Detection and Response tools (SecOps tools)

Security Operations Center (SOC)

- The SOC is the operational arm of the CISO
- A SOC is a dedicated team responsible for
  - monitoring security events across an organization
  - detecting threats and anomalies
  - responding to incidents
  - improving security posture over time
  - implements and provides metrics and reports to the CISO on threat landscape and incident trends.

Detection (and Response)

- SOC needs
  - Detection of intrusions and anomalies on end-systems
  - Detection of intrusions and anomalies at larger scale
  - Correlation of data form several sources
  - Stop intruders or react to problems as quickly as possible

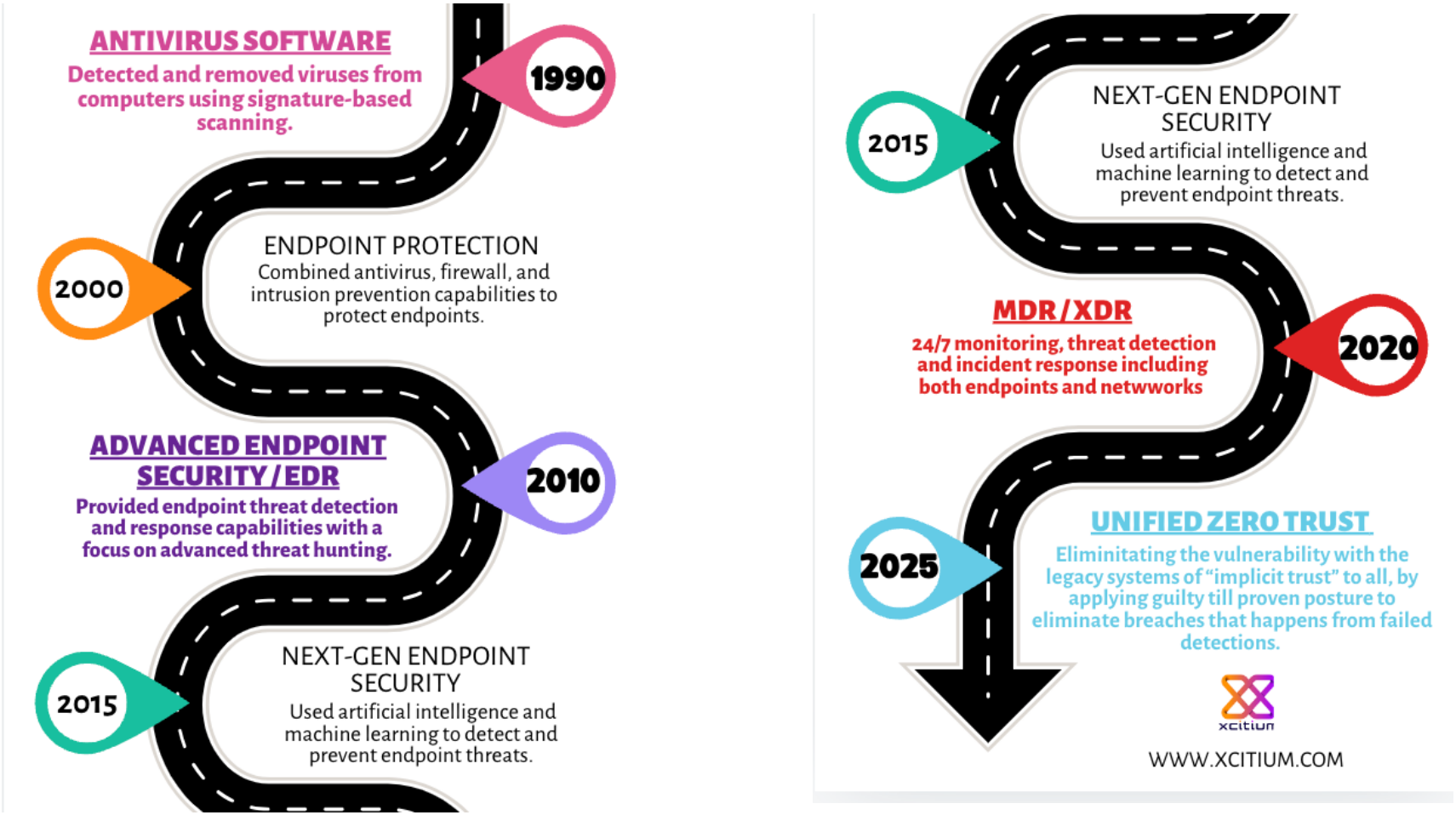
- It takes advantage of tools like SIEM, SOAR, EDR, and XDR.

Two point of views

- Endpoint centric
  - Detect and react locally, quickly with a reduced amount of data available
  - EDR, XDR
- Organization centric
  - Collection of data from many sources to get a big picture of what is going on and possibly react
  - SIEM, SOAR

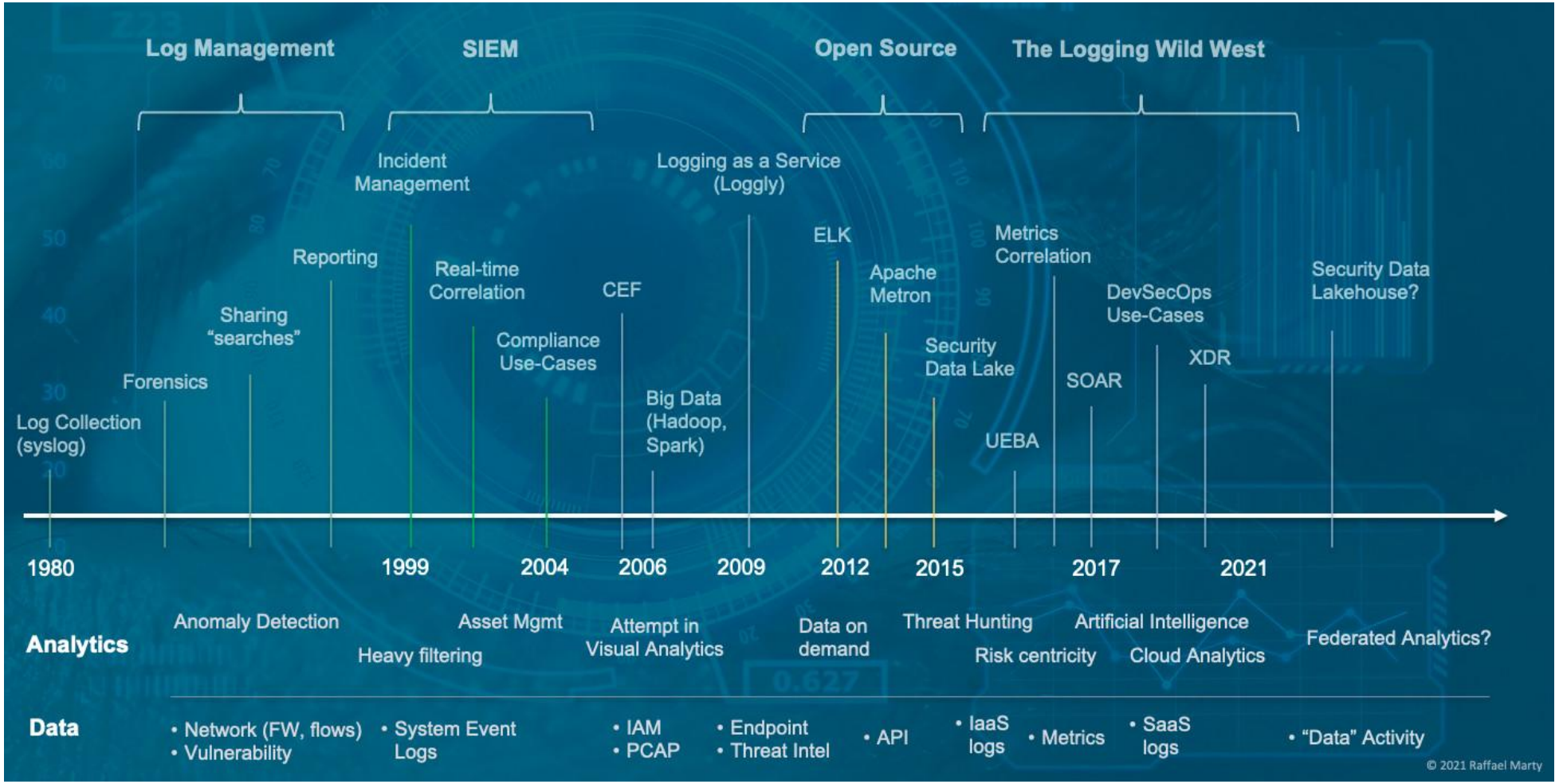
- They are two point of views that are currently converging
  - Convergence does not mean same language though…

history of EDR-like systems



- https://melih.com/the-evolution-of-endpoint-security-from-antivirus-to-unified-zero-trust/

SIEM history



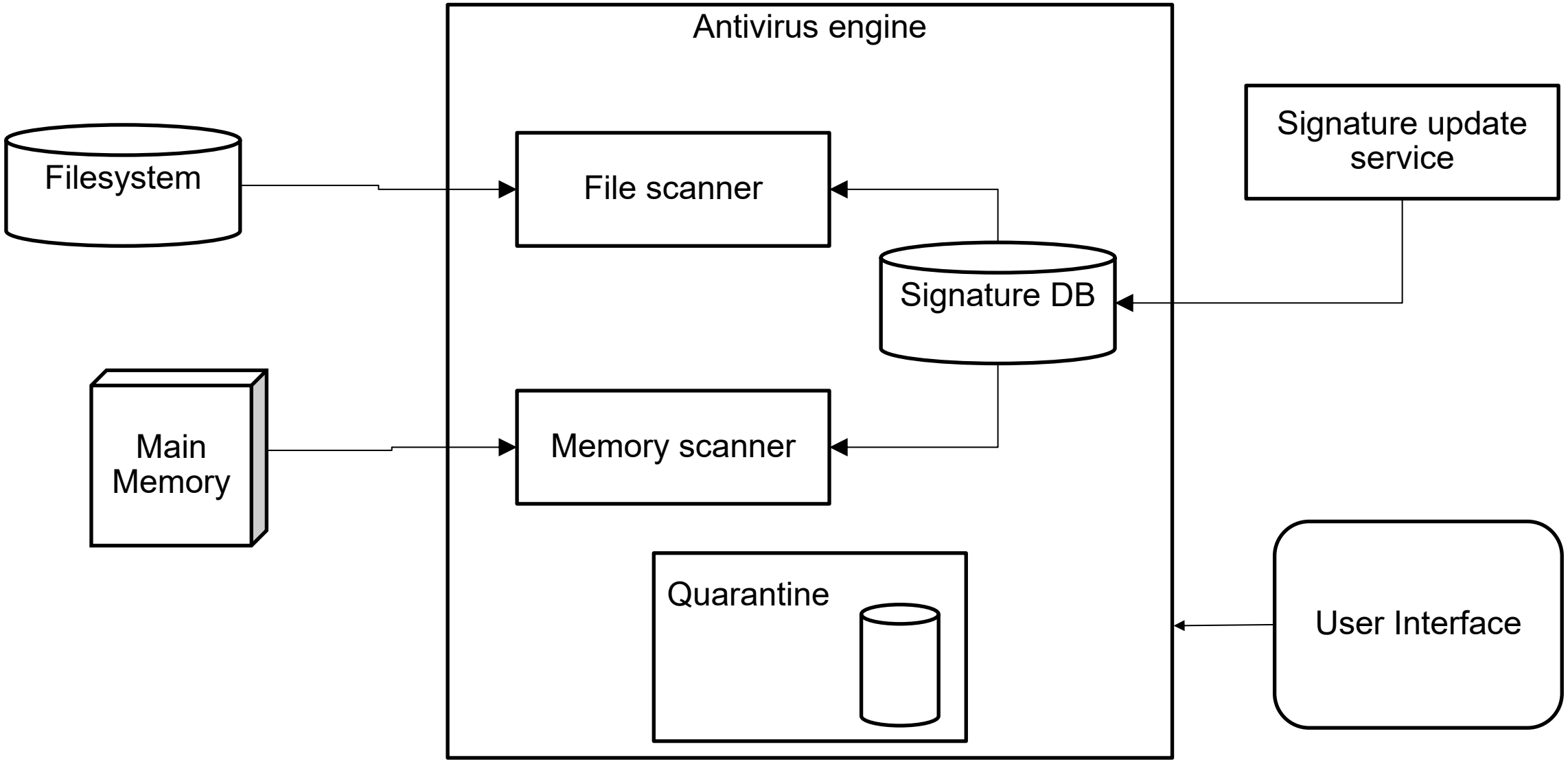
A Logging History Lesson – From syslogd(8) to XDR by Raffel Marty

Anti-virus

- Key Characteristics:
  - Signature-based detection
  - Periodic scanning of files and memory
  - Centralized update mechanism

- Components:
  - Antivirus Engine: Installed on endpoint, scans files and memory.
  - Signature Database: Contains known malware patterns.
  - Signature update service: Pushes new signatures to endpoints.
  - Quarantine Module: Isolates detected threats.
  - User Interface: Allows manual scans and settings.

Antivirus architecture



Endpoint Detection and Respones (EDR)

- Endpoint Detection and Response (EDR) Architecture
  - Continuous monitoring of endpoint activity
  - Behavioral analysis and anomaly detection
  - Real-time response (e.g., isolate host, kill process)
  - Integration with threat intelligence
  - Support forensic analysis by collecting and save relevant data
  - Threat hunting (of normally undetected threats)

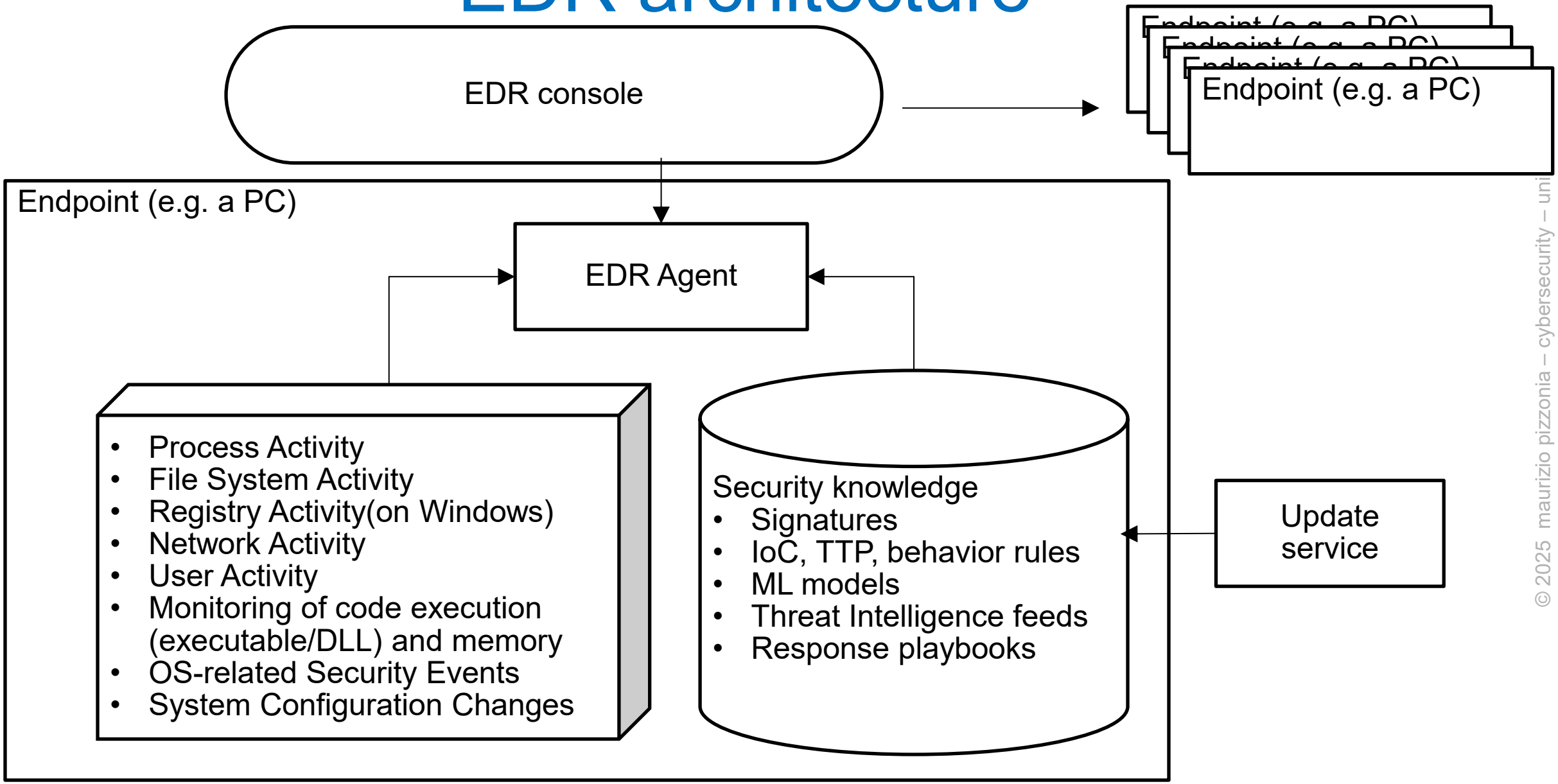
EDR: considered data (examples)

- Process Activity
  - Process creation and termination
  - Parent-child process relationships
  - Command-line arguments
  - Hashes of executables
- File System Activity
  - File creation, modification, deletion
  - Access to sensitive or system files
  - File path and metadata
  - Suspicious file drops (e.g., in /tmp folders)
- Registry Changes (on Windows)
  - Registry key creation/modification
  - Persistence mechanisms (e.g., Run keys)
- Network Activity
  - Outbound/inbound connections
  - DNS queries
  - IP addresses and ports
  - Protocols used (HTTP, HTTPS, SMB, etc.)
- User Activity
  - Logins/logouts
  - Privilege escalation attempts
  - Remote desktop or shell usage
- Monitoring of code execution (executable/.so/.DLL) and memory
  - In-memory execution of code
  - Suspicious memory patterns
- OS-related Security Events
  - OS security logs
  - Failed login attempts
- System Configuration Changes
  - New services or drivers
  - Scheduled tasks
  - Group policy changes

EDR “security knowledge”
updated regularly

- Signature Databases
  - For detecting known malware and threats, similar to traditional antivirus.
- Detection Rules and Heuristics
  - Behavioral rules (e.g., suspicious shell usage)
  - Tactics, techniques, and procedures (TTPs) based on frameworks like MITRE ATT&CK.
- Machine Learning Models
  - Some EDRs use ML to detect anomalies or classify threats.
  - These models are periodically retrained and/or updated.
- Threat Intelligence Feeds
  - IoC: IPs, domains, file hashes, and URLs associated with malicious activity.
  - Often integrated from third-party or proprietary sources.
- Response Playbooks
  - Automated response actions (e.g., isolate host, kill process).
  - Can be configured to reflect new threats or organizational policies.
- Agent Software
  - The endpoint agent itself receives updates for:
    - New detection capabilities
    - Performance improvements
    - Security patches

EDR architecture



EDR response examples

- Isolate Endpoint from Network
  - Prevents lateral movement or data exfiltration
  - while allow EDR console communication.
- Kill Malicious Process
- Delete or Quarantine File
- Rollback Changes
  - e.g. for ransomware
- Initiate Forensic Data Collection
  - memory dumps, network traffic, or logs
- Alert and Notify
  - to SOC with forensic data
- Block execution of certain other executables
- Trigger SOAR Playbooks

EDR, response and SOC

- Response actions can be…
  - Fully automated
  - Manual
  - Hybrid (man-in-the-loop): a human analyst makes key decisions during the response process

eXtended Detection and Response (XDR)

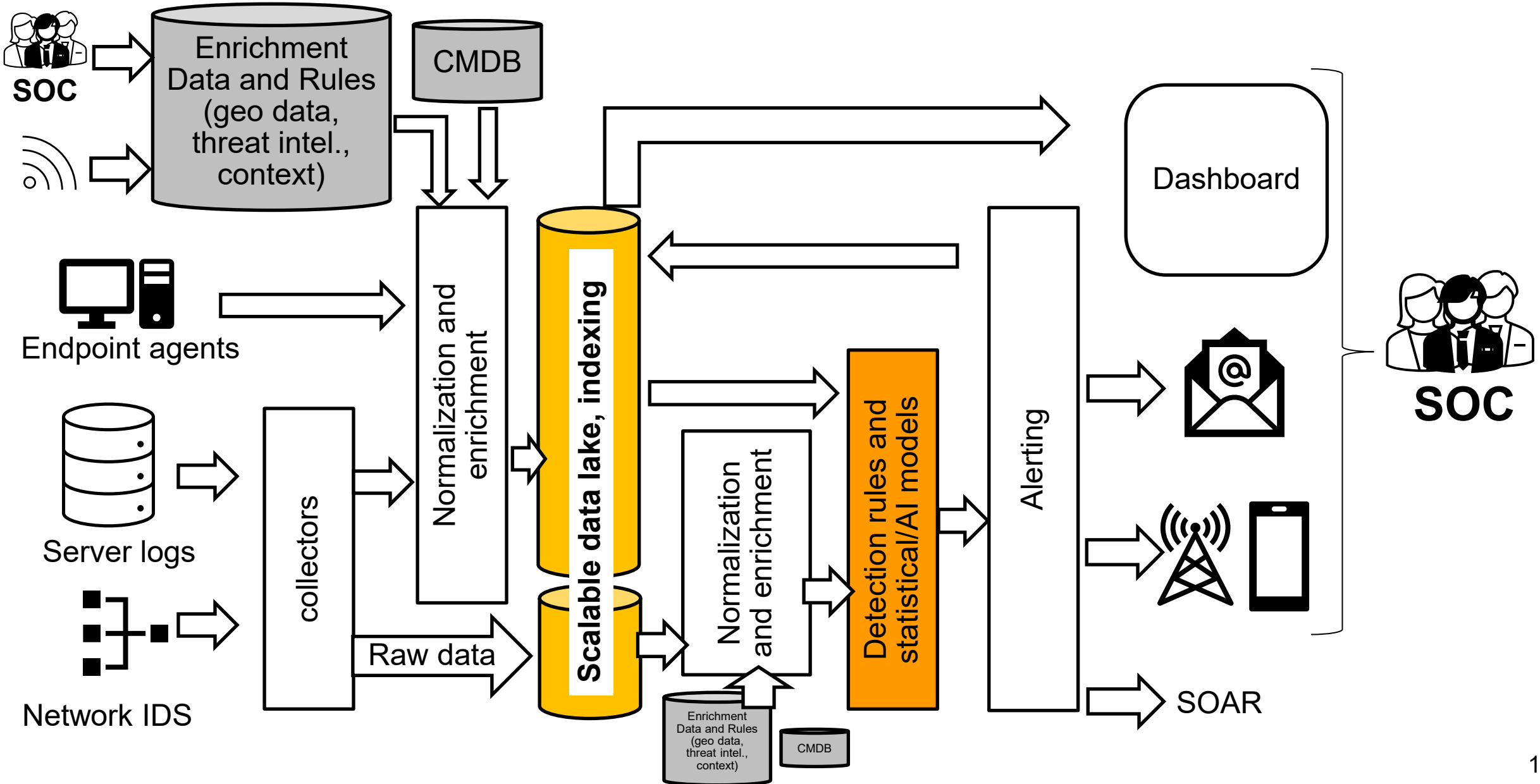
- Evolution of EDR
- Typically cloud-native
- Add…
  - correlating signals across endpoints, network, cloud, and identity systems.
  - Network: NIDS traffic patterns, DNS anomalies
  - Email: phishing attempts, malicious attachments/links
  - Cloud activity logs: access patterns, API calls, misconfigurations
  - Identity and access logs: MFA failures, unusual login locations
  - SIEM logs: correlated events from firewalls, proxies, VPNs, etc.

- Support detecting **multi-vector attacks**

Security Information and Event Management (SIEM)

- combines log management, event correlation, and security analytics
- Purpose:
  - Detect, analyze, and respond to security incidents in real time.
- Core Functions:
  - Collect logs & events
  - Correlate across systems
  - Alert on anomalies
  - Support compliance

SIEM Architecture



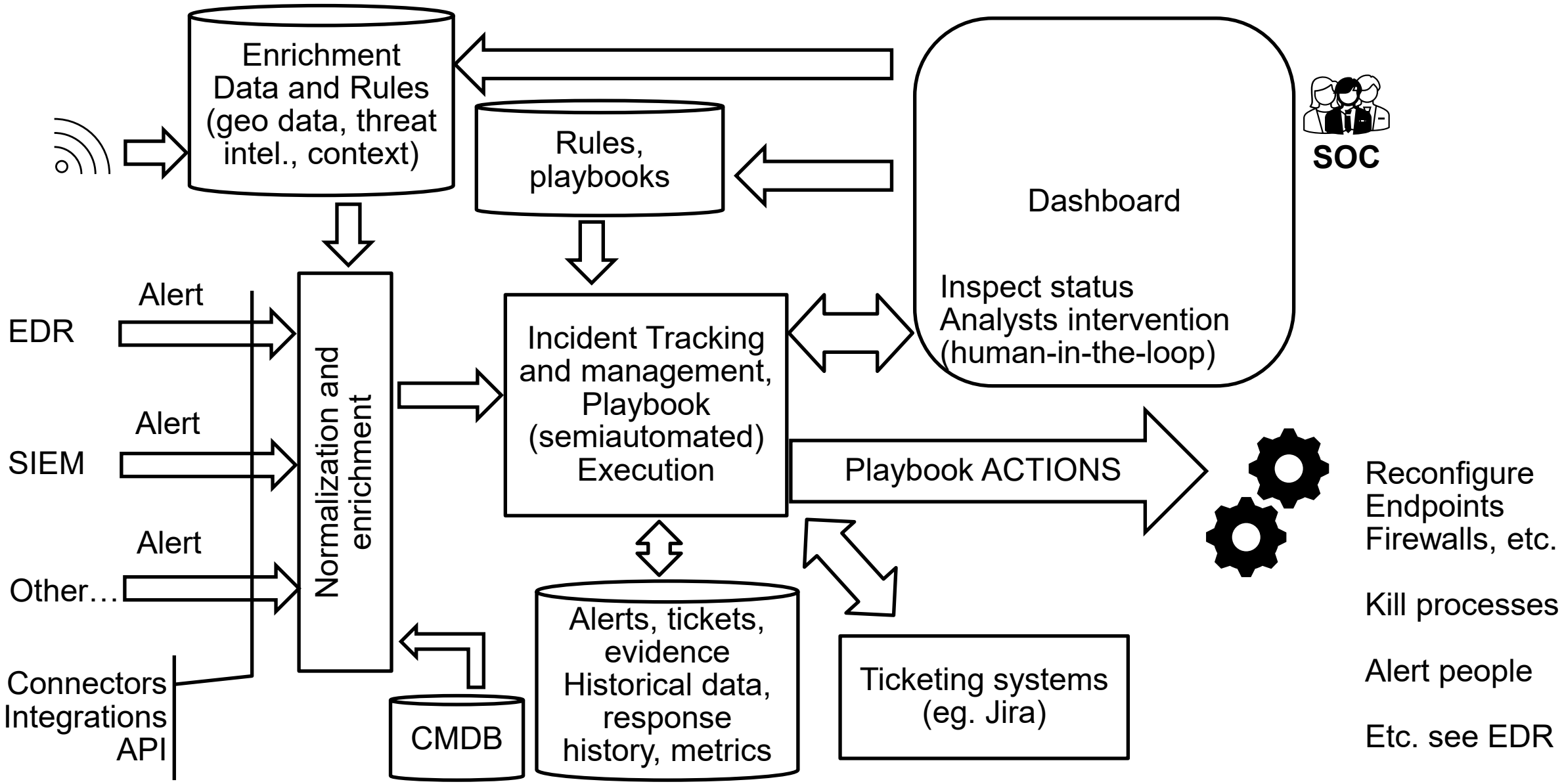
SIEM data flow

- Collect data from endpoints, network, NIDS, thorough agents (push) or collectors (pull)
- Enrich data with context taken form other sources
  - E.g. geolocalization, hostnames, Configuration Management DB, other info from threat intelligence feeds, etc.
- Store in a data lake (raw or processed), indexed
- Retrieve possibly with further enriching of data to…
- …apply detection rule-based and/or anomaly-based
- Alerts are notified and/or put into the data lake
- SOC can use a dashboard to manage the process

SOAR

- SOAR stands for Security Orchestration, Automation, and Response
- It is a platform that helps security teams coordinate, automate, and accelerate incident response by integrating multiple cybersecurity tools and processes.
- It typically connects to tools like…
  - SIEM
  - EDR
  - Threat Intelligence Platforms (TIP)
  - Ticketing systems (JIRA, ServiceNow)
  - Firewalls, email gateways, IAM, etc.

SOAR architecture



Current SIEM/XDR systems

- SIEM evolved to include
  - reaction (SOAR) functionalities
  - Endpoint data collection (typical of EDR)
- XDR evolved to include
  - data from a large number of systems, logs, devices, etc (typical of SIEM)

- Enterprise level solutions usually are (or aim to be)…
  - Cloud based, real-time, anomaly-based (UEBA), integrated with threat intelligence feeds to know the most up-to-date threats

Zero Trust

- No differences between trusted and untrusted entities or users: **Always verify**
- Identity and Access Management (SSO, MFA, RBAC)
- “Assume Breach”: e.g. design systems as if attacker is already inside
- Least privilege
- Network micro-segmentation (mini firewalls)
- Continuous monitoring
- Check device security posture before connection
- etc.

Zero Trust vs. detection and response

- Zero Trust tools are the first line of defense
- SIEM/XDR are the second line of the defense

- They are increasingly integrated, though
  - IAM → SIEM/XDR
  - ZT logging → SIEM/XDR
  - SIEM/XDR detection → IAM user blocked, ZT policy update, etc.

Open Source SIEM/XDR Tools

Tool	Type	Key Features	Pros	Cons
Wazuh	SIEM + XDR	Log analysis, threat detection, compliance, vulnerability scanning, FIM	strong community, excellent endpoint security	Requires tuning for large deployments, limited SOAR capability
UTMStack	SIEM + XDR	Real-time correlation, threat intelligence, compliance reporting, SOAR playbooks (for paid version)	More user friendly than wazuh, easy deployment	Smaller community than Wazuh, less scalable,
OSSEC	SIEM (HIDS)	Host-based intrusion detection, log monitoring	Lightweight, simple setup	Limited visualization, lacks XDR features
Security Onion	SIEM + NIDS	Network monitoring, packet analysis, intrusion detection	Great for network security, strong toolkit	Complex setup, resource-intensive

Wazuh, UTMStack and Security Onion are based on ELK stack