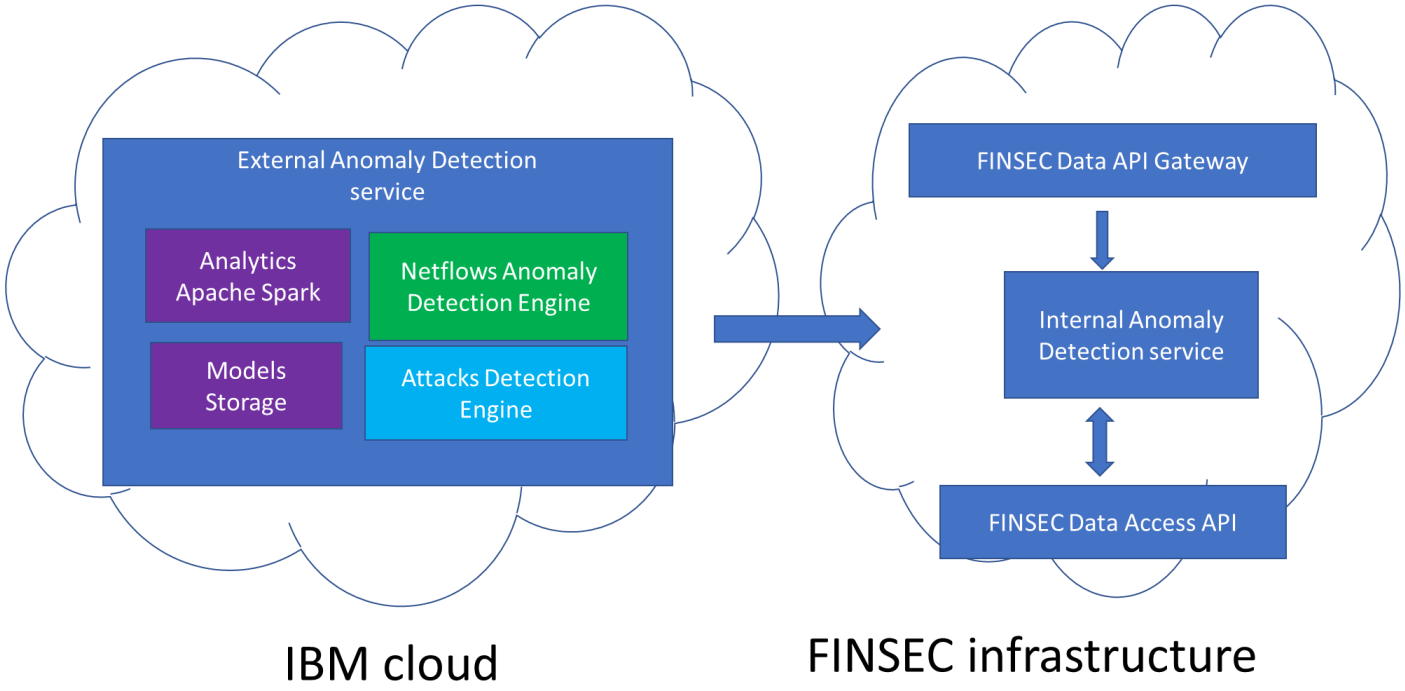
Anomaly Detection and Response in Finance Sector Infrastructures

Omri Soceanu – AI Security Group Manager, IBM Research

Part of this work has been carried out in the scope of the FINSEC project (contract number 786727),
which is co-funded by the European Commission in the scope of its H2020 program. The authors gratefully acknowledge the contributions of the funding agency and of all the project partners.

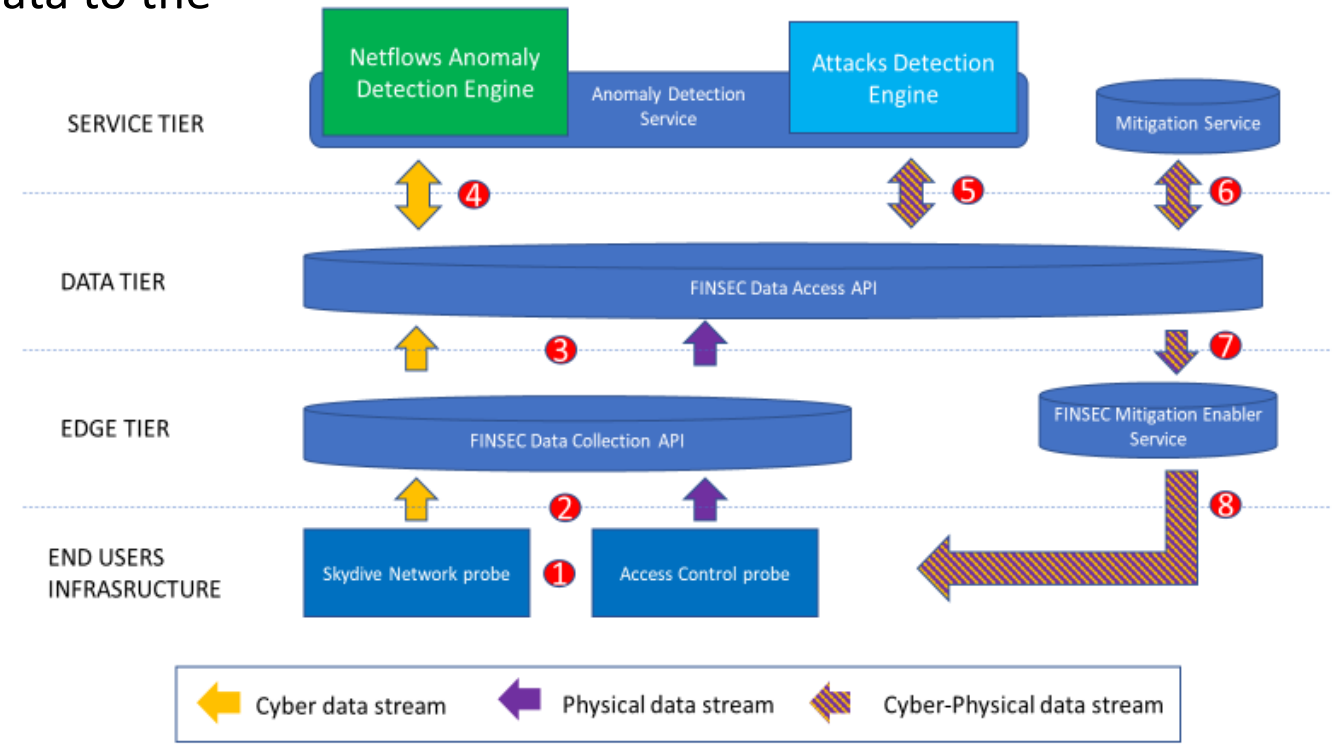
Anomaly Detection and Finance

IBM Anomaly Detection Service



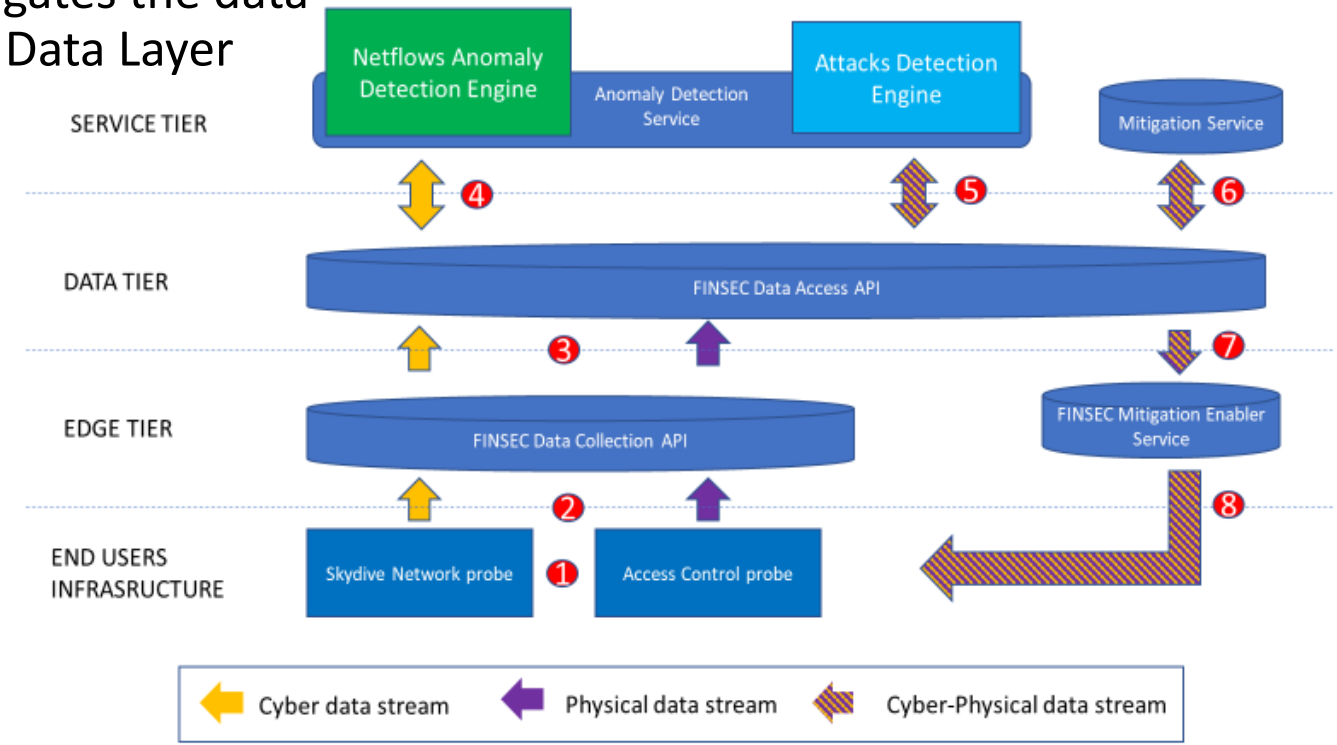
Mitigation flow

1. Probes push the data to the Data Collector



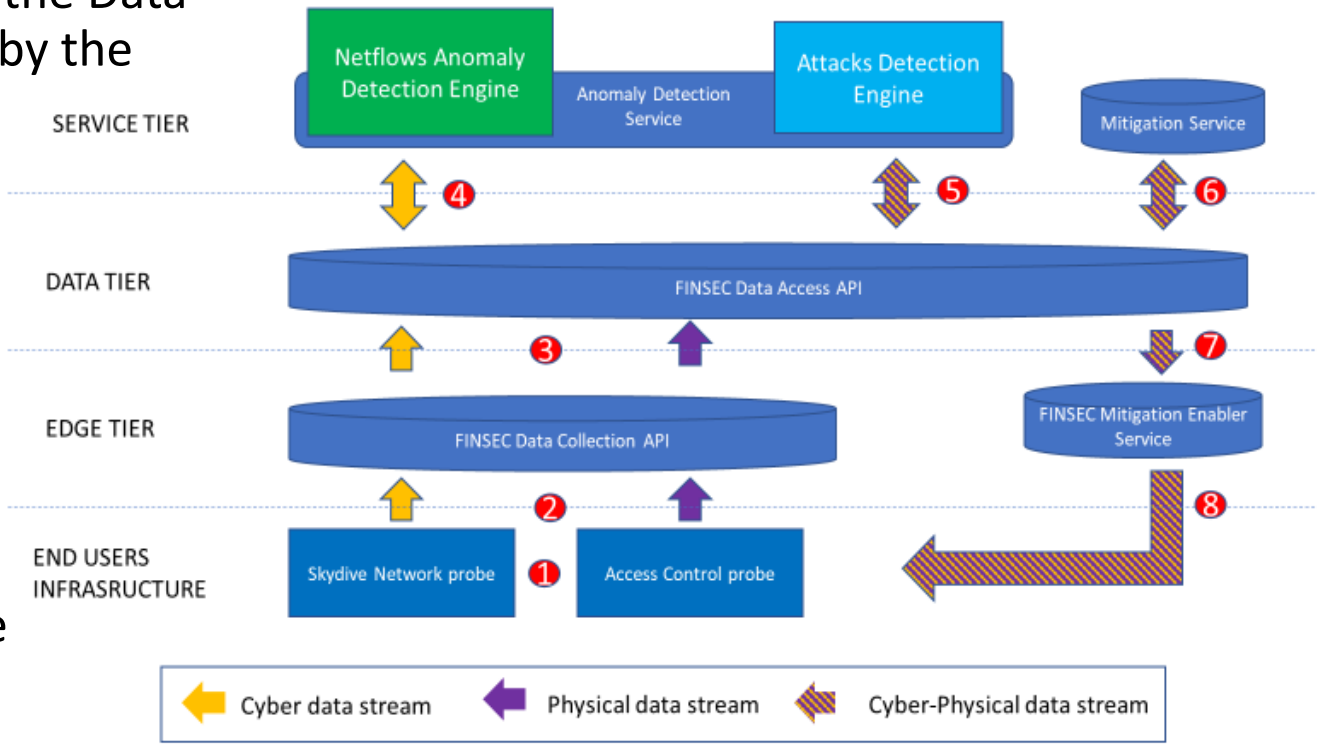
Mitigation flow

2. Data Collector aggregates the data and pushes it to the Data Layer



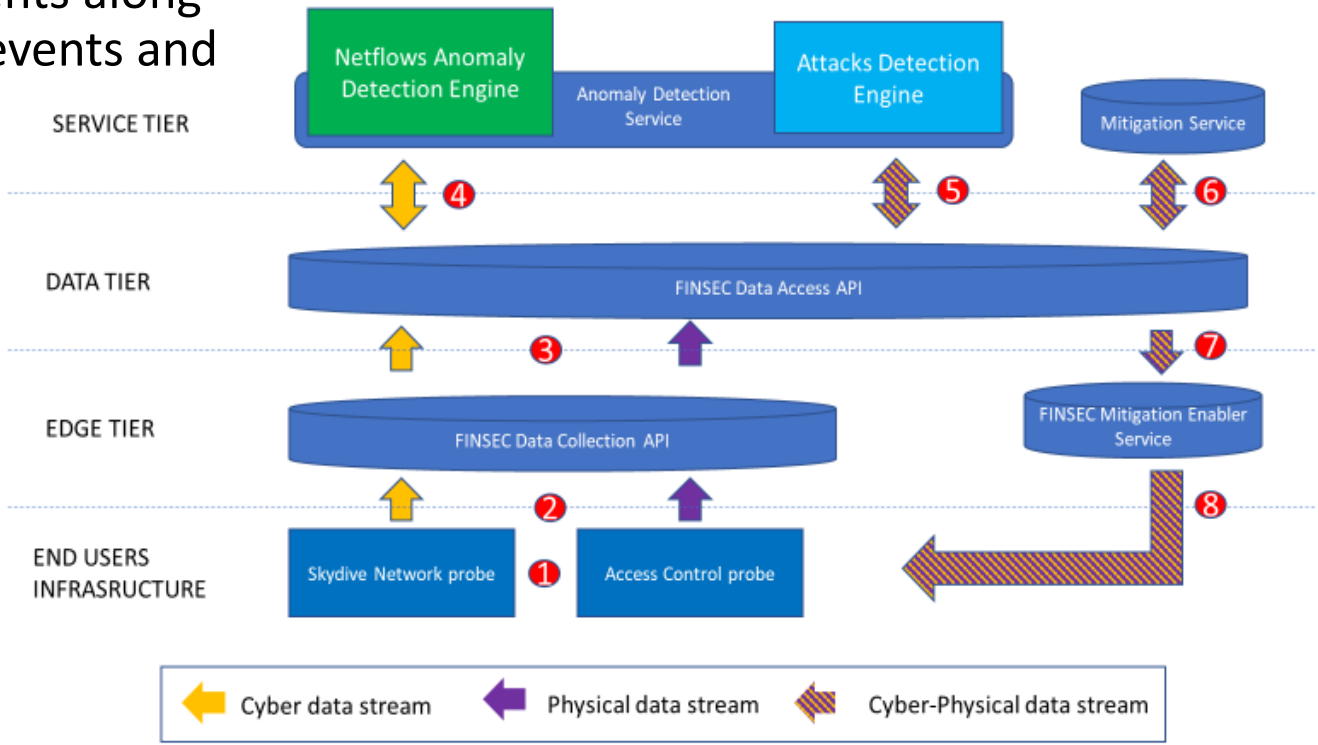
Mitigation flow

3. Netflow data from the Data Layer is processed by the Netflow Anomaly Detection Engine of the Anomaly Detection Service and the Netflow anomaly events detected in the Netflow Anomaly Detection Engine are reported to the Data Layer



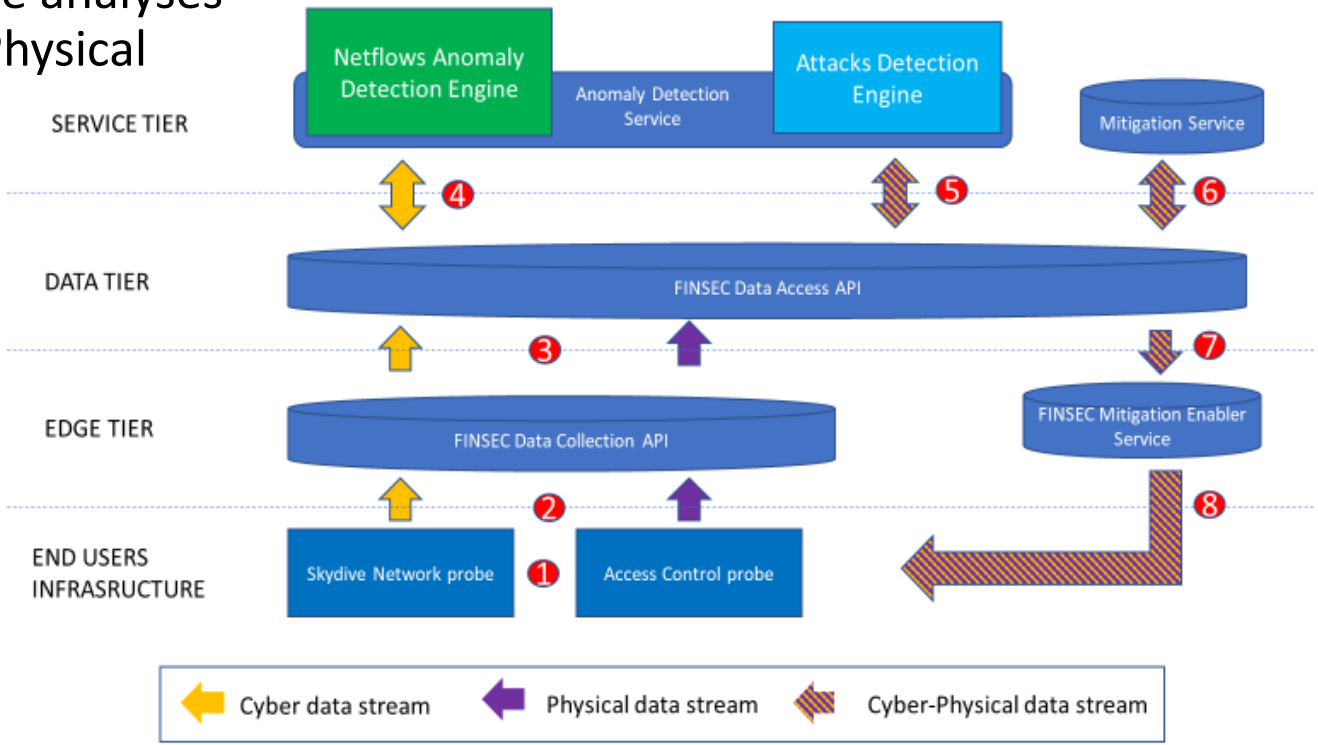
Mitigation flow

4. Netflow anomaly events along with Access Control events and events produced by other services are analyzed by the Attack Detection Engine and the detected Cyber-Physical attacks are reported to the FINSEC Data Layer



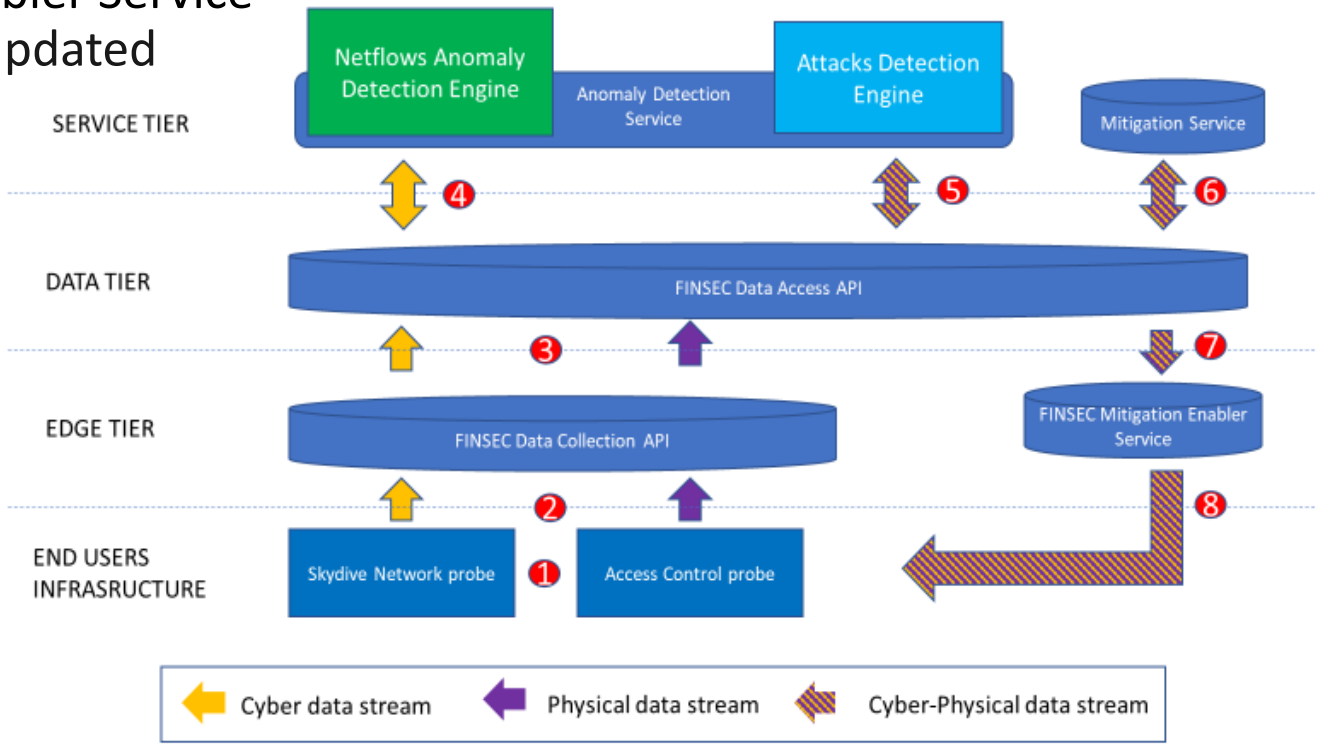
Mitigation flow

5. The Mitigation Service analyses the detected Cyber-Physical attacks and produces the corresponding Course-of-actions



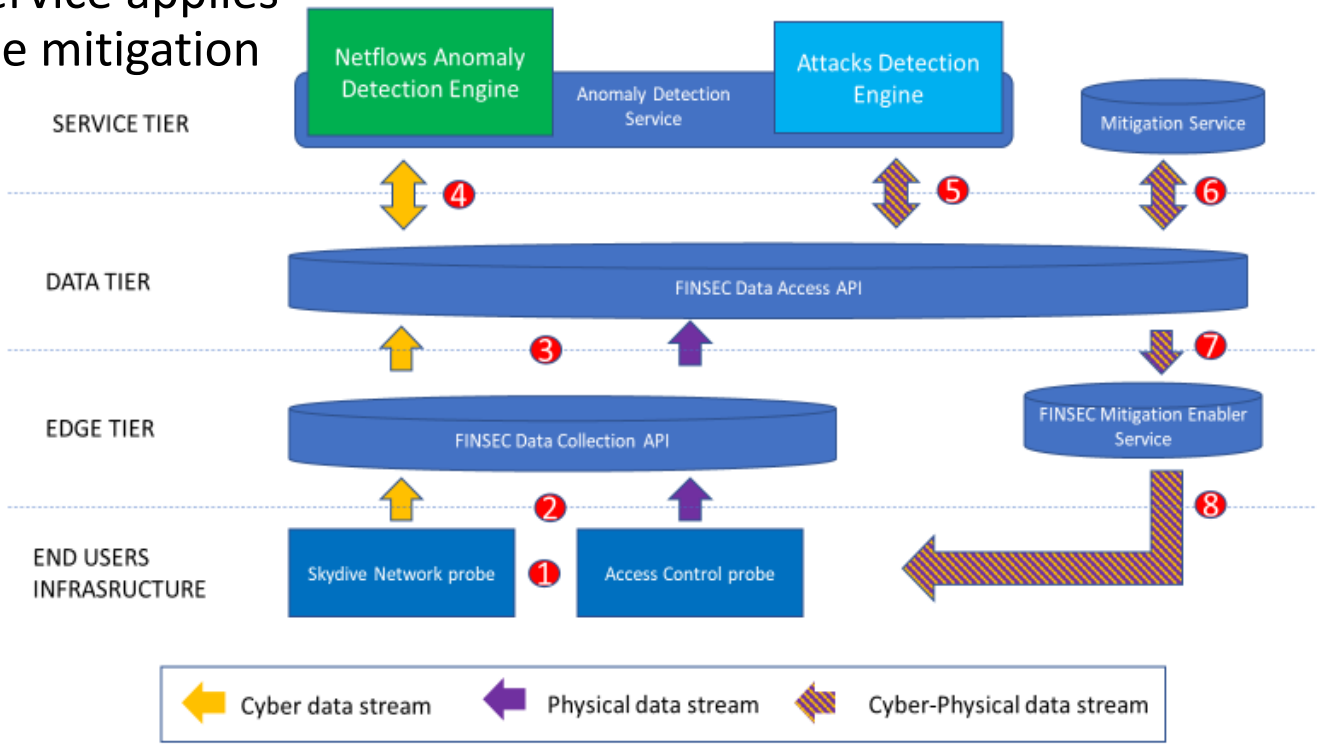
Mitigation flow

6. The Mitigation Enabler Service analyses recently updated Course-of-actions and decides what mitigation action to trigger



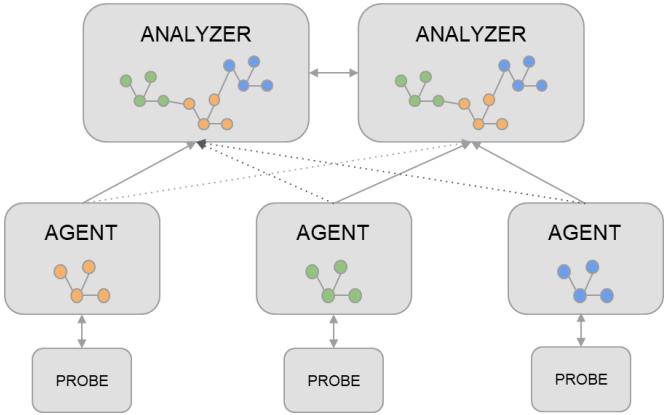
Mitigation flow

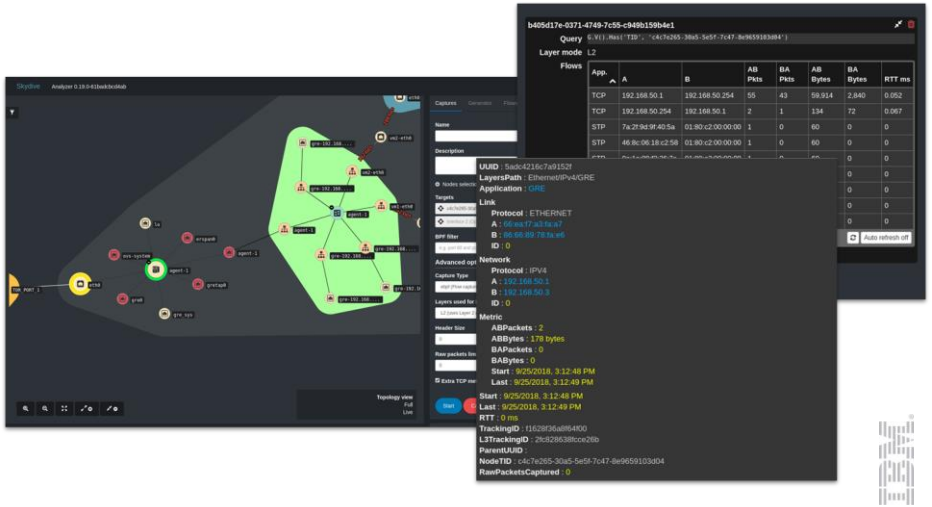
7. Mitigation Enabler Service applies Probe API to apply the mitigation action on the probes



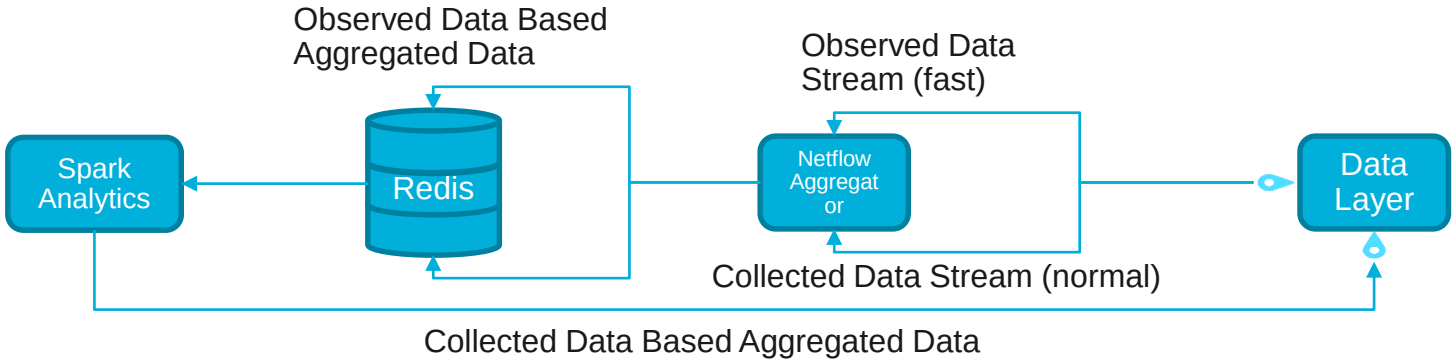
Skydive probe

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





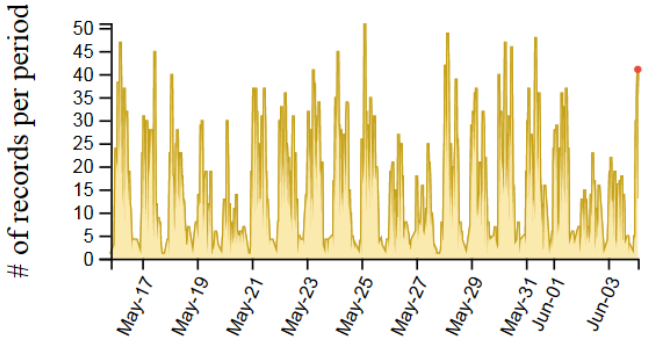
Network Anomaly Detection Engine



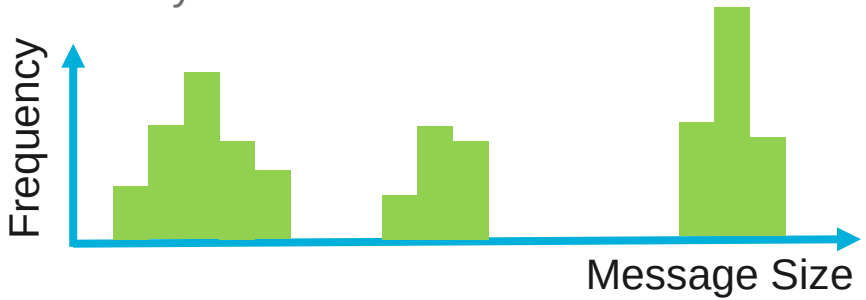
Analytics name	Analytics Description
Suspicious outbound access	Detect unusual outbound access
Suspicious inbound access	Detect unusual inbound access
Data leakage detection	Detect egress services with higher than typical outbound volumes
Reconnaissance/port scan attack detection	Detect services with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

(Meta) Data Insights

- Multi-resolution temporal patterns



- Limited message size variability



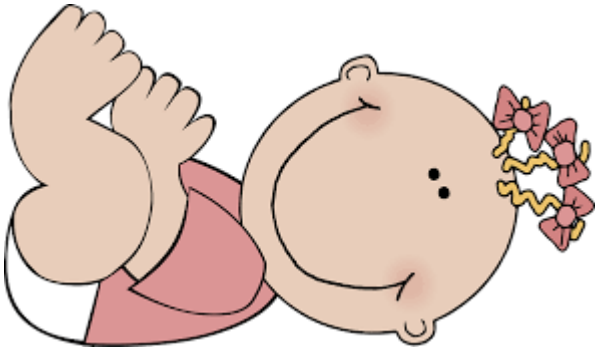
(Meta) Data Insights

- More than security

Conclusions

- Successful use in FINSEC pilots

- Using only meta-data we were able to detect:
  - Security anomalies
  - Malfunctions
- Developed a scalable solution
- Provide a useful security solution



Thank you