Securing Critical Infrastructures In The Financial Sector

Adaptive and Intelligent Data Collection

Challenges

- Intelligent monitoring and data collection of security related information
- Predictive analytics over the collected data based on AI/DL-based mechanisms that enable the identification of complex attack patterns
- Triggering of preventive and mitigation measures in advance of the occurrence of the attack
- Amount of data collected is growing every day, and these huge amounts of data can no longer be stored efficiently or processed in real time

Impact on businesses

Security of critical financial infrastructure and services

- tracked and maintained through the collection and analysis of security-related data
- intelligent, efficient, secure and timely manner

Making security data collection and analysis intelligent

- capable of quickly spotting, learning from, and addressing zero-day threats
- economizing of resources and accessing the right information at the right time
- configuring data collection probes and adapting collection strategies

Cyber & Physical Integrated Security

Security violations

- detect anomalies in the physical system domain which aren’t introducing anomalies in the cyber domain

Combine knowledge from both cyber and physical domains

- estimate the real impact of attacks on cyber-physical system
- optimize the computation and reduce attack detection latency

Integrate control algorithms and estimation techniques

Data collection requirements

Efficiency - collected data should be compact

- needed data should be collected in a real-time and high-speed manner to decrease the time delay of attack detection

Privacy - sensitive information should be protected

Resource consumption

- power, memory, and network bandwidth in the process of data collection and data communication

Adaptability and Intelligence

- adaptable to the context of the physical and cyber-world, as well as to the changing security context
- intelligent towards optimizing the amount of information available for the security task at hand, while ensuring availability of the proper information.

Configurability - data collection systems (e.g., probes) must be configurable

Automation

- automate data collection and adaptation by adjusting to different environmental contexts and situations.
- ML techniques are helpful for implementing automatic adaptable solutions capable of adjusting to new situations and timely reacting in the face of threats and anomalies

Data Sources and Data Collection Categories

Data sources

- From which security event data are collected include, but are not limited to, network traffic data, firewall logs, web logs, system logs, router access logs, database access logs, and application logs, system statistics, etc.

Data Collection Categories

- **Packet-level data** consists of a packet header and a packet payload. Generated when using protocols like TCP, UDP, ICMP, etc.: Source/Destination IP address, Source/Destination port, Time to live, Timestamp, Packet payload, Packet size, and Number of packets.
- **Flow-level data** consists of stream of packets: Flow count, Flow type, Flow size, Flow direction, Flow duration, and Flow rate
- **Connection-level data**: Connection will contain many flows
  - Flow does not have size restriction, i.e., the flow is generated even if a single packet has been exchanged but a connection is generated by at least two packets
  - Connection level data can be divided into: Connection size, Connection duration, Connection count, and Connection type
- **Host-level data** are collected from a host
  - Provide comprehensive knowledge of system events such as its records host activities, changes, resource consumption, etc.
  - Two commonly used types: CPU and Memory usage and Operation log

Predictive Security Analytics for Adaptive Data Collection

- Predictive analytics are used to predict security attacks, threats, and anomalies
- Based on the predicted security events, mitigation measures can be triggered, for example, to adapt the data collection rate, close a door, etc.
- Requires constant monitoring, capturing, and processing large amounts of various data
  - Collected data are often redundant. Thus, the storing and processing resources are used unnecessary, and the same prediction results can be achieved with significantly less data
  - Important to develop lightweight predictive data analytics that can give earlier indications about possible attacks based on less data amount and processing
  - reducing the amount of collected and processed data while maintaining the required level of threat detection.
- For lightweight specific level of analytics for adaptive data collection strategies
  - Algorithms such as Random Forest, Random Forest, Adaboost, Decision Tree, Support Vector Machine, etc can be used with promising accuracy results (close to 99%).
- For identification of complex attack patterns
  - AI/DL-based predictive analytics can be used

Quality attributes for analytics of data collection

Performance

- measure of how quickly a system responds to user inputs or other events
- ML algorithm optimization, feature selection and extraction, data cutoff

Accuracy

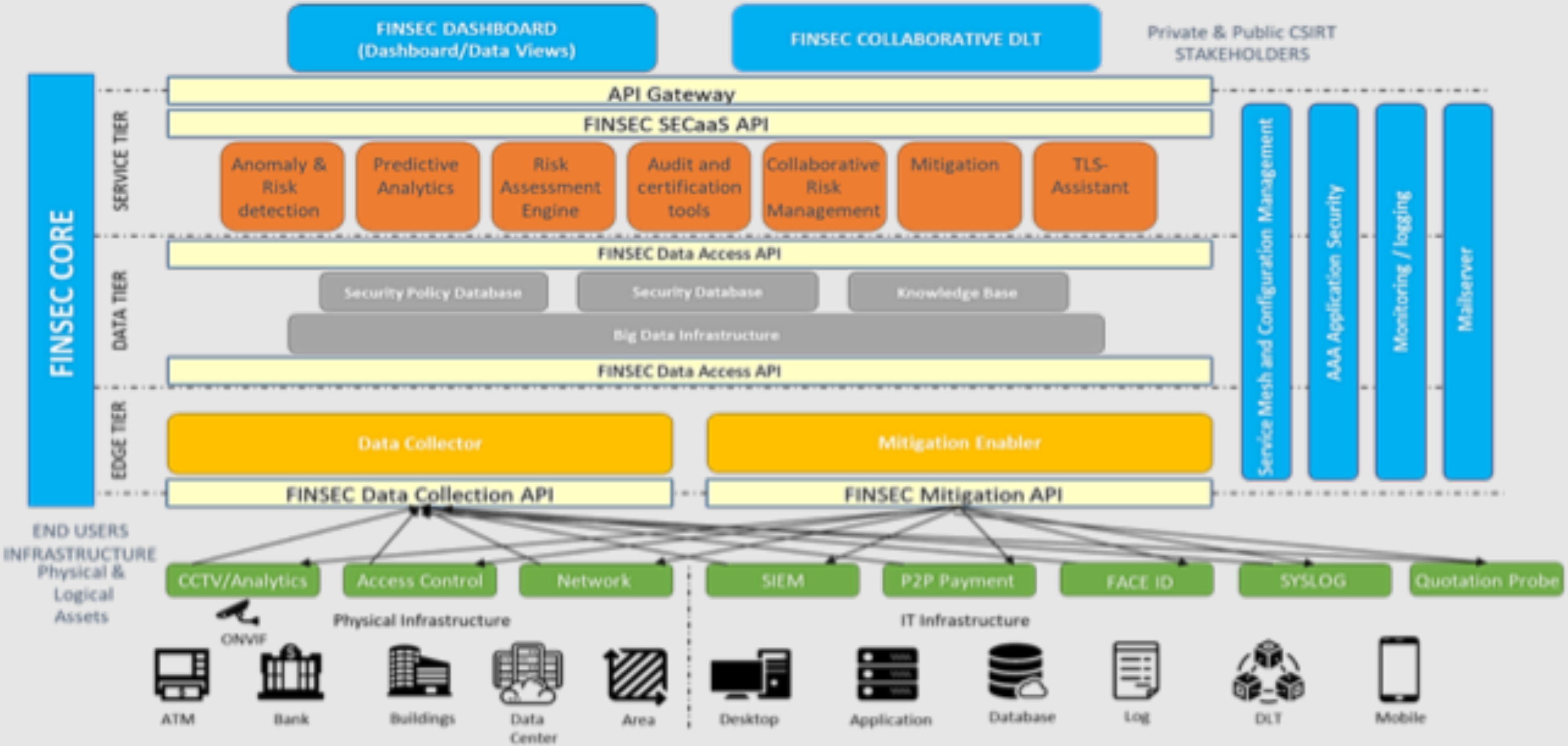
- measure to which a system provides the right results with the needed degree of precision
- alert correlation, combining signature-based and anomaly-based detection

Security & privacy assurance

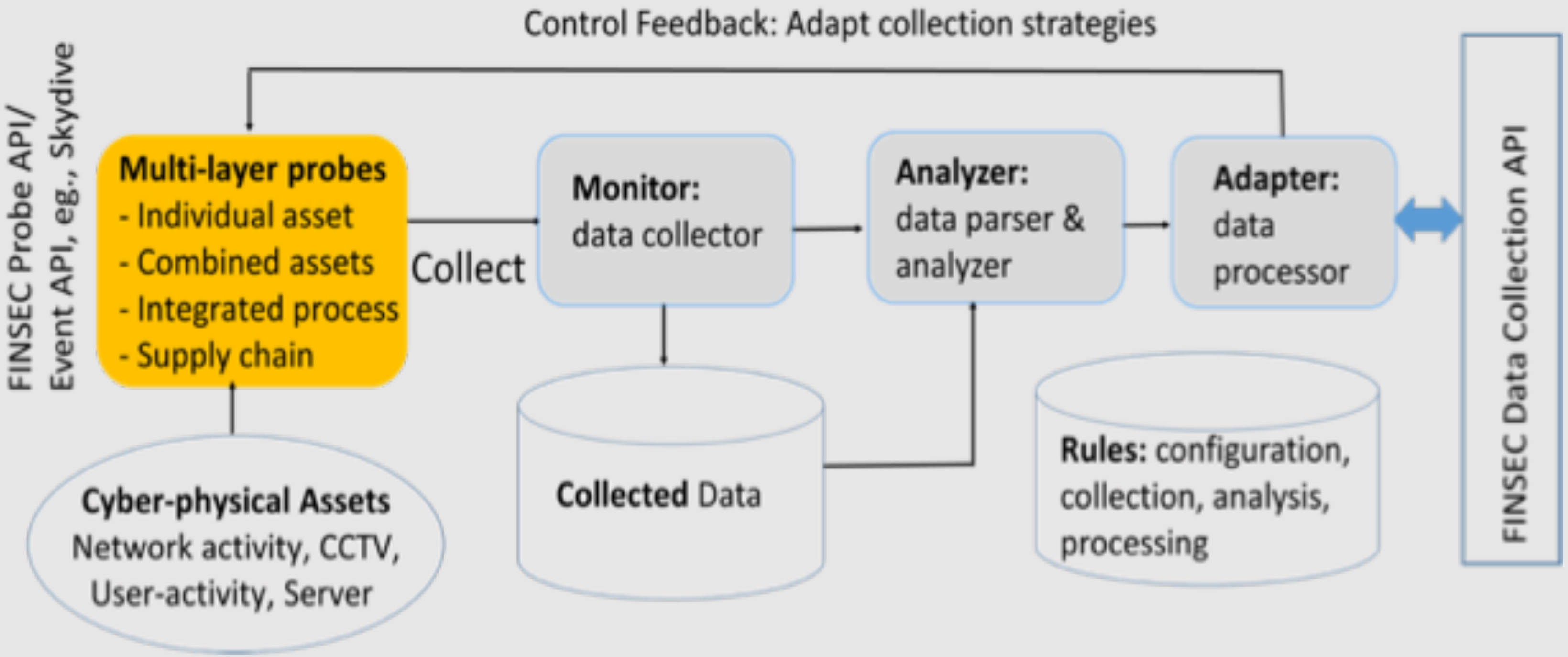
- measure of how well a system protects itself and its data from unauthorized access, and measure of privacy assurance to help users trust the system
- authenticity and integrity of security event data

Adaptive and Intelligent Data Collection in the Financial Sector [1]

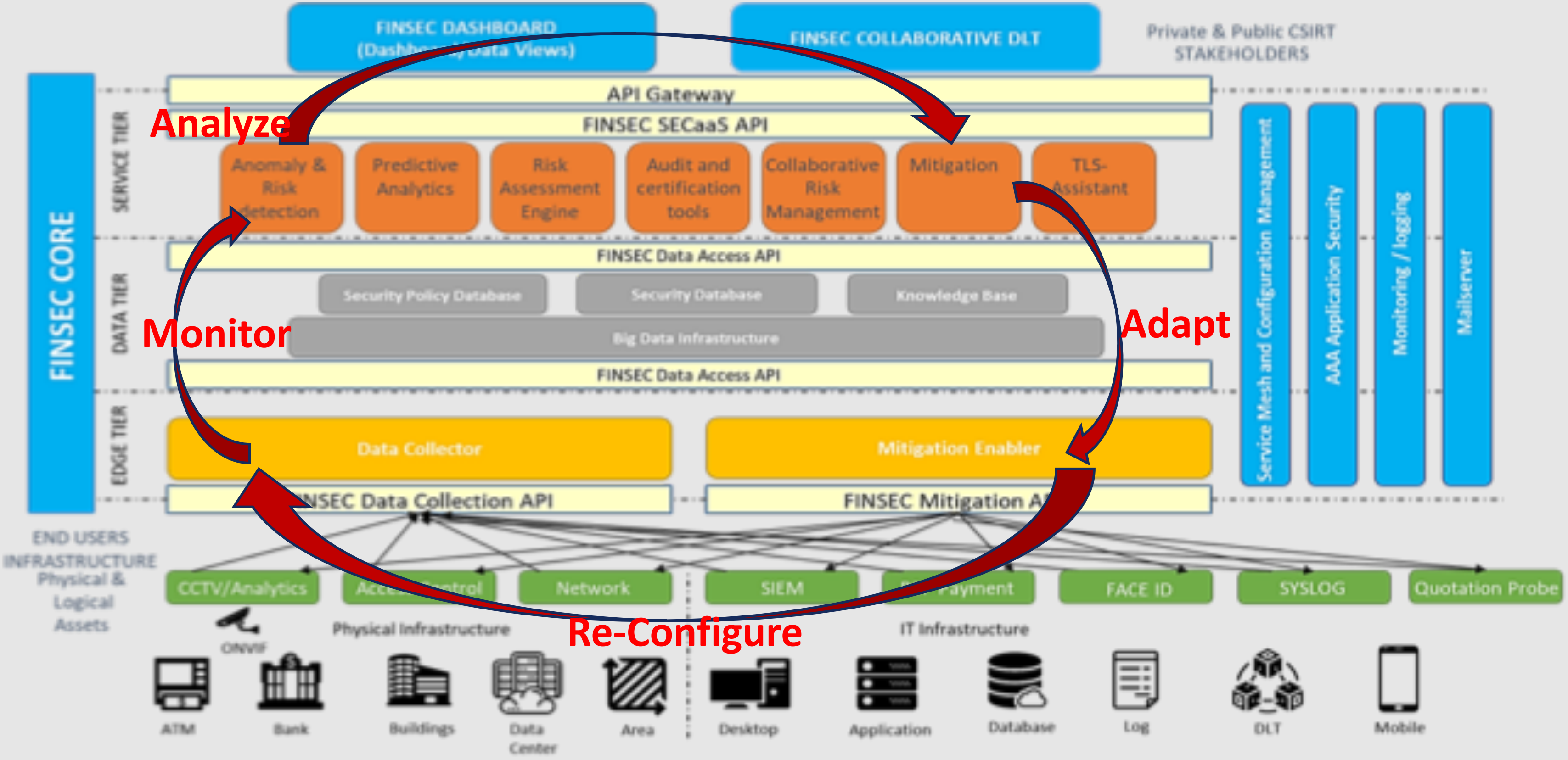
FINSEC Reference Architecture in Brief



FINSEC Adaptive & Intelligent Data Collection



Mapping to the FINSEC Reference Architecture



Security Probes

Security probes capture and assess

- overall security of servers, networks, databases, etc. and generate events when they find problems

The FINSEC probes implemented for data collection and analytics

- CCTV probe
- Access Control probe
- Network Skydive probe
- SIEM probe
- P2P Payment probe
- FaceID probe
- Syslog
- Quotation probe
- App Login

Security Probes: CCTV probe

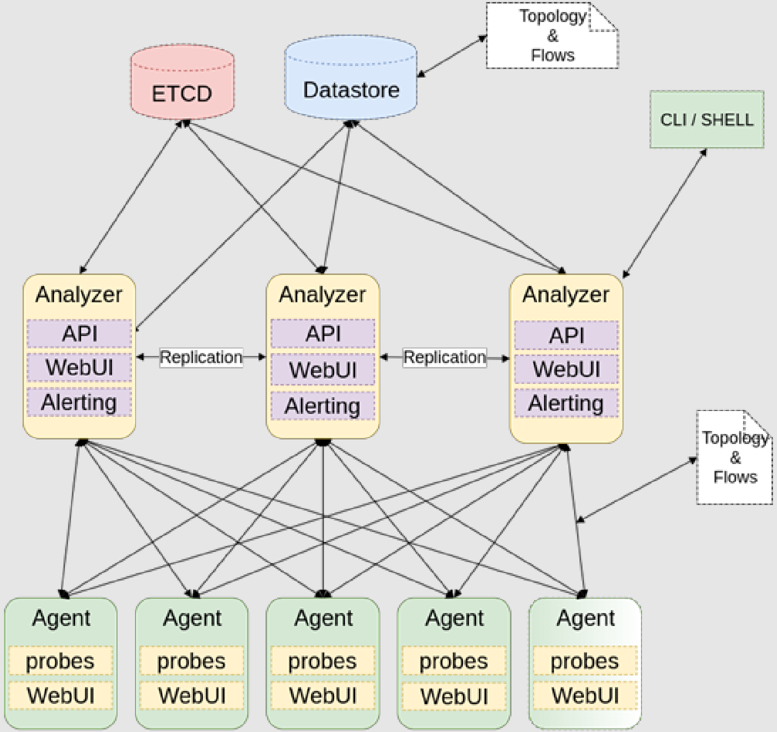
- Monitors CCTV, analyzes movements, and detects physical events that may cause threats
- Analytics service produces events coming from observations of physical interactions by CCTV
- FINSEC ATM Pilot is correlating physical and cyberattacks in ATM networks
  - The goal is to detect and correlate actions that represent a possible targeted attack on the ATM itself and its components, such as taking the whole ATM or exploiting it or breaking the components.

Security Probes: Access Control probe

- Correlates cyber-physical events by
  - checking the access to a secured area by both the use of a badge and a fingerprint and the state change signaled by movement sensors, vibration sensors, gas sensors, and temperature sensors
- Data access events
  - indicate legitimate authentication through HID (Human Interface Device) readers and fingerprint readers

Security Probes: Network Skydive probe

- An open-source real-time network topology and protocols analyzer
- provides real-time insights on network activity which can be used for anomaly detection
- provides agents that act as data collectors, employing efficient mechanisms
  - control the granularity of data collected and collection intrusiveness
  - enable to capture CPU, memory and network overheads
  - allow extra flexibility in capturing network topology and network flow data, as compared to other existing tools



Security Probes: SIEM probe

- SIEMs (Security Information and Event Management) collect information about the monitored IT system by using agents deployed close to the infrastructure elements
- Information is encapsulated in the form of events, stored and correlated to identify anomalous behaviors, discover possible threats, and detect security incidents
- Offers a security administrator
  - a view of the security status and of the activity that is going on in the monitored system.
- In FINSEC, the SIEM probe is based on the XL-SIEM (Cross-Layer SIEM) tool developed by Atos
  - produces alarms by correlating events received from different sources to offer extended information to other components.
- Event sources
  - application logs and sensors such as HIDS (Host Intrusion Detection Systems), NIDS (Network Intrusion Detection Systems), and AntiVirus.

Security Probes: P2P Payment probe

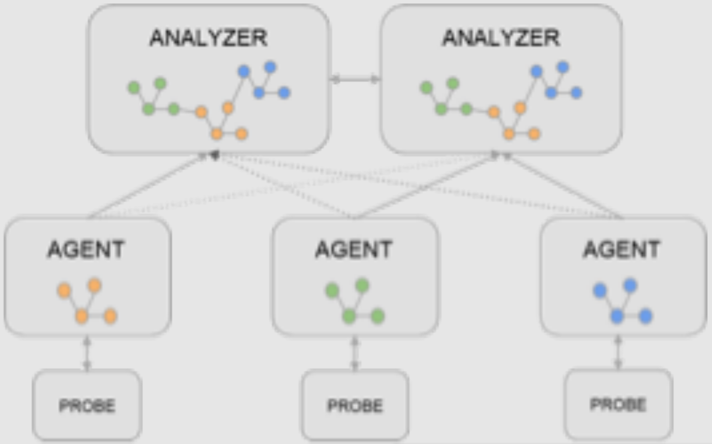
- P2P Payment Probe consists of three modules that contribute features to the FINSEC platform
  - P2P Pay module monitors and collects data of peer-to-peer payments sent on Blockchain infrastructure by end users via their commercial banks
  - Block chain module monitors and collects Blockchain infrastructure parameters useful for anomaly detection on payments sent on Blockchain and Blockchain itself
  - Actuation module provides a web service interface to send specified events and commands to P2P Payment probe.

Adaptive Data Collection Strategies

- Content variation
  - adjust sampling rate to content similarity
- Security threats
  - tuning the rate of data collection based on the security context
- Application driven
  - request start duration, request send duration, request management duration, response send duration, next request start duration
- Anomaly detection
  - more historical data, physical measurement, change of acquisition, outlier-driven rate of acquisition
- Enhanced security risk analysis
  - environmental and risk changes

Skydive probe goals (IBM)

- Topology exploration and visualization
- Network traffic capture
- Make network troubleshooting easier
- SDN agnostic
- Real-time / post-mortem network analysis framework
- Lightweight, easy to deploy



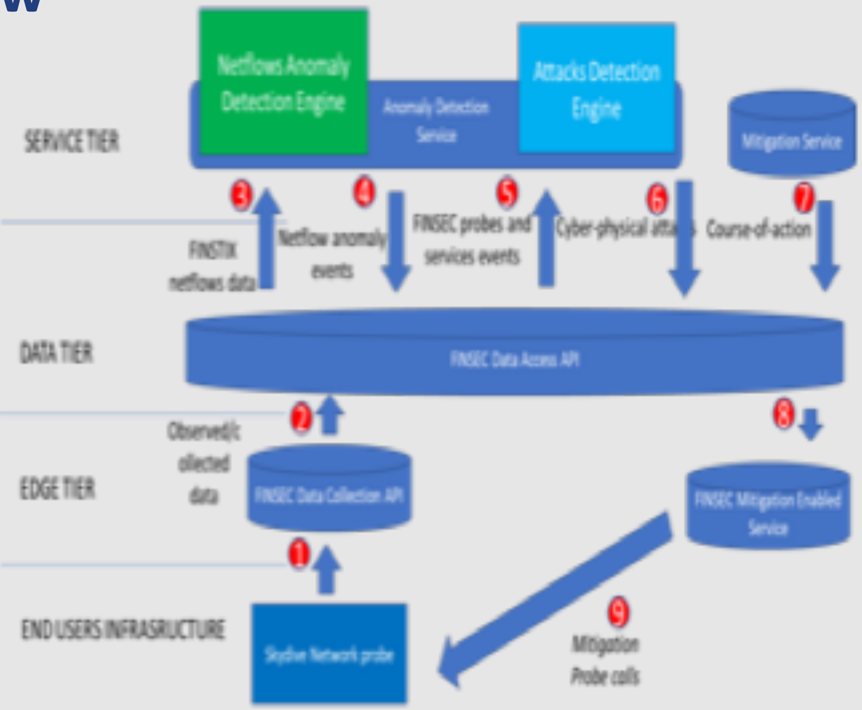
Skydive probe in FINSEC

- Flows classification according to the traffic type (internal, ingress, egress, unknown);
- Flows in FINSTIX format;
- Integration with FINSEC services e.g., Data Collector, Mitigation Enabler
- The Adaptive Data supported by Mitigation Enabler API:
  - Capturing enable/disable: this is supported at the granularity of flow classification
  - Capture sampling: support capturing of a representative sample of the entire volume, sampling is done per each individual classification and is defined in a percentage point (0% to 100%)
  - Capture aggregation level: this feature enable to control the time window used for aggregation of data (typically 30s), a smaller window providing higher resolution at the cost of higher resources (mainly bandwidth)
  - The mitigation controlled by “observation/level-of-detail” policy with 3 predefined modes:
    - normal: 100% sampling for egress and ingress, 30s aggregation time
    - **alert**: 100% sampling for egress and ingress, **10%** sampling for internal, **15s** aggregation time
    - **alarm**: 100% sampling for egress and ingress, **20%** sampling for internal, **10%** sampling of unknown, 15s aggregation time

Adaptive Data Collection Flow

Analytics based on Skydive data

Analytics name	Analytics Description
Suspicious outbound access	Detect unusual outbound access
Suspicious inbound access	Detect unusual inbound access
Data leakage detection	Detect egress services with higher than typical outbound volumes
Reconnaissance/port scan attack detection	Detect services with higher than typical number of connection requests for different IP ports
Insider threat detection	Detect services with higher than typical response volumes



Adaptive Data Collection by Skydive probe as part of Anomaly Detection mitigation chain

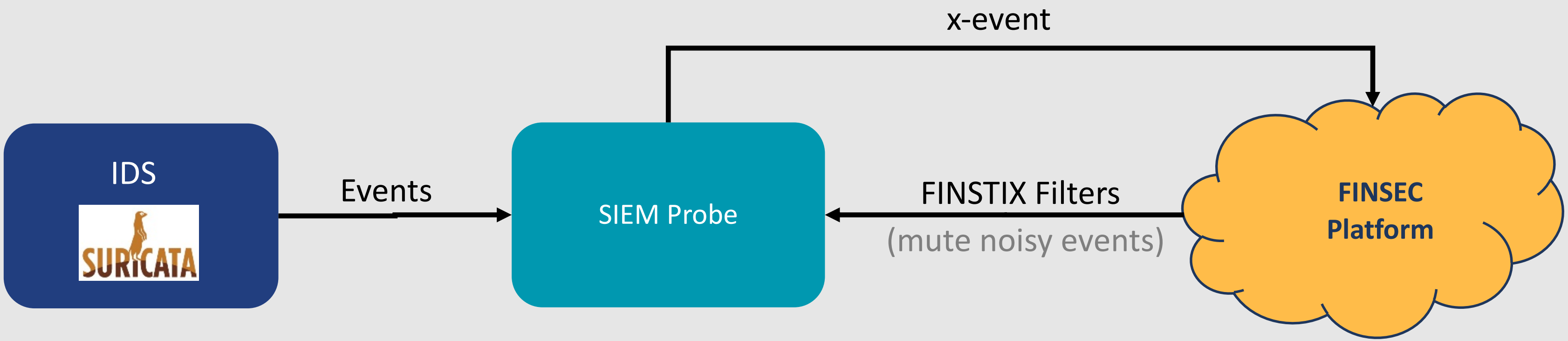
Main steps of the Adaptive Data Collection for Skydive probe as demonstrated in FINSEC Anomaly Detection mitigation chain:

- Step 1: The Netflow data acquired by the Skydive probe and pushed into the Data Collector
- Step 2: The data aggregated and pushes it to the Data Layer
- Steps 3-6: he data analysed by Anomaly Detection Service and the detected Cyber-Physical attacks are reported to the FINSEC Data Layer
- Steps 7-8: The attacks are analysed and the observation policy updates the Skydive probe are selected
- Step 9: The observation policy is applies by Skydive probe and modifies the Netflow data acquisition mode

SIEM Probe – Adaptive and Intelligent Data Collection (Atos)

- **SIEM Probe Reconfiguration – Capability to mute noisy events**:
  - When the same event/alarm is being generated multiple times in a short period
  - SIEM Probe automatically creates a *FINSTIX filter* to skip those events for a given period:
    - Useful when facing repetitive attacks like bruteforce attacks or automatic scans
    - E.g., same attacker IP performing the same attack attempts against the same target
  - Increases the *quality* of reported data by the SIEM Probe to the FINSEC Platform
  - Helps security teams to spot (focus on) other attacks by skipping noisy events

SIEM Probe – Capability to mute noisy events

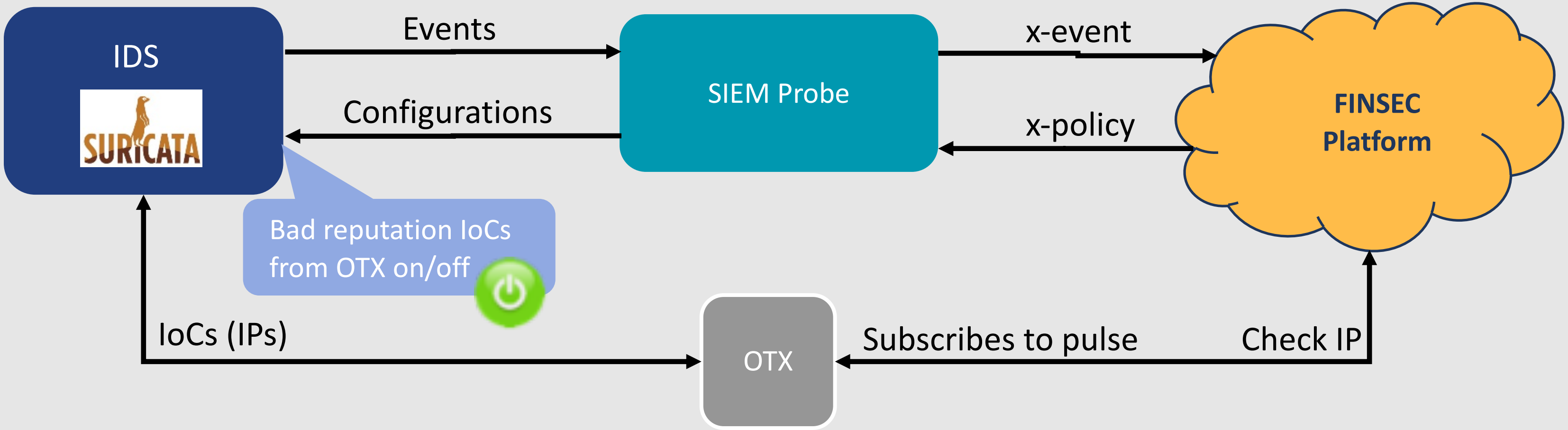


- **Adaptive Data Collection Workflow View**:
  1. Attack is detected in IDS sensor -> x-events are sent to FINSEC Platform
  2. x-events are analyzed: If same x-event detected multiple times, FINSTIX Filter is created and communicated to the SIEM Probe (e.g., mute noisy event for 10 minutes)
  3. SIEM Probe starts muting these x-events (for 10 minutes) improving quality of data and efficiency of the decision making

SIEM Probe – Adaptive and Intelligent Data Collection

- **IDS Sensor Reconfiguration – IoCs extender**:
  - IDS downloads from external Threat Intelligence sources (like OTX) lists of IoCs related to IPs already detected as malicious (e.g. two IPs that belong to the same attack campaign)
  - IDS generates a **bad reputation list** with IoCs downloaded from OTX
  - IDS enables or disables the detection of bad reputation IoCs via *FINSEC standard policy* “observation/level-of-detail”, with two compatible conditions:
    - **Alert**: Enables the generation of events when connections from IPs present in the OTX bad reputation list are detected, even if the IP is not attacking. It works in “heuristic” mode.
    - **Normal**: Disables the generation of events from OTX bad reputation list. Generates events only when attacks or suspicious activity is detected.
  - The “alert” policy can be configured by default or when an attack is detected

SIEM Probe – IDS Sensor Reconfiguration – IoCs extender



- **Adaptive Data Collection Workflow View**:

1. Attack is detected in IDS sensor -> x-events are sent to FINSEC Platform
2. x-events are analyzed: Searches in OTX pulses (IoCs lists) that contains attacker's IPs and subscribes to them
3. IDS updates the IoCs list from OTX pulses where it is subscribed
4. Any related IP that connects to the platform generates new events even if it is not attacking (heuristic mode)

Concluding remarks

Improved quality of collected data

- efficiency and accuracy of methods of attack detection and defense
- tune the rate of the data collection at the various monitoring probes

Improved detection capability

- correlating wide-ranging data sources and using predictive analytics

Increased automation & optimization

- control feedback with adaptive collection
- economizing of resources: bandwidth and storage of security information

AI/DL-based security models for data collection

- adaptability and extendibility with the data drift, continuous discovery of new system threats, and vulnerabilities

References

[1] Habtamu Abie et al. 2020. “Adaptive and Intelligent Data Collection and Analytics for Securing Critical Financial Infrastructure” in Cyber-Physical Threat Intelligence for Critical Infrastructures Security: A Guide to Integrated Cyber-Physical Protection of Modern Critical Infrastructures. Edited by John Soldatos, James Philpot and Gabriele Giunta. pp. 104–142. Now Publishers. DOI: 10.1561/9781680836875.ch7.

[2] L.M. He, Z. Yan, and M. Atiquzzaman, “LTE/LTE-A Network Security Data Collection and Analysis for Security Measurement: A Survey”, IEEE Access, vol. 6, issue 1, pp. 4220–4242, 2018. doi: 10.1109/ACCESS.2018.2792534

[3] L. Cazorla, C. Alcaraz, and J. Lopez (2013). Towards Automatic Critical Infrastructure Protection through Machine Learning. In: Luiijf E., Hartel P. (eds.) Critical Information Infrastructures Security. CRITIS 2013. Lecture Notes in Computer Science, vol. 8328. Springer, Cham.

[4] F. Ullah and M.A. Babar, “An Architecture-Driven Adaptation Approach for Big Data Cyber Security Analytics,” 2019 IEEE International Conference on Software Architecture (ICSA), Hamburg, Germany, 2019, pp. 41–50. doi: 10.1109/ICSA.2019.00013

[5] X.Y. Jing, Z. Yan, andW. Pedrycz, “SecurityData Collection andData Analytics in the Internet: A Survey,” IEEE Communications Surveys and Tutorials, 2018. doi: 10.1109/COMST.2018.2863942 (IF: 20.23)