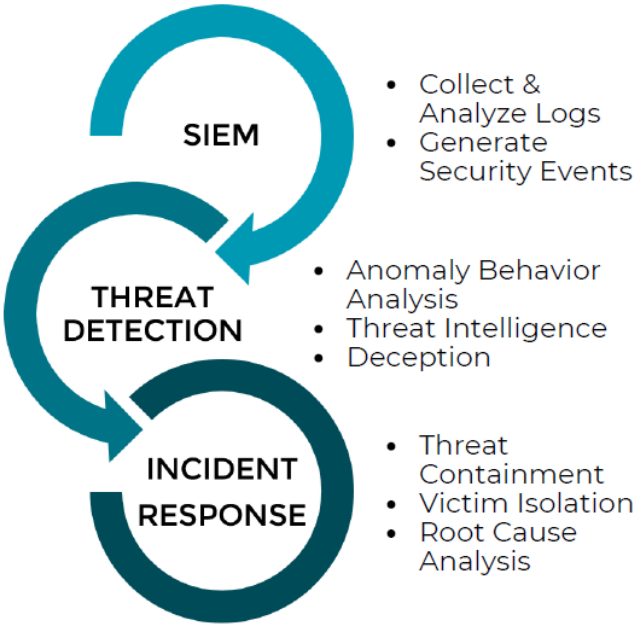
BLUE TEAM HACKING DEFENSE

IN-SIGHT | INCIDENT, DETECTION & RESPONSE



- Collect & Analyze Logs
- Generate Security Events

- Anomaly Behavior Analysis
- Threat Intelligence
- Deception

- Threat Containment
- Victim Isolation
- Root Cause Analysis

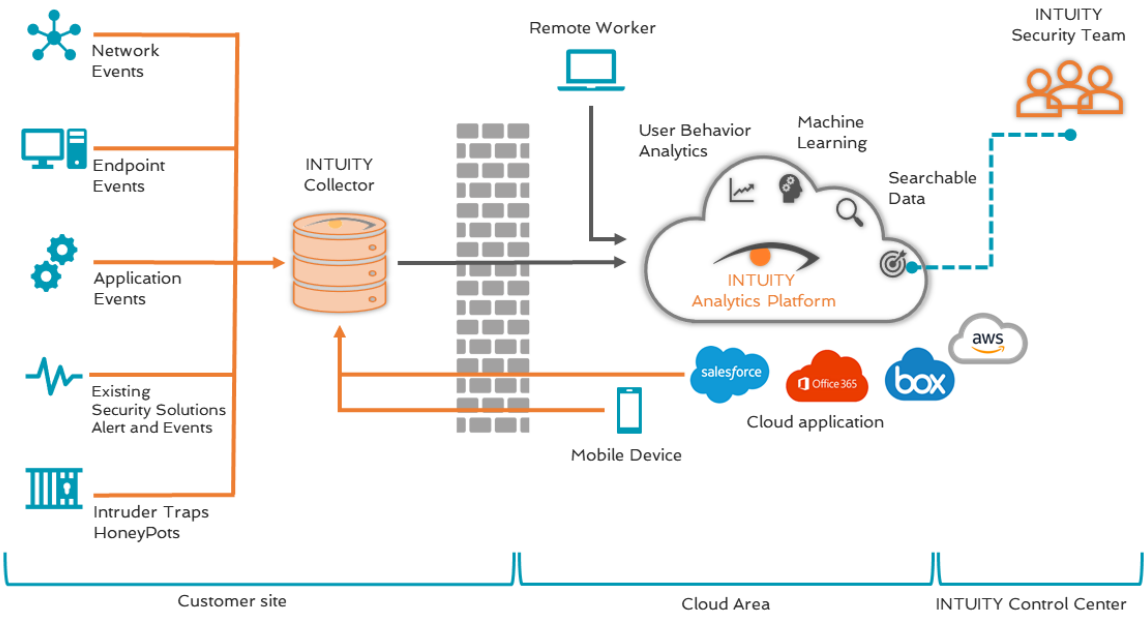
To increase your ability to detect an attack in progress and react as quickly as possible, you can activate **deception** features such as: Honeypot, Honeyfile, Honeyuser, Honeycredential.

The INTUITY IN.SIGHT service was born from the awareness, matured in the provision of Red Team services, of the methods, tools and procedures used during a cyber attack and, consequently, the most effective strategies to detect and block it. For this reason, the IN.SIGHT service is provided by both analysts and ethical hackers.

The service is aimed at companies that want to equip themselves for the detection and management of computer incidents, or that want to extend existing services by including visibility on what happens at the endpoint (PC and Server), on mobile devices (laptops, smartphones and tablets) or on cloud systems (AWS, Google, Microsoft and others).

IN.SIGHT increases your IT visibility, allowing you to react promptly, prevent damage, and comply with the most common safety standards such as ISO27001, GDPR, and PCI DSS.

ARCHITECTURE



Powered by RAPID7

The service's architecture involves the installation of one or more collectors at the customer's premises, the distribution of agents on PC, server, and mobile devices, and an interface with the cloud services of interest.

The correlation functionalities are performed by a cloud platform (in compliance with GDPR regulations), while the analysis and communication with the customer is guaranteed by a team of specialists. The service can guarantee results as soon as it is activated because, thanks to the distributed agents, it immediately recognizes significant threats and can correlate any anomaly with known attack methods.

DELIVERABLE

- Technical Report: weekly.
- Executive Report: monthly.
- In the event of a critical alarm, the Security Team takes charge of the problem and starts the analysis, performing predefined containment actions. You can define automatic actions to block the threat as soon as it is detected. The Security Team and the client will be in continuous contact until the incident is closed.
- In case of important "Notable Behavior" warnings, the Security Team will start the analysis within the next working day and work until the most appropriate action is determined. The customer is notified of the analysis in progress and is kept up to date on developments until the incident is closed.
- Open communication with INTUITY Red Team for advice and support.

USE CASE

- Security Operation and Competence Center for SMEs and Enterprise.
- Add-On for existing SOC services: increased visibility to endpoint, cloud, and mobile users.
- Integration with tools already implemented (Network Analyzer, Advanced Threat Protection System).