INPRESEC Platform Overview

Artificial Intelligence and Machine Learning for better Information Security & Privacy

Paradigm shift in Information Security

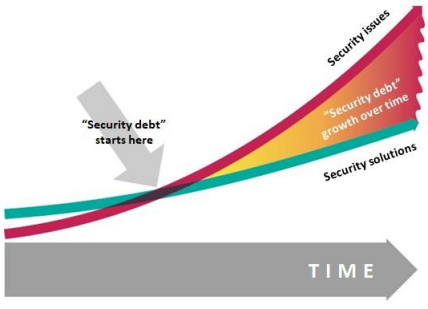
Predict – Prepare – Prevent – Detect

Tens of millions of security interesting events happen monthly. Humans hardly can cope with all of them. Breaches cost a lot of money and not money only.

The problem of today's information security and the "security debt" growth over time is reflected through a rapidly increasing number of security breaches. Organizations are not able to cope with all of the threats, attacks and risks any more. There is:

- significant amount of manual work
- lack of focus and concentration leading to errors
- lack of skilled professionals and tools
- increasing cost

There is no true predictive approach on the market.



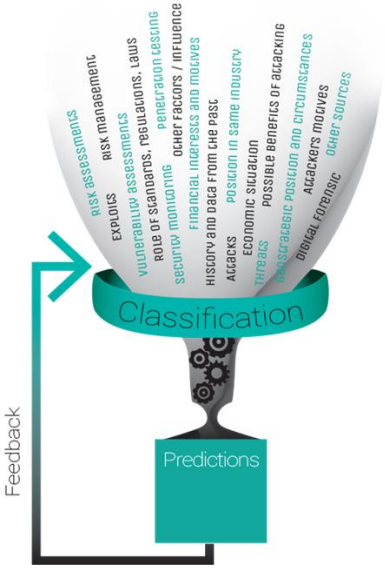
INPRESEC Solution: INPRESEC uses Artificial Intelligence, Machine Learning, Predictive Analytics, Threat Intelligence to provide classification and prediction of security threats, issues and attacks.

INPRESEC Security Solutions are based on a Common Platform that employs modules that detect and prevent activities that violate security policy, including, but not limited to intrusions, data leaks and similar.

With our holistic approach, the system classifies these activities as normal or anomalies i.e., allowed or not allowed, or predicts activities that violate security policy. System alerts the security and/or network administrators about the occurrences of events that are not allowed - and optionally reacts to them.

INPRESEC Platform consists of six components:

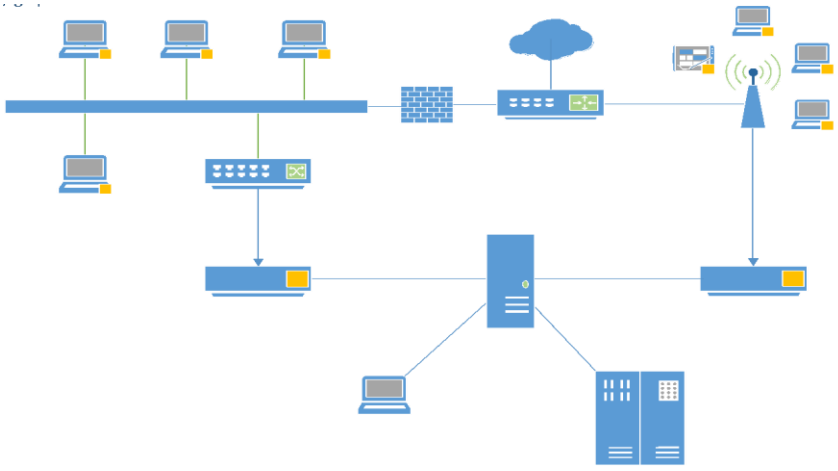
- Agent
- Sensor
- Server
- Administrative Panel
- Trainer
- Prediction Module



These components make a multilevel and multilayered system which operates on network level, on host level and protects system components, users, application and data, following the "defense in depth" approach. The platform also shifts the paradigm in the sense that it looks into issues within a "holistic approach", providing detection of various threats and attacks to the system and working in collaboration with the prediction module (currently in development).

INPREEC Solution also provides additional "***security analyst in the loop***" concept, with supervised learning – the solution becomes more and more clever over time and requires less human intervention, saving significant amounts of time and money, while significantly improving security posture of the system and reducing the risk.

An example diagram of the INPRESEC platform is shown on the figure below.



Platform components

INPRESEC Sensor is a network-based security system that analyzes network traffic and seeks possible security violations in it. Sensors may be implemented as software, deployed on a networked computer or separate appliance, set in the wired or wireless network environment. Sensor detects attacks, intrusions, data leaks and similar activities that violate security policy and reports, prevents or cancels these activities on the network. Sensor alerts the security and/or network administrators and collaborates with the INPRESEC Server.

INPRESEC Agent is a host-based security system, implemented as software installed on a computer (e.g., server, desktop, laptop), mobile device (e.g., phone, tablet) or network device (router, firewalls or access point). In the future, it will be possible to install it on other IoT (Internet of Things) enabled devices. Agent analyzes events and behavior of the underlying systems and seeks for possible security violations. Agent detects attacks, intrusions, data leaks and similar activities that violate security policy and reports, prevents or cancels these activities. Agent collaborates with the INPRESEC Server.

INPRESEC Server is software that integrates functions of Sensors and Agents. Server collects information from Sensors and Agents deployed throughout a network and analyzes it. Server provides Sensors and Agents with updates and new classification and prediction models trained with Machine Learning algorithms. Server provides security and/or network administrators with information on system status and activities that violate security via Administrative Panel. Servers can be linked to SOC / CERT centers or with other security software or devices: antivirus software, SIEM tools and firewalls. Server can be deployed on the client's corporate network or used as an INPRESEC service.

INPRESEC Administrative Panel is a set of GUI tools intended to facilitate configuration, monitoring, management, tuning, and preparing reports about system components' activity. It can be accessed via a Web browser, locally or remotely, from the computer or mobile device. It is implemented as a part of the server software.

INPRESEC Trainer is a training system component based on machine learning (ML). Trainer uses labeled (annotated) data sets either created by security analysts or during annotation of events and reports of the working system and creates new models with higher detection accuracy. By machine learning, our system provides continual improvement of systems which is of paramount importance for customers and adapting to a variety of threats, attacks, as well as specific requirements that customers may have.

INPRESEC Prediction Module is a component based on machine learning (ML) and artificial intelligence. Using various parameters and input data from a set of internal and external sources, it analyzes them and, through a set of our proprietary algorithms, gives probabilities of possible threats and attacks. These data will be later distributed as input to our system and help to set alert levels, thresholds, prevention measures etc. Note: this component is in development and planned for patent application.

Advantages and Value

This system provides set of advantages:

- Efficient protection of computer and communication networks and systems
- In-depth protection: users, applications, and data
- Detection and protection of individual systems/devices and networks
- In-depth protection: user's applications and data

Value Proposition INPRESEC offers is: less pain, less risk:

- Predicts, prevents & detects security threats and attacks before they affect live systems
- Continual improvement process. Demonstrable accuracy of approximately 99% after a set of learning cycles.
- Minimizes work of security teams, while improving accuracy, reaction time and security solutions performance
- Saves significant amounts of money, time and efforts for companies and organizations.

Services and Product Model

INPRESEC can be an additional tool in the Security Operations Center (SOC).

Depending on usage scenario, various business/deployment models can be used:

- Cloud based service
- On premises product model: hosted by the client, serviced by INPRESEC, depending on requirements
- Service model: Security as an (INPRESEC hosted) Service

In more details, INPRESEC provides choice of services and products offering through:

- Subscription model to information security services
    - Subscription to INPRESEC solution services as MSSP (Managed Security Services Provider)
    - Cloud based service - Virtual appliance and similar models
- Product & systems with licensing, implementation, integration and support for users and partners who want on-premises systems.

Also, other services can be provided:

- Information gathering and dissemination through specialized data feeds (Threat Intelligence & Predictions)
- Services, SDK
    - System learning, fine tuning
    - Partners' training, education, learning
    - SDK libraries and tools for 3rd party use, royalties

Administrative panel

The Administrative Panel is accessed via a web browser. It is implemented as a responsive web application, with the aim to be usable with different browser geometries. It includes the following tools:

- Operation-supporting tools, including:
  - Dashboard
  - Clients viewer
  - Reports management
  - User actions log viewer
  - Client events log viewer
- Administrative tools
  - Users management
  - Clients management
  - Models management
  - Training sets management

On the screenshot below you can see the dashboard, designed to provide a bird eye-view of key recent activities of clients (sensors, agents) and users (security analysts reviewing and classifying the reports and doing other actions using the Administrative Panel).