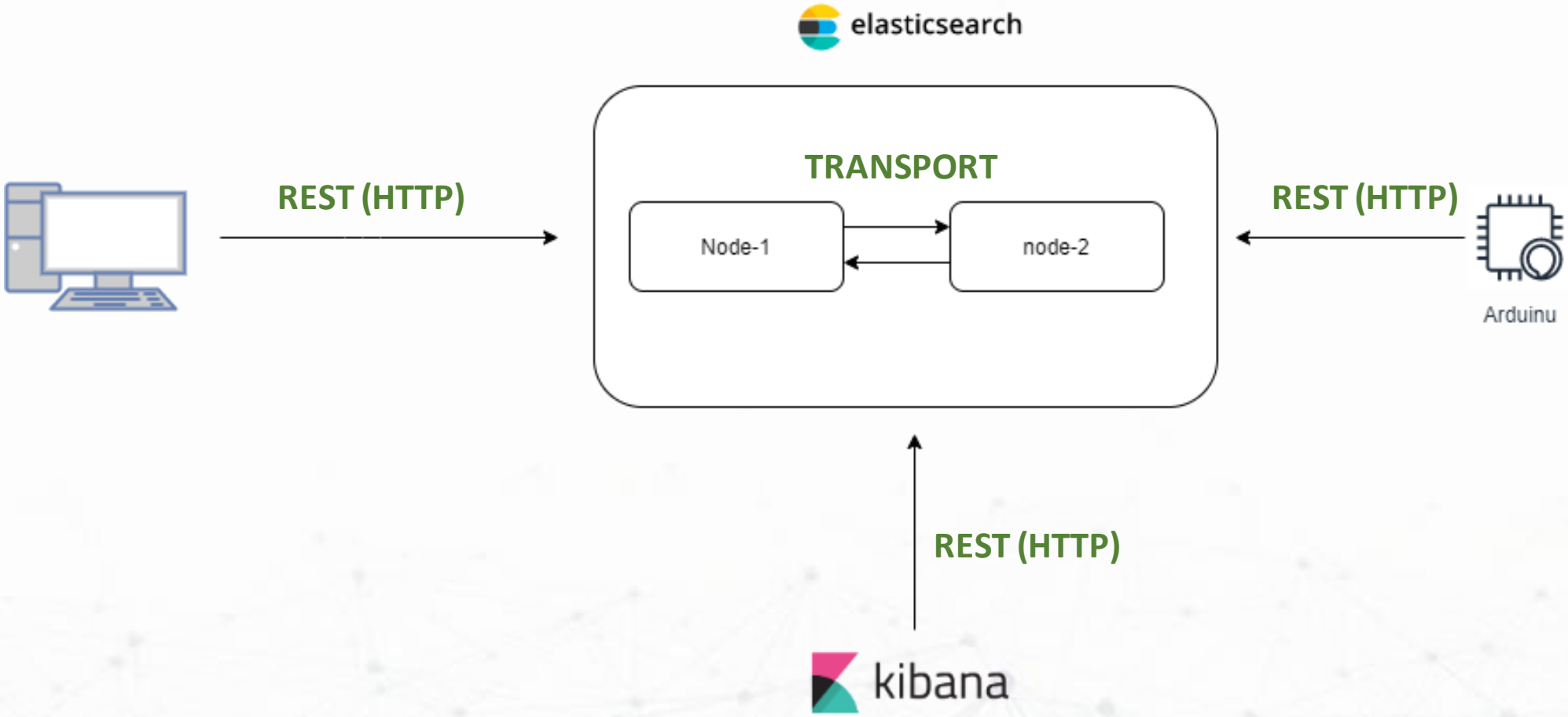
Data storage, sharing & security.
-Audit & Monitoring-

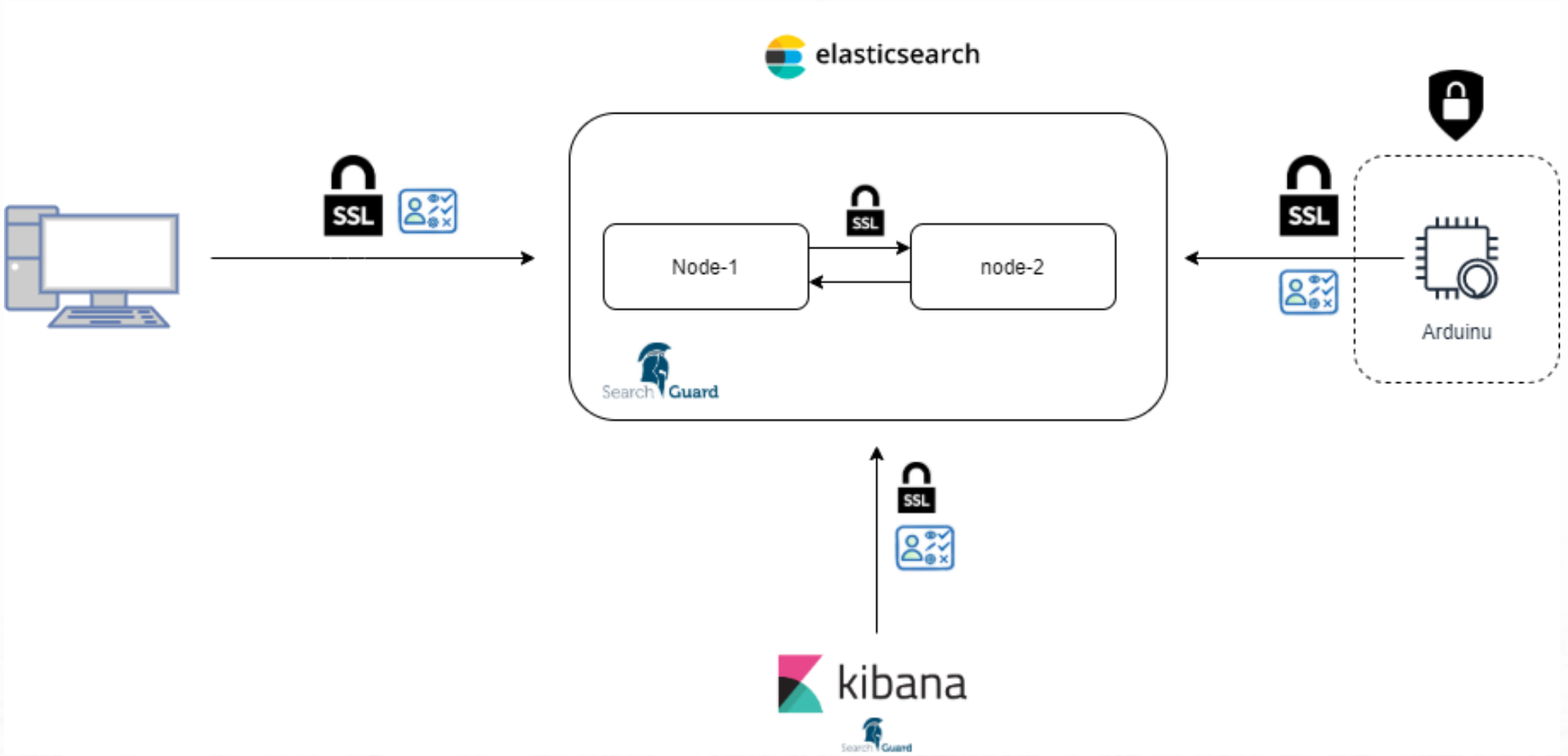
ESME – INGE1 INTERNATIONAL TRACK

zakaria@elbazi.co

Elasticsearch in our use case:



Elasticsearch in our use case (Security):



ESME sudria

Elasticsearch in our use case (Security):

- Make the IoT devices inaccessible publicly or in an exposed network.
- Securing access to the Elasticsearch index (REST & transport):
  - Securing the communications between the user and the cluster
  - Securing inter-node communications (multi-nodes cluster)
  - Implementing **Role & permissions-based access control** to the cluster and the dashboards in Kibana.

Elasticsearch in our use case (Monitoring):

- **How are we going to know that everything works fine ?**
  - **State of IoT devices**
  - **State of the DB**
  - **I/O to the db (data is being received and stored as expected)**
  - **Access to the data base (Anomalies, unauthorized accesses,etc)**
  - **etc.**

ESME sudria

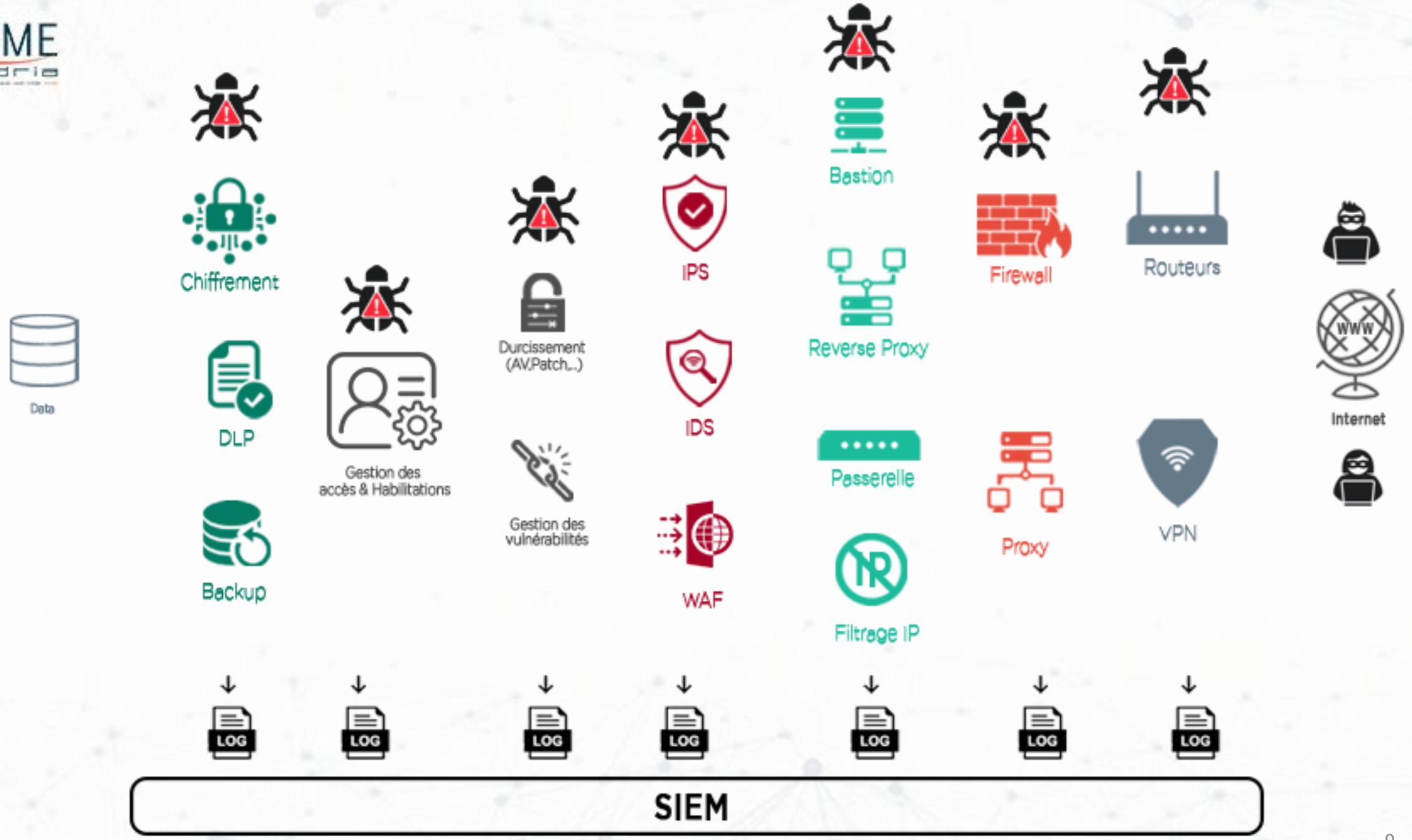
Elasticsearch in our use case (Monitoring):

- We need to **Monitor** our architecture.
- Monitor simply means get the logs from the different components and read/analyze them to detect usual & unusual behaviors.
- Eventually trigger specific action (alerts) in case of anomalies.
  - Continually reporting the state of the IoT objects.
  - Continually reporting the state of the storage (elasticsearch cluster)
  - Monitor access to the cluster (audit logging & read/write queries) for any anomalies

Elasticsearch in our use case (Monitoring):

- Create specific elasticsearch indices for monitoring the IoT devices and for audit logging.
- Add a module for alerting (send alerts and execute actions when anomalies are detected),etc

typical information system security policy :


Data
Chiffrement
DLP
Backup
Gestion des accès & Habilitations
Durcissement (AV,Patch...)
Gestion des vulnérabilités
IPS
IDS
WAF
Bastion
Reverse Proxy
Passerelle
Filtrage IP
Firewall
Proxy
Routeurs
VPN
Internet
LOG
SIEM

typical information system security policy :

- **Multi-layer security (VPNs, Firewalls, Intrusion detection and prevention, security rules, backups, data loss preventions,etc)**
- **Every layer generates logs that are sent to central analyzer (SIEM : security information management system).**
- **SIEMs analyze the different log events for anomalies and suspicious activity.**
- **Elasticsearch is one of the popular tools used in SIEMs thanks to it's capabilities in log search, and real time analysis.**

Elasticsearch in our use case (Security):