**ISO/OSI Model versus TCP/IP Model.**

A picture containing text, screenshot, font

Description automatically generated

|  |  |
| --- | --- |
| OSI Model |  |
| Application layer |  |
| Presentation |  |
| Session |  |
| Transport |  |
| Network |  |
| DataLink |  |
| Physical |  |
| TCP/IP Model |  |
| Internet |  |
| Network access |  |

**Data flow between layers**A picture containing text, screenshot, font, printing

Description automatically generated

|  |  |
| --- | --- |
| Data fed into application layer of sender |  |
| Encapsulation |  |
| Header attaches to data |  |
| Presentation |  |
| Session |  |
| Transport |  |
| Network |  |
| Data link and trailer |  |
| Physical |  |
| Representation |  |
| As itself |  |
| Segments |  |
| Packets |  |
| Frames |  |
| Bits |  |
| Receiver |  |
| Received into of receiver |  |
| Decapsulation |  |
| Detaches |  |
| Flows downwards |  |
| In the form of 0 and 1 |  |
| upwards |  |

**TCP three-way handshake**A picture containing text, screenshot, font, number

Description automatically generated

|  |  |
| --- | --- |
| Client |  |
| SYN |  |
| Synchronize Sequence Number |  |
| And ACK |  |
| Acknowledgement of received message and sequence number to start next segment |  |
| From server |  |

**Zenmap GUI which scans the IP**

A screenshot of a computer

Description automatically generated with medium confidence

**FSteps of Nessus vulnerability scanning**A picture containing text, screenshot, font, purple

Description automatically generated

|  |  |
| --- | --- |
| Define the scan parameters, e.g., ports to be scanned, plugins to be enabled |  |
| Perform host discovery using protocols like TCP,UDP,ICMP to identify hosts |  |
| Port scan based on the available |  |
| Conduct service detection to identify the service behind each port |  |
| Detect the operating system |  |
| Run each host against a database of known vulverabilities |  |

A diagram of metasplolit commands

Description automatically generated with low confidence**Commands of Metasploit**

|  |  |
| --- | --- |
| Show targets |  |
| Advanced |  |
| Nops |  |
| Evasion |  |
| Options |  |
| Payload |  |
| Examples of Metasploit commands |  |

**Risk assessment within the risk management process**

A diagram of a risk management process

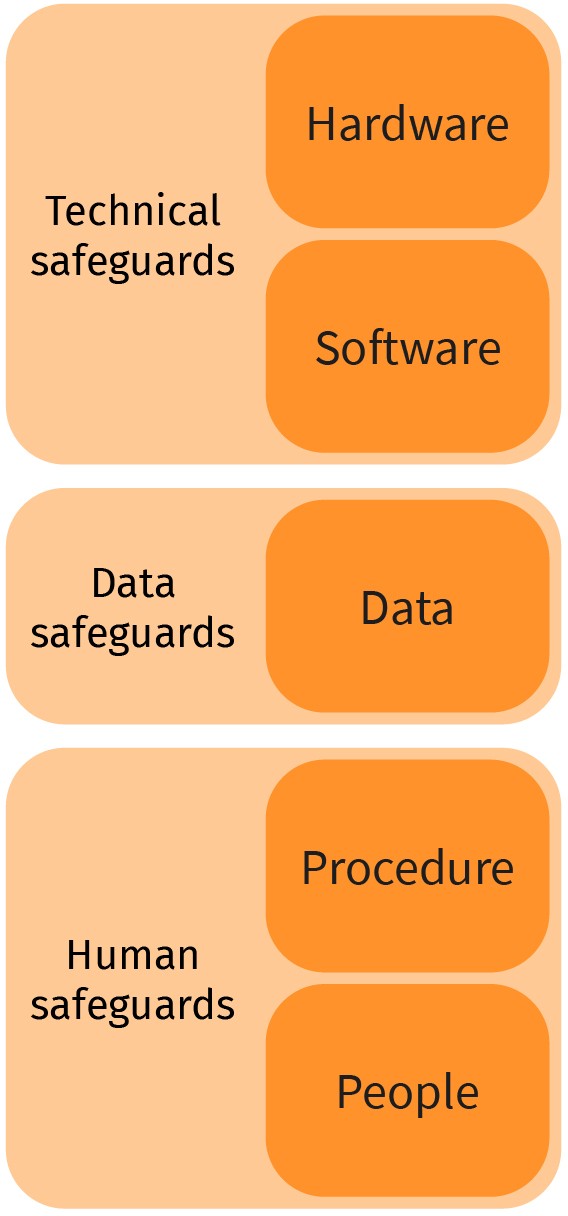
Description automatically generated with low confidence

|  |  |
| --- | --- |
| Access the risk |  |
| Identifies the threats and assesses the risk in the organization |  |
| Information and |  |

**Inherent risk and Residual Risk.**A picture containing diagram, design

Description automatically generated

|  |  |
| --- | --- |
| Inherent risks |  |
| Applying controls |  |
| Residual |  |

**Five components of Information system and related safeguards**

|  |  |
| --- | --- |
| Technical safeguards |  |
| Hardware |  |
| Software |  |
| Data |  |
| Human |  |
| Procedure |  |
| People |  |

**Security Evaluation Roles**

A picture containing text, screenshot, diagram, font

Description automatically generated

|  |  |
| --- | --- |
| TOE: Target of evaluation |  |
| Instance |  |
| Certification |  |

**IDS Classification**

A picture containing text, screenshot, font, design

Description automatically generated

|  |  |
| --- | --- |
| Considers patterns to detect intrusion |  |
| Signature-based IDS/Rule-based |  |
| Classification on approach |  |
| Anomaly-based Behavior-based |  |
| Considers as intrusion |  |
| Detection Systems |  |
| Host-based IDS |  |
| Places sensors in network |  |
| Based |  |
| Data sources |  |
| Hybrid |  |
| Host |  |

**Working of Signature-based IDS**

A picture containing diagram, text, screenshot, line

Description automatically generated

|  |  |
| --- | --- |
| Incoming packets |  |
| Signature database |  |
| Matching |  |
| Yes |  |
| Alert |  |
| System admin |  |
| no |  |

**Working of Anomaly-based IDS**

A picture containing text, screenshot, font, diagram

Description automatically generated

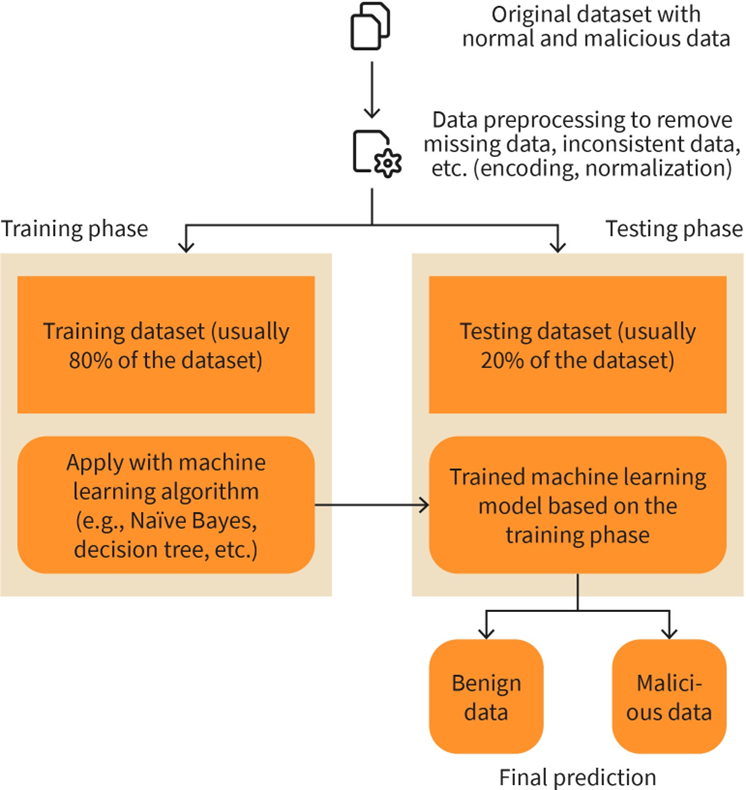
|  |  |
| --- | --- |
| Incoming packets |  |
| Anomaly |  |
| Detection |  |
| By comparing |  |
| Profiled behaviour |  |
| Real packets |  |
| Profiling |  |
| Anomaly detected |  |
| Alert |  |
| System admin |  |

A picture containing text, screenshot, diagram, line

Description automatically generated**NIDS and HIDS**

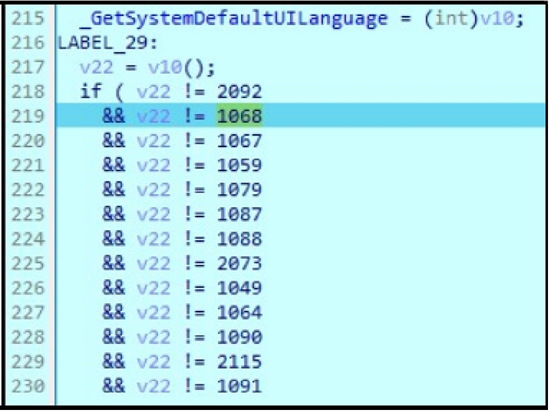
|  |  |
| --- | --- |
| Internet |  |
| Firewall |  |
| Network-based IDS |  |
| Printer Host-based |  |
| PC |  |
| Mobile |  |

**Machine Learning for IDS**

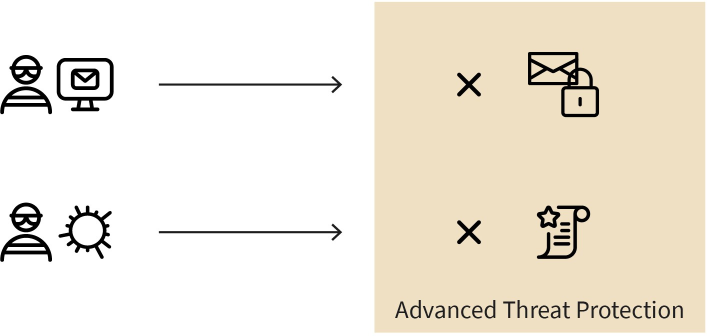


|  |  |
| --- | --- |
| Original dataset with normal and mailicious data |  |
| Preprocessing to remove missing, inconsistent, etc. (encoding, normalization) |  |
| Training phase |  |
| Usually of the dataset |  |
| Apply with machine learning algorithm (e-g, Naïve Bayes, decision tree) |  |
| Testing |  |
| Trained model based on the |  |
| Benign |  |
| Malicious |  |
| Final prediction |  |

**Language Check IoC of LockBit 2.0 Ransomware**

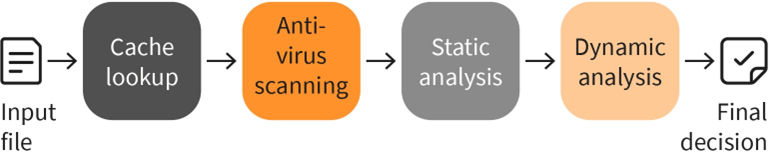
****

**Advanced Threat Protection**



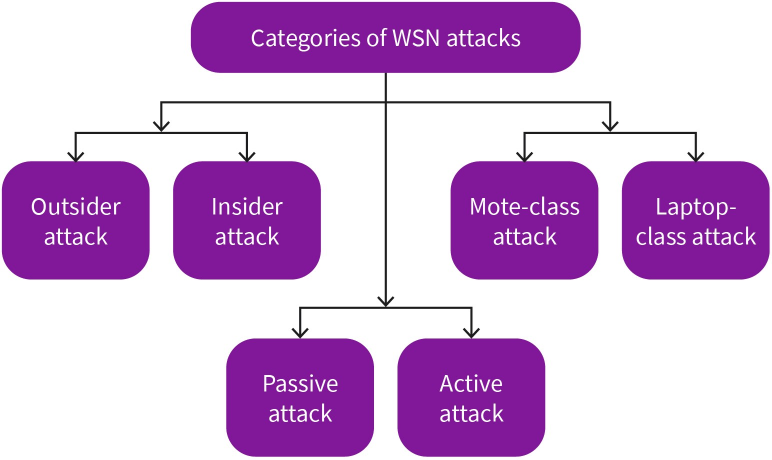
|  |  |
| --- | --- |
| Advanced Threat Protection |  |

**Example of Advanced Threat Protection**



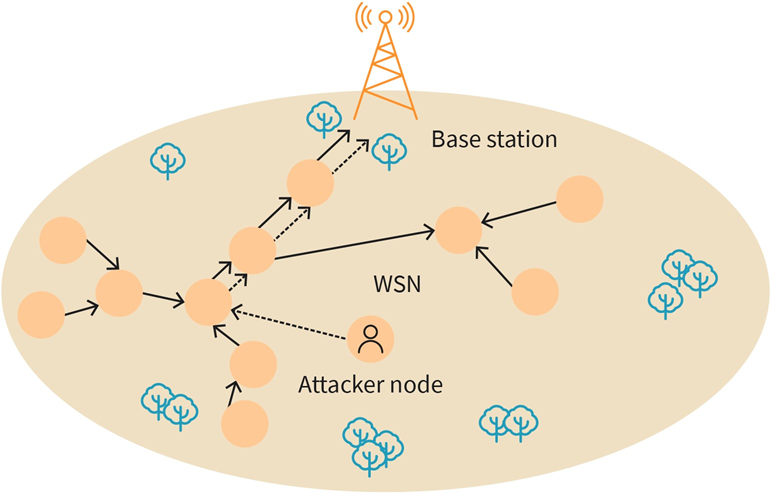
|  |  |
| --- | --- |
| Input file |  |
| Cache lookup |  |
| Anti-virus scanning |  |
| Static analysis |  |
| Dynamic |  |
| Final decision |  |

**Categories of WSN attacks**

****

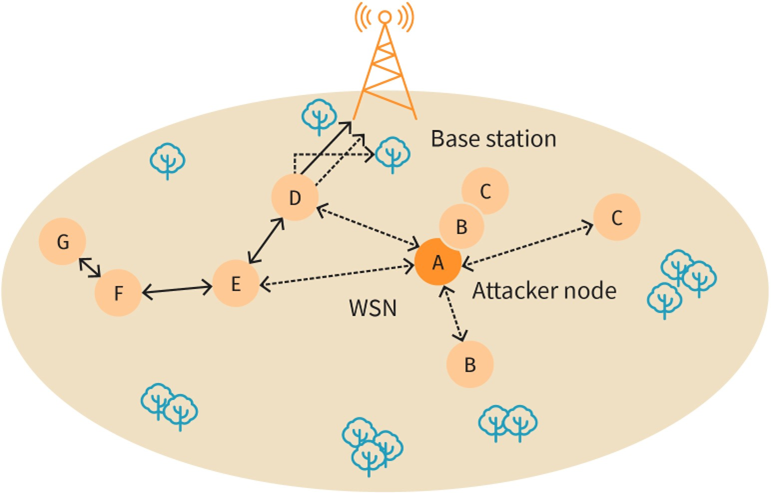
|  |  |
| --- | --- |
| Categories of WSN attacks |  |
| Outsider |  |
| Insider |  |
| Mote-class attack |  |
| Laptop-class |  |
| Passive |  |
| Active |  |

**Path-based DoS in WSNs**

****

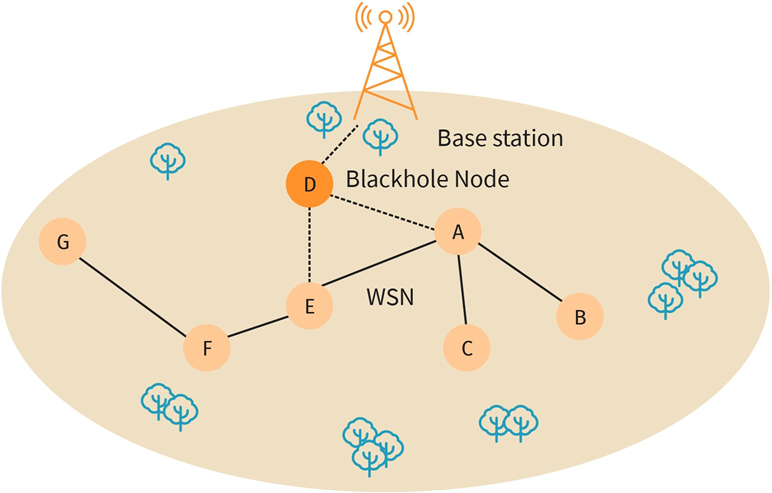
|  |  |
| --- | --- |
| Based station |  |
| WSN |  |
| Attacker node |  |

**Sybil attack in WSNs**

****

|  |  |
| --- | --- |
| Base station |  |
| WSN |  |
| Attacker node |  |

**Blackhole attack in WSNs**

****

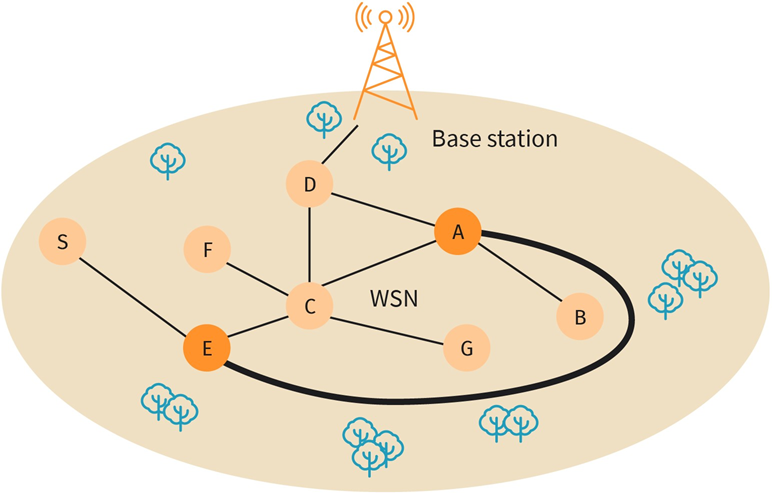
|  |  |
| --- | --- |
| Base station |  |
| Blackhole Node |  |
| WSN |  |

**Node replication attack in WSNsA diagram of a base station

Description automatically generated with medium confidence**

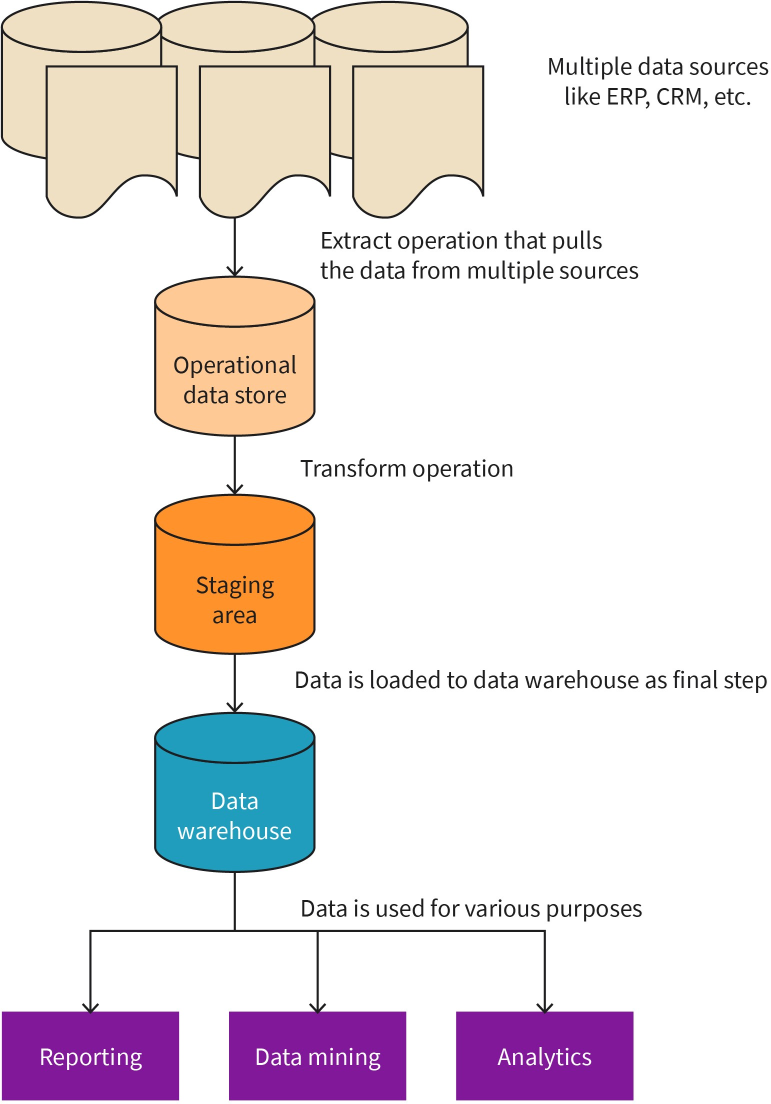
|  |  |
| --- | --- |
| Base station |  |
| WSN |  |

**Wormhole attack in WSNs**

****

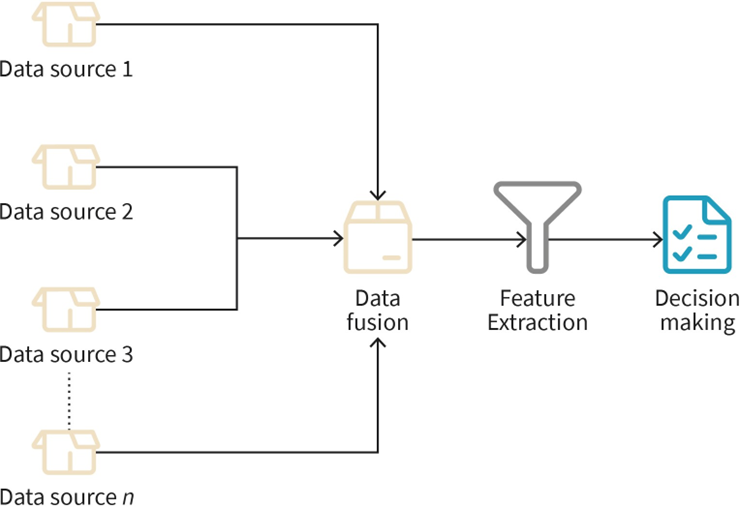
|  |  |
| --- | --- |
| Base station |  |
| WSN |  |

**Working of ODS**

****

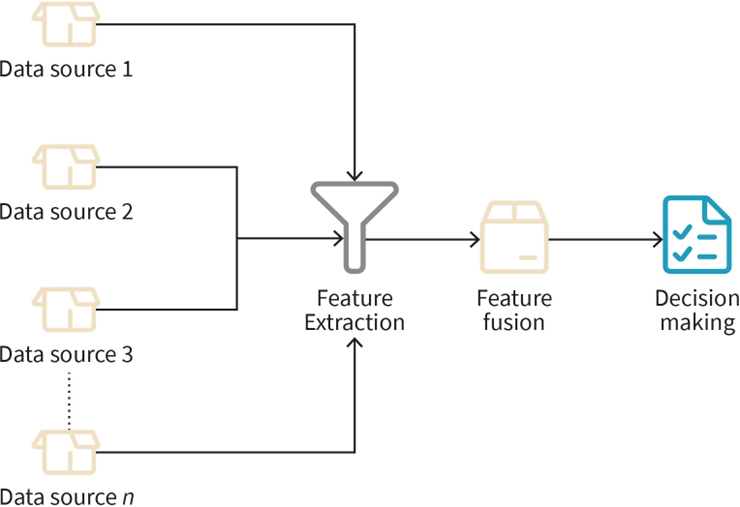
|  |  |
| --- | --- |
| Operational store |  |
| Staging area |  |
| Warehouse |  |
| Reporting |  |
| Mining |  |
| Analytics |  |
| Multiple data sources like ERP, CRM, etc. |  |
| Extract operation that pulls the data from multiple |  |
| Transfer operation |  |
| Is loaded to data warehouse as final step |  |
| Is used for various purposes |  |

**Low-level Data fusion**

****

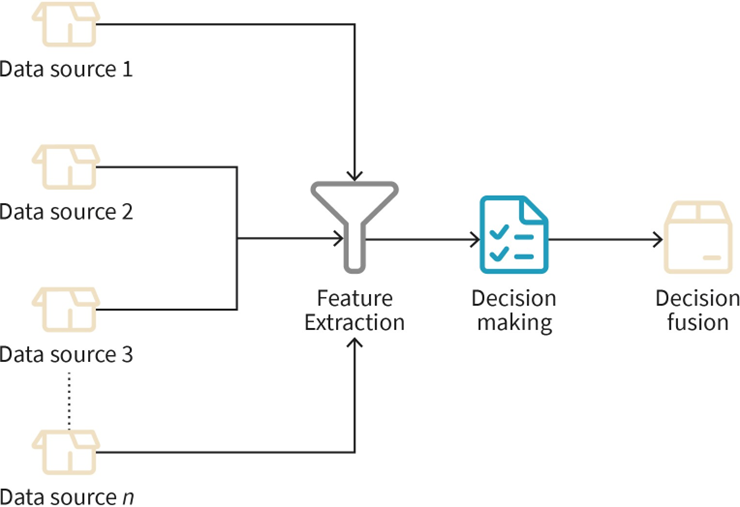
|  |  |
| --- | --- |
| Data source |  |
| Fusion |  |
| Feature Extraction |  |
| Decision making |  |

**Medium-level Data fusion**

****

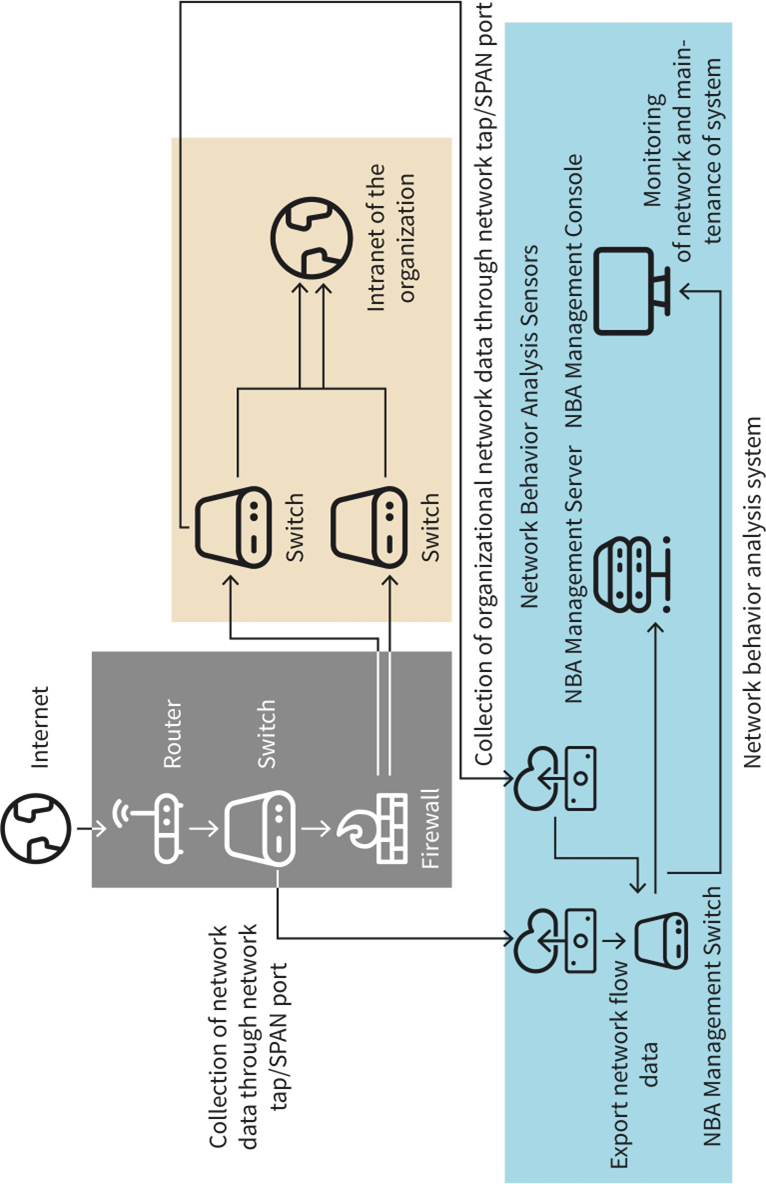
|  |  |
| --- | --- |
| Data |  |
| Feature Extraction |  |
| Fusion |  |
| Decision making |  |

**High-level Data fusion**

****

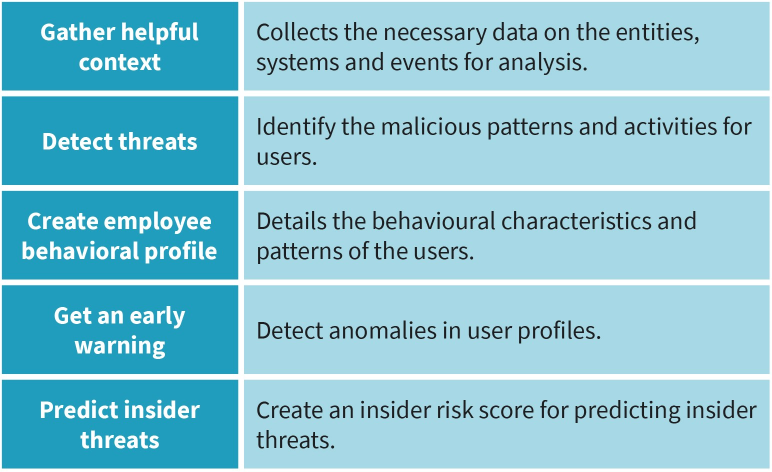
|  |  |
| --- | --- |
| Data |  |
| Feature Extraction |  |
| Decision making |  |
| fusion |  |

**Network Behaviour analysis model architecture**

****

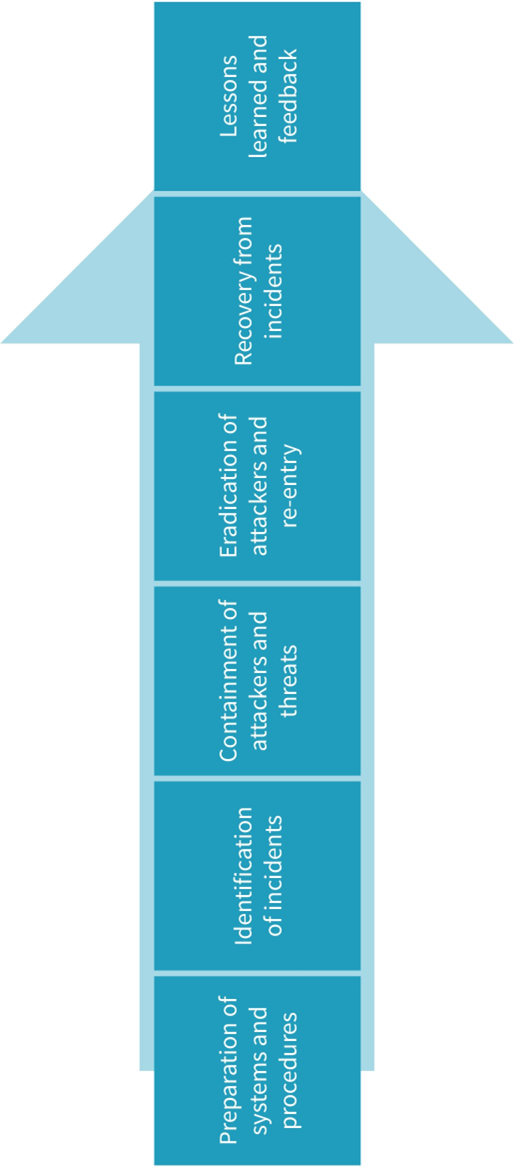
|  |  |
| --- | --- |
| Collection of network data trough tap/SPAN port |  |
| Internet |  |
| Router |  |
| Switch |  |
| Firewall |  |
| Intranet of the organization |  |
| Export flow |  |
| NBA Management |  |
| Behavior Analysis Sensors |  |
| Server |  |
| Console |  |
| Monitoring and maintenance of system |  |

**Five levels of UEBA**

****

|  |  |
| --- | --- |
| Gather helpful context |  |
| Detect threats |  |
| Create employee behavioral profile |  |
| Get an early warning |  |
| Predict insider |  |
| Collects the necessary on the entities, systems and events for analysis. |  |
| Identify the malicious patterns and activities for users. |  |
| Details the behavioural characteristics and of the |  |
| anomalies in profiles. |  |
| an insider risk score for predicting |  |

**Phases of incident response**

****

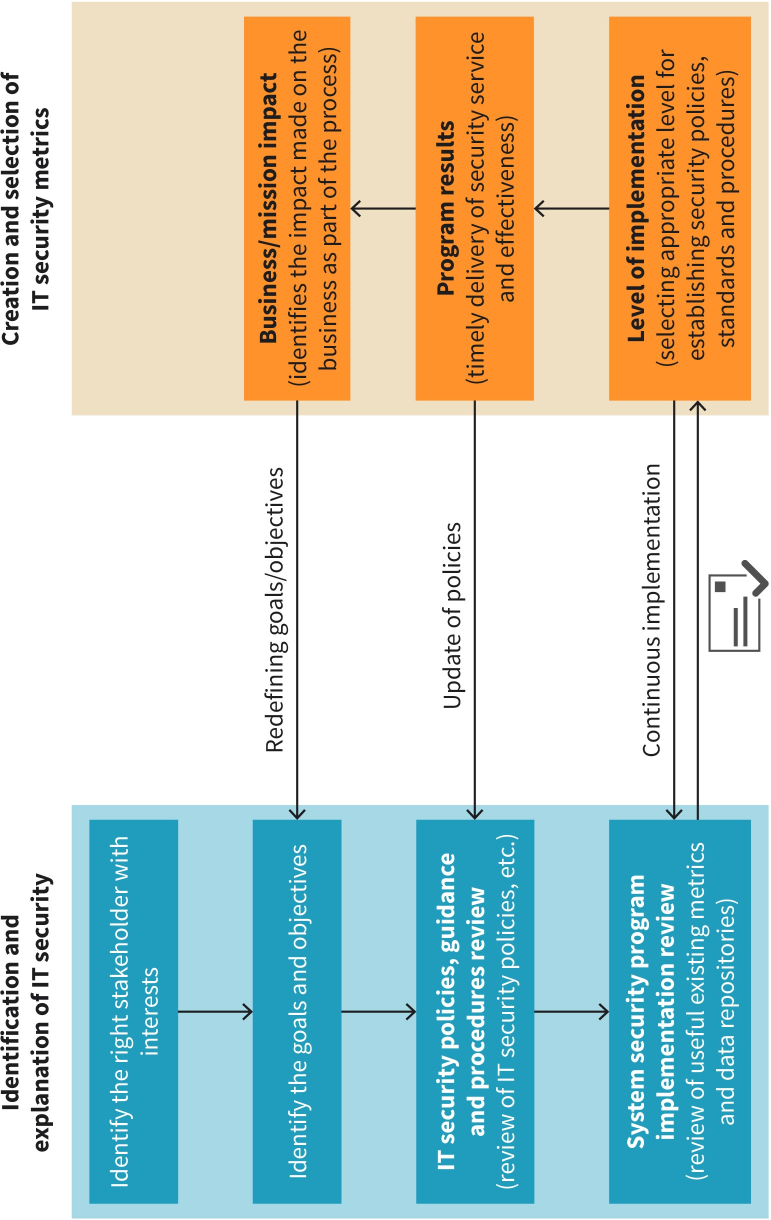
|  |  |
| --- | --- |
| Preparation of systems and procedures |  |
| Identification of incidents |  |
| Containment of attackers and threats |  |
| Eradication of and re-entry |  |
| Recovery from incidents |  |
| Lessons learned and feedback |  |

**Factors for selecting a security metric**

****

|  |  |
| --- | --- |
| Purpose |  |
| Controllability |  |
| Context |  |
| Best Practices |  |
| Quantitative |  |
| Data quality an ease of collection |  |
| Selection of security metrics |  |

**IT Security metric development process**

****

|  |  |
| --- | --- |
| Identification and explanation of IT security |  |
| Identify the right stakeholder with interests |  |
| The goals and objectives |  |
| Policies, guidance and procedures review etc. |  |
| System security program implementation review (of useful existing metrics and data repositories) |  |
| Redefining |  |
| Update of |  |
| Continuous |  |
| Creation and selection of metrics |  |
| Business/mission impact (identifies the impact made on the business as part of the process) |  |
| Program results (timely delivery service and effectiveness) |  |
| Level of (selecting appropriate level for establishing security policies, standards and procedures) |  |

**Examples of primary and secondary stakeholder**

****

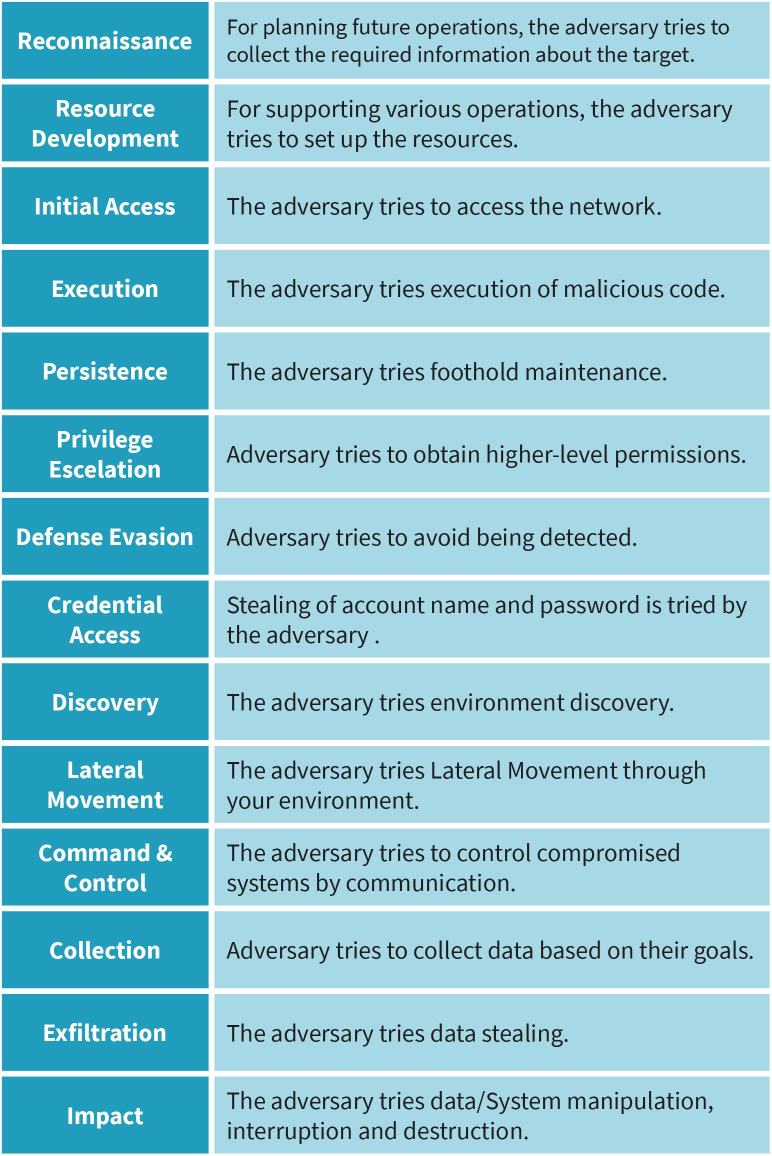
|  |  |
| --- | --- |
| Primary stakeholder |  |
| Head of agency |  |
| Chief information officer (CIO) |  |
| Security program manager/Information system security officer (ISSO) |  |
| Owner |  |
| Administrator/network |  |
| IT support personnel |  |
| Secondary |  |
| Chief financial |  |
| Training organization |  |
| Human resources |  |
| Inspector general (IG) |  |

**Structure of ISO/IEC 27001 standardA picture containing text, screenshot, font, number

Description automatically generated**

|  |  |
| --- | --- |
| Chapters for formality |  |
| Foreword |  |
| Introduction: overview of the standard |  |
| Scope: mentions the generic ISMS requirements |  |
| Normative references: mandatory read standards |  |
| Terms and definitions: similar to the ISO/EC 27000 |  |
| Bibliography |  |
| Mandatory for certification |  |
| Context of the organization: Provides organizational context |  |
| Leadership: Deals with leadership of management |  |
| Planning: abstracts the information on managing the changes in ISMS |  |
| Support: Assigns adequate and competent resources |  |
| Operation: Outlines various operations |  |
| Performance Evaluation: Deals with monitoring, estimating etc. |  |
| Improvement: Refines |  |
| Discretionary chapters |  |
| Annex A: Deals with security controls detailed in IDO/IEC |  |
| Explained more fully |  |

**14 tactics in the enterprise matrix**

****

|  |  |
| --- | --- |
| Reconnaissance |  |
| Resource Development |  |
| Execution |  |
| Persistence |  |
| Privilege Escelation |  |
| Defense Evasion |  |
| Credential Access |  |
| Discovery |  |
| Lateral Movement |  |
| Command& Control |  |
| Collection |  |
| Exfiltration |  |
| Impact |  |
| For planning future operations, the adversary tries to collect the required information about the target. |  |
| For supporting various access the network. |  |
| Execution of malicious code. |  |
| Foothold maintenance |  |
| To obtain higher-level permissions |  |
| Avoid being detected |  |
| Stealing of account name and password is tried by |  |
| Environment discovery |  |
| Lateral Movement through your |  |
| Control compromised systems by communication |  |
| Adversary tries to collect data based on their goals |  |
| Stealing |  |
| Manipulation, interruption and destruction. |  |