explains the key features of OpenSASE.

Introduction

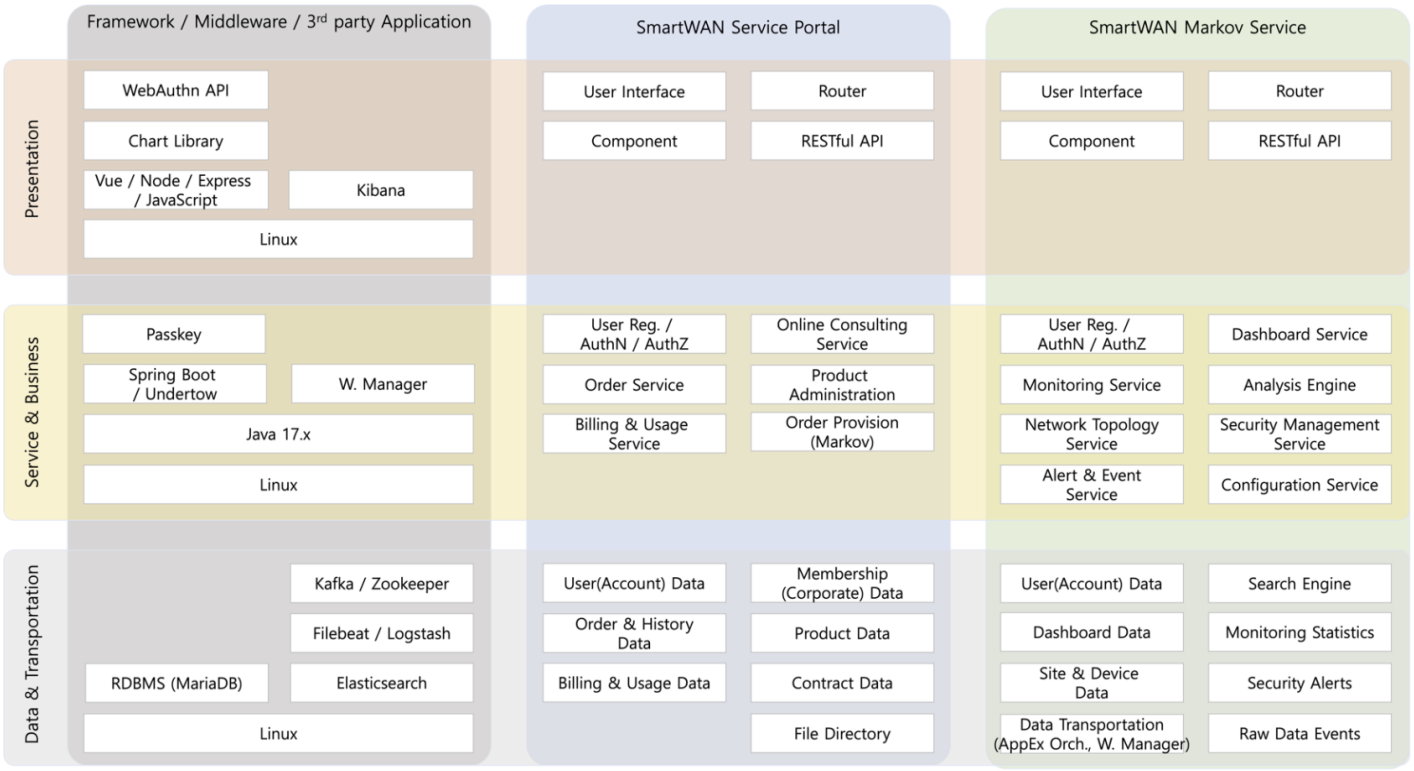
> This document will be continuously updated, and not all the features presented may be fully implemented.
> Some parts of the content are based on the Markov project.

Overview

Unified Security Platform is to provide real-time security monitoring and response services to the customers.
This document describes the key concepts of the platform and provides key features under development.

Architecture

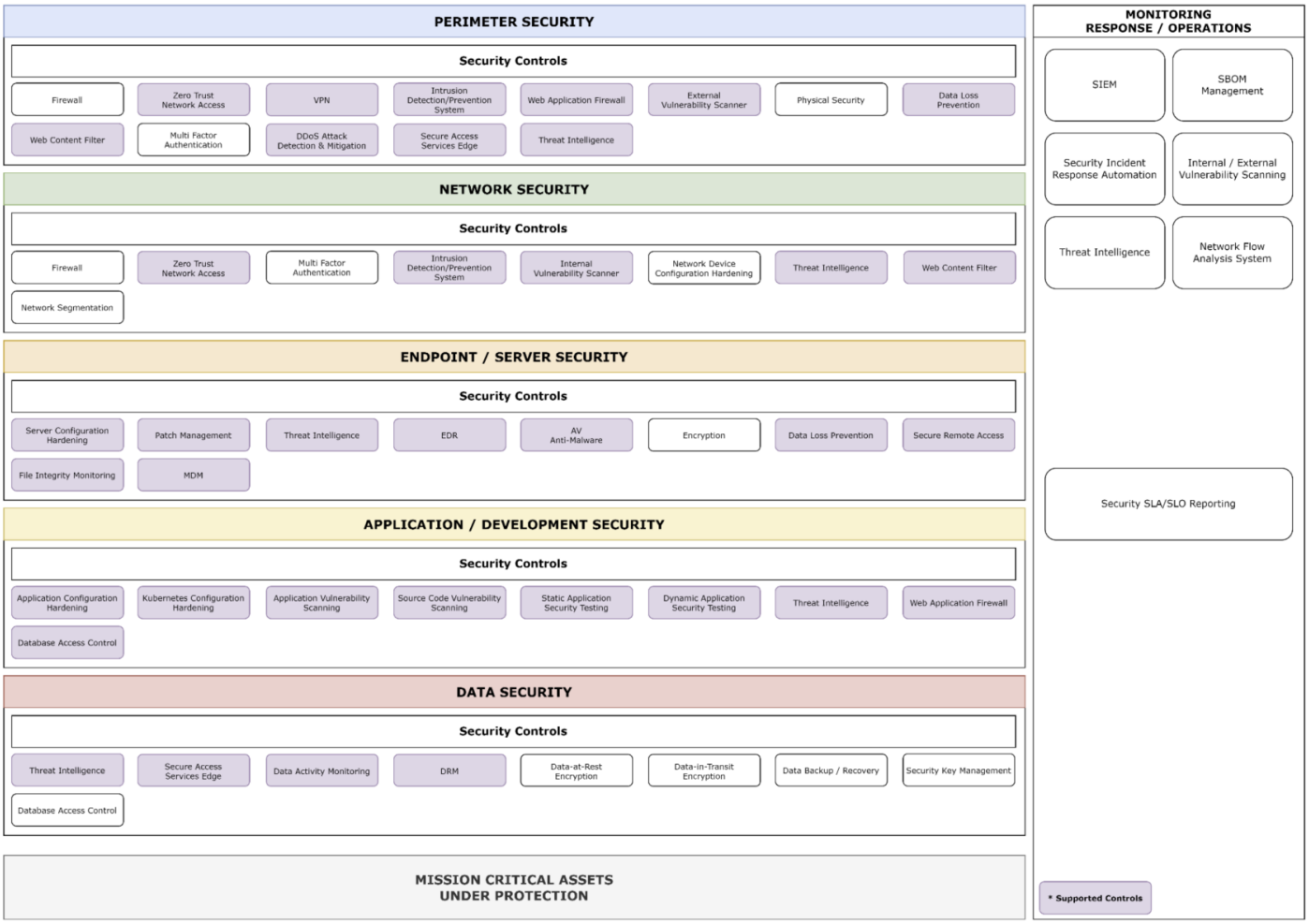
Technical Architecture



This diagram illustrates the end-to-end architecture of the SmartWAN service platform, integrating presentation, business logic, and data layers. The system leverages modern technologies including Vue.js/Spring Boot for frontend/backend, Kafka for real-time data streaming, and Elasticsearch for

analytics. All services are deployed on Linux environments, with RESTful APIs enabling seamless communication between modules.

Defense-in-Depth security model



This architecture diagram maps the key security controls required in each layer of the Defense-in-Depth security model and illustrates how they are supported by this integrated security platform.

The platform is capable of collecting and monitoring logs generated from the security controls highlighted in purple within each layer.

This visual representation clearly demonstrates the scope and capabilities of the integrated security platform across the various layers of the Defense-in-Depth model.

Key Concepts of the Platform

Unified Security Monitoring

The platform integrates traditional on-premises data center security features with cloud environment security capabilities, enabling comprehensive monitoring from a single, unified interface.

This convergence allows customers to maintain consistent security visibility across hybrid infrastructures.

Versatile Data Collection and Analysis

Employing both agent-based and agentless approaches, the platform collects a wide array of log data and vulnerability assessment information.
This multi-faceted data gathering strategy enables thorough security analysis, providing a comprehensive view of the customer’s security posture.

Advanced Security Data Lake

Leveraging a high-performance security data lake capable of sub-second queries on multi-terabyte datasets, the platform offers sophisticated security analytics for network flows.
This capability surpasses traditional security monitoring platforms, providing deep insights into network behavior from a security perspective.

Proactive Security Management

The system incorporates robust vulnerability management features through active security configuration checks and vulnerability identification.
This proactive approach helps customers identify and address potential security weaknesses before they can be exploited.

Streamlined Compliance Management

Offering key compliance management functionalities, the platform facilitates efficient management of compliance evidence.
This feature simplifies the process of meeting regulatory requirements and maintaining audit readiness across various compliance frameworks.

Cloud Security Posture Management

The system offers **comprehensive Cloud Security Posture Management (CSPM)** capabilities for major public cloud platforms, including **Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP)**. This feature provides **in-depth security analysis at the account level**, offering organizations valuable insights into their cloud infrastructure's security stance.

Multi-Cloud Coverage

- Assesses **security configurations across AWS, Azure, and GCP environments**, providing a unified view of an organization's cloud security posture.

Account-Level Analysis

- Performs **detailed security assessments** at the account level, ensuring thorough coverage of all cloud resources and configurations.

Compliance Checks

- Evaluates cloud configurations against **industry-standard best practices and compliance frameworks**.

Automated Assessments

- Conducts **regular, automated scans** of cloud environments to identify potential misconfigurations and security risks.

Detailed Reporting

- Provides **comprehensive security posture analysis reports**, highlighting vulnerabilities, misconfigurations, and areas for improvement.

Remediation Guidance

- Offers **actionable recommendations** to address identified security issues and enhance overall cloud security.

Continuous Monitoring

- Ensures **ongoing assessment of cloud environments** to maintain and improve security postures over time.

By leveraging these **advanced CSPM capabilities**, organizations can **significantly enhance their cloud security, ensure compliance with industry standards, and maintain a robust security posture across their multi-cloud environments**.

GRC Assessment and Evidence Management

> GRC : Governance, Risk & Compliance

The system offers **comprehensive assessment reporting capabilities** for key compliance audits and certifications, including **ISO, PCI-DSS, and ISMS-P**. This feature is designed to assist customers in ensuring adherence to **various regulatory requirements**.

Compliance Mapping and Reporting

- **Data Source Integration**: Logs and data collected from various sources are systematically processed and analyzed.
- **Compliance Requirement Mapping**: Each piece of collected data is mapped to specific requirements of different compliance standards.
- **Compliance Status Tracking**: Provides **real-time visibility** into the organization's compliance posture across multiple frameworks.
- **Evidence Management**: Automated mapping facilitates **easy management and retrieval of compliance evidence**.

This **integrated approach** to compliance reporting and evidence management significantly **reduces the complexity and workload** associated with maintaining multiple compliance certifications.

Network Flow Information Collection and Analysis

The platform **collects, visualizes, and analyzes network flow information** from various sources, including **NetFlow/IPFIX from network switches** and **VPC flow logs from public cloud services**. Network flow data is **correlated with threat intelligence feeds** to perform comprehensive analysis, enabling the detection of **potential security incidents** and **unauthorized access attempts by external threat actors**.

Multi-Source Flow Collection

- Collects **NetFlow and IPFIX data** from **network devices** such as switches, routers, and firewalls.
- Gathers **VPC flow logs** from **major public cloud providers** (AWS VPC Flow Logs, Azure NSG flow logs, GCP VPC flow logs).
- Supports **flow data collection from virtualized network infrastructures**.

Data Visualization

- Provides **interactive dashboards** to present network flow data in a customizable format.
- Displays **network traffic patterns, volume trends, and geo-mapping** of network connections.

Advanced Analytics

- Utilizes **behavioral analysis** to identify anomalies in network traffic patterns that may indicate security threats.
- Conducts **protocol analysis** to gain insights into protocol usage and potential misuse.
- Evaluates **performance metrics** to analyze network performance and utilization trends.

Threat Intelligence Integration

- **Real-time correlation** of network flow data with up-to-date **threat intelligence feeds**.
- **Indicator matching** to identify traffic involving **known malicious IP addresses, domains, or networks**.
- Assigns **risk scores** to network connections based on threat intelligence data.

Security Incident Detection

- Utilizes **machine learning algorithms** for **anomaly detection** in network traffic.

- Flags **unauthorized access attempts** from external sources.
- Monitors **data exfiltration** by detecting unusual outbound traffic patterns.

Comprehensive Reporting

- Generates **customizable reports** on network activity, security incidents, and compliance status.
- Provides tools for **forensic analysis** of security events.
- Supports **regulatory compliance** with network traffic documentation.

By combining **robust network flow collection** with **advanced analytics and threat intelligence integration**, this platform empowers organizations to **maintain a strong security posture, quickly detect potential threats, and gain deep insights into their network activities across both on-premises and cloud environments**.

Security Configuration Assessment

The system offers a **comprehensive Security Configuration Assessment** feature that evaluates the security settings of registered customer assets. This functionality ensures adherence to **industry best practices** and **company security policies**.

Automated Configuration Checks

- Performs regular, automated scans of host systems to assess their security configurations.
- Evaluates a wide range of security settings, including **operating system parameters, application configurations, and network settings**.

Compliance Verification

- Compares current system configurations against predefined **security benchmarks and standards**.
- Identifies deviations from **recommended security practices** and **company-specific policies**.

Customizable Rule Sets

- Allows for the **creation and modification of assessment rules** to align with specific organizational requirements.
- Supports the implementation of **industry-standard benchmarks** as well as **custom security policies**.

Detailed Reporting

- Generates **comprehensive reports** highlighting configuration issues and compliance status.
- Provides **actionable recommendations** for remediation of identified security misconfigurations.

Continuous Monitoring

- Offers **real-time visibility** into the security posture of assessed systems.
- Enables **quick detection and response** to configuration changes that may impact security.

Integration Capabilities

- Seamlessly **integrates with other security tools and processes** within the organization's infrastructure.
- Facilitates a **holistic approach to security management and compliance**.

By leveraging this **Security Configuration Assessment** feature, organizations can **maintain a robust security posture, ensure compliance with industry standards, and quickly identify and address potential vulnerabilities** arising from misconfigurations.

Security Events Collection and Analysis

Agent-Based Log Collection

The platform leverages agent-based log collection capabilities, utilizing the Wazuh agent for comprehensive security event monitoring and analysis.

Supported Operating Systems

The Wazuh agent can be deployed on a wide range of operating systems, including:

- Windows
- Linux distributions
- macOS
- FreeBSD
- OpenBSD
- Solaris

For details on supported platforms, refer to the Official Wazuh Agent Documentation.

Flexible Log Collection

The platform offers versatile log collection options:

- Ability to monitor various log file types and formats
- Support for Windows event logs
- Customizable log parsing and formatting

Configurable Log Sources

Administrators can configure the agent to collect logs from:

- System logs
- Application logs
- Custom log files
- Windows event channels

Advanced Features

- Real-time log monitoring and analysis
- File integrity monitoring
- Command output collection
- Centralized configuration management

Scalability

The agent-based approach allows for efficient log collection across large-scale environments, from individual endpoints to enterprise-wide deployments.

By leveraging the Wazuh agent's capabilities, the platform provides a robust foundation for comprehensive security event collection and analysis across diverse IT infrastructures.

Agentless Log Collection (Active Mode)

The platform actively collects logs from devices that do not support agent installation, such as network devices. It uses SSH to connect to devices and execute commands for log and status information retrieval.

Agentless Collection Method

The system utilizes Secure Shell (SSH) protocol to establish secure connections with target devices, enabling remote log and status information retrieval without on-device agents.

Supported Devices

This method is ideal for:

- Network switches and routers
- Firewalls
- Load balancers
- Other network appliances or devices with limited software installation capabilities

Collection Process

- **Secure Connection**: The platform initiates an SSH connection to the target device.
- **Command Execution**: Pre-configured or custom commands are executed on the device.
- **Data Retrieval**: Log data or status information is collected based on command output.

Flexibility

- **Customizable Commands**: Administrators can tailor the commands executed on each device type to collect specific logs or information.
- **Scheduled Collection**: Log retrieval can be automated regularly to ensure up-to-date information.

This agentless approach significantly enhances the platform's ability to provide a holistic view of an organization's security posture, integrating both agent-supported and agentless devices.

Agentless Log Collection (Passive Mode)

The platform offers advanced log processing capabilities with a focus on **syslog protocol integration**. Its architecture is highly flexible and scalable, adapting to various log volume requirements.

Syslog Processing

The system efficiently handles logs transmitted via the syslog protocol, a widely used standard for system logging.

Flexible Ingestion Architecture

Depending on anticipated log volume, the platform can be configured with:

- **Multiple Remote Syslog Servers**: For distributed log collection and processing.
- **Message Bus Systems**: Integration with technologies like Kafka for high-throughput log streaming.

Scalable Design

The platform's architecture is tailored to match expected log volumes, ensuring optimal performance and resource utilization.
This approach enables efficient management of varying loads, from small-scale deployments to enterprise environments with massive log volumes.

Public Cloud Audit Logs Collection

The platform offers comprehensive **audit and management log collection** for major public cloud environments, including **AWS, Google Cloud Platform (GCP), and Microsoft Azure**. This integration allows organizations to centralize and analyze critical operational data from their multi-cloud infrastructures.

- **Multi-Cloud Coverage**: Native support for major cloud providers ensures broad visibility across diverse cloud environments.
- **Audit and Management Focus**: The platform collects security-critical audit and management logs for compliance and operational oversight.
- **Extensible Framework**: Custom integrations can be developed for cloud services not natively supported.
- **Tailored Solutions**: The platform adapts to unique organizational requirements, enabling additional integrations as needed.

By centralizing these critical logs, the platform enhances **cloud governance, security monitoring, and compliance management** across multi-cloud environments.

SaaS Audit Logs Collection

The platform supports **log collection from various SaaS applications**, providing multi-source log integration tailored to client needs.

- **Diverse SaaS Integration**: Collect logs from multiple SaaS services, accommodating various application types and data formats.
- **Customizable Implementation**: Integration is provided on a per-request basis to meet unique client requirements.
- **Flexible Log Collection**: The system handles multiple log types and sources simultaneously for a comprehensive view of an organization’s SaaS ecosystem.
- **Scalable Solution**: As new SaaS applications emerge, the platform can incorporate additional log sources as needed.

This flexible and extensible approach enables **deeper insights into SaaS operations, enhanced security monitoring, and improved operational visibility** across cloud-based services.

Topics to discuss [NDA]

LLM/SLM Integration

Anomaly Detection & MLOps

Automated Response

Federated Authentication

Vulnerability Management

Agent-Based Vulnerability Detection

The platform provides **comprehensive vulnerability analysis** based on operating system and package information collected from deployed agents.

Data Collection

- Agents gather detailed information about the host's operating system, installed packages, and configurations.
- This data is continuously collected and sent to the central platform for analysis.

Vulnerability Analysis

- The collected information is correlated with up-to-date vulnerability databases.
- The platform identifies potential vulnerabilities by comparing installed software versions against known vulnerabilities.

Real-Time Detection

- Agents continuously monitor and report changes, enabling real-time detection of new vulnerabilities.
- This allows for rapid identification of security risks introduced by system updates or new software installations.

Comprehensive Coverage

- The agent-based approach enables deep scanning of endpoints, including those that may be difficult to assess with network-based scans.
- It provides visibility into vulnerabilities across a diverse range of operating systems and software packages.

Efficient Processing

- By leveraging agent-collected data, the platform performs vulnerability assessments more efficiently than traditional network-based scans.
- This approach reduces network overhead and allows for more frequent vulnerability checks.

By utilizing this agent-based vulnerability detection method, the platform offers organizations a powerful tool for maintaining a robust security posture and quickly identifying potential threats.

SBOM (Software Bill of Materials) Analysis

The platform provides **advanced SBOM analysis capabilities**, leveraging agent-based systems to generate and analyze comprehensive software component inventories.

SBOM Generation

- **File System Scanning**: Agents perform thorough scans of file systems to identify and catalog software components.
- **Container Image Analysis**: The system examines container images to extract detailed component information.
- **CycloneDX Format**: SBOMs are generated in the **industry-standard CycloneDX format**, ensuring compatibility and ease of integration.

Vulnerability Identification

- **Component Analysis**: Each identified software component is scrutinized for known vulnerabilities.
- **Continuous Monitoring**: The system regularly updates its vulnerability database to provide current security insights.
- **Risk Assessment**: Vulnerabilities are prioritized based on severity and potential impact.

Comprehensive Reporting

- **Detailed Inventories**: Customers receive **comprehensive lists of all software components** in their systems.
- **Vulnerability Reports**: The platform provides **detailed reports** on identified vulnerabilities associated with SBOM components.
- **Actionable Insights**: Reports include recommendations for **remediation and risk mitigation**.

Integration and Automation

- **CI/CD Pipeline Integration**: SBOM generation and analysis can be integrated into **continuous integration and deployment (CI/CD) processes**.
- **Automated Alerts**: The system can be configured to **send alerts** when critical vulnerabilities are detected in SBOM components.

By utilizing **SBOM analysis**, customers gain **deep visibility into their software supply chain**, proactively identify security risks, and maintain a **robust security posture** across their IT infrastructure.

Remote Vulnerability Analysis

The platform offers **comprehensive remote vulnerability analysis**, focusing on two key areas:

Public IP Asset Discovery

The system performs thorough scans of **customer public IP ranges** to identify exposed assets.

- Utilizes **advanced IP range detection techniques** to accurately determine the customer's public IP address blocks.
- Employs **network scanning tools** to discover active hosts and services within these IP ranges.
- Identifies and catalogs **internet-facing assets** such as web servers, databases, and other network services.
- Provides a **detailed inventory** of exposed assets, including IP addresses, hostnames, and open ports.

Automated HTTPS URL Vulnerability Assessment

The platform conducts **automated security scans** on HTTPS URLs to detect vulnerabilities.

- **Comprehensive web application vulnerability scans** on discovered HTTPS endpoints.
- Utilizes a combination of **passive and active scanning techniques** to minimize impact on target systems.
- **Assess SSL/TLS configurations** for potential weaknesses.
- Checks for **common misconfigurations** in web servers and application frameworks.
- Generates **detailed reports** highlighting discovered vulnerabilities, severity levels, and recommended remediation steps.

This approach enables organizations to **proactively identify and address security weaknesses** in their internet-facing infrastructure, significantly enhancing their **overall security posture**.