

+500  **IT**
YEARS ACUMULATED IN CONSULTING

10 
OFFICES
AMERICAS-EMEA

12 
STRATEGIC
ALLIANCES
/ PARTNERS

7  **IP**
SOLUTIONS
   

40% 
more AGILE &
deployment cost
reduction

myCloudDoor

 **myCloudDoor**
Cybersecurity & Innovation

4 
CLOUD AREAS
CONSULTING
MANAGED
ANALYTICS
PROJECTS

+ 100 
CLIENTS

COMPETENCIES

- GOLD CLOUD PLATFORM
- GOLD DATACENTER
- GOLD DATA PLATFORM
- GOLD DATA ANALYTICS
- GOLD DEVOPS
- GOLD APPLICATION DEVELOPMENT
- GOLD APPLICATION INTEGRATION
- GOLD CLOUD PRODUCTIVITY
- SILVER MESSAGING
- SILVER COLLABORATION AND CONTENT
- SILVER SECURITY
- SILVER SMALL AND MIDMARKET CLOUD SOLUTIONS

12  

80% 
CERTIFIED
CONSULTANTS

IN CLOUD
BUSINESS

TOP 3
COMPANIES

SAP on Azure LeaderShip

A large white graphic on the left side of the slide. It consists of a stylized cloud shape at the top, a vertical line extending downwards from the center of the cloud, and a white circle at the bottom of the line. The text "myCloudDoor MYCD-CERT® SOC" is positioned to the right of the circle.

myCloudDoor MYCD-CERT® SOC

Strengthen your business security against cyber threats with **myCloudDoor SOC**, based on Microsoft Sentinel and powered by artificial intelligence

Key challenges in a SOC

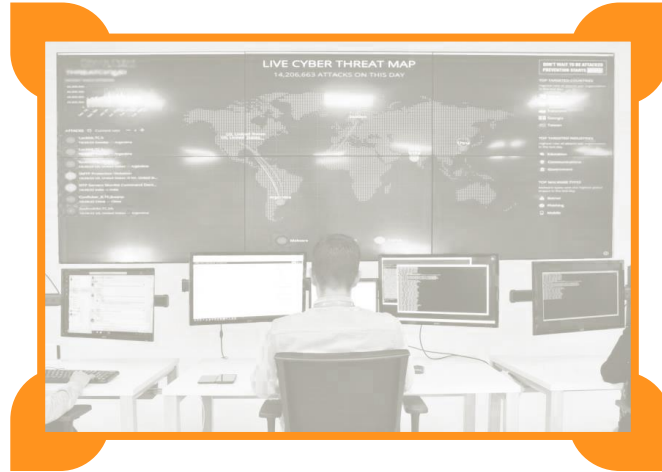
Advanced attacks pose challenges to traditional defenses and security analysts

1 Complexity and costs

The use of tools deployed in silos and disjointed flows increases costs, complexity and effectiveness.

2 Undetected threats

Traditional approaches are mainly based on detecting the known



3 Limited visibility

Digital transformation, heterogeneous (IT/OT) environments and cloud adoption create a need for additional monitoring and more blind spots.

4 Slow response time

Today's threats are extremely complex and increasingly automated, making it harder and harder for human analysts to assess and manage them at the necessary speed.



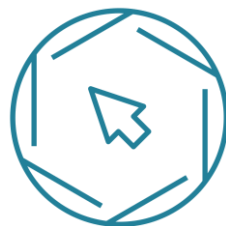
What do we need?

Necessary changes in the SOC approach



Eliminate data silos

Gain visibility across different data sources relevant to analysts - from cloud, IT/OT environments to data.



Unify flows / Centralize tools

Work without continuous jumping between tools using a single platform that centralizes the entire process.



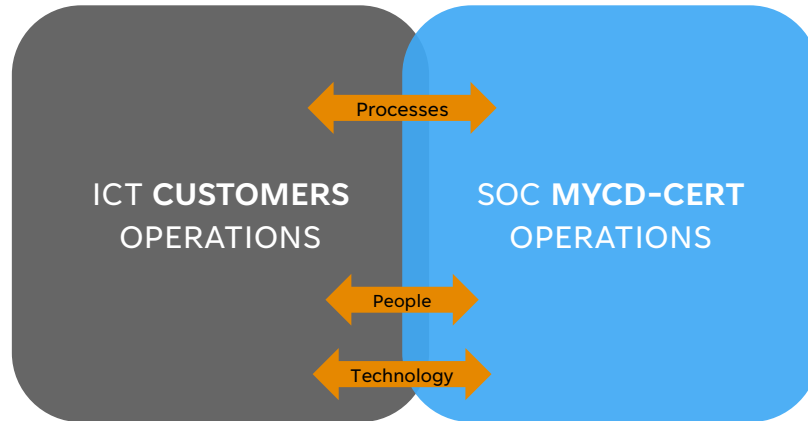
Automate tasks

Let the machines do the hard work - both repetitive, routine tasks and complex analysis.

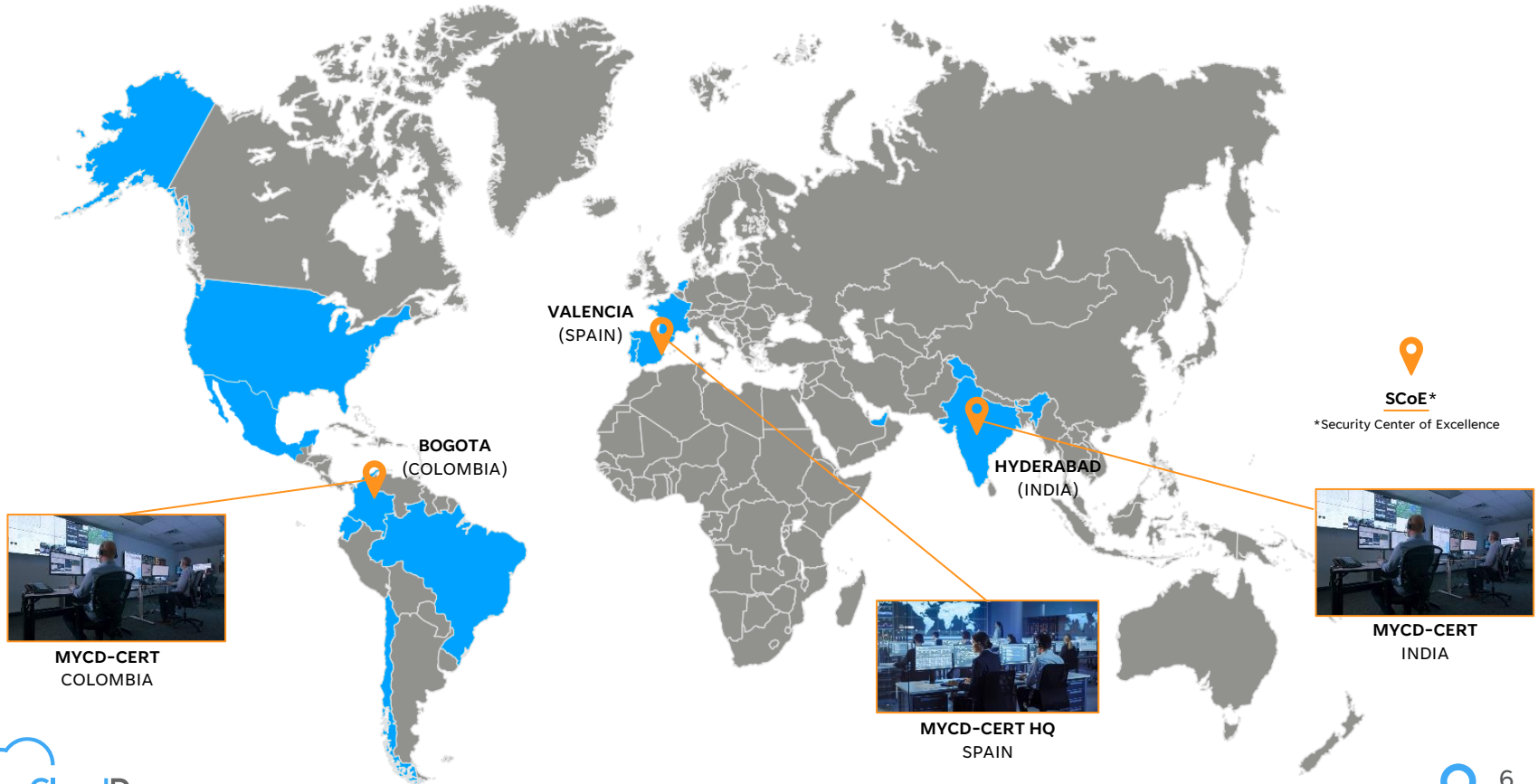
Security Operations Center (SOC)

myCloudDoor MYCD-CERT® SOC

myCloudDoor MYCD-CERT® SOC is the information security operations center responsible for carrying out the analytical security (proactive and real-time threat detection) and operational security (vulnerability and incident management) activities that myCloudDoor makes available to our **clients** for the delivery of cybersecurity services, using market-leading tools offered "as-a-service", according to their needs. myCloudDoor' innovative Security Operations Center (SOC) offers a differentiating service that combines threat intelligence and rapid response to security incidents, in a real 24x7x365 mode.



MYCD-CERT geographical distribution



SOC Managed Cybersecurity Services

Benefits



SOC Managed Cybersecurity Services

Integrated Cybersecurity Services

24x7 Security Incident Monitoring and Management



Threat modelling & MITRE Threat Map



Threat Hunting



Service Management and Continuous Improvement



Detect & Respond (MXDR)



myCloudDoor

Protect



Technical Security Office

Identify



Advanced Vulnerability Management (AVM)

Respond & Recover



Digital Surveillance



24x7 Incident Response (DFIR)



myCloudDoor Managed Extended Detection and Response (MXDR)



Managed Extended Detection and Response (MXDR)

Basic principles of service. myCloudDoor MXDR platform

DETECTION



Advanced Threat Detection

myCloudDoor cybersecurity experts discover threats, early, by leveraging advanced threat intelligence from MITRE Threat Map and Threat Intelligence from Microsoft, our detection use cases, behavioral analysis engines (UEBA), machine learning, and statistical analytics.

Threat Intelligence Feeds

Threat intelligence applied to the customer's specific context, Microsoft threat intelligence, Third Party intelligence feeds, and adversary simulation.

INVESTIGATION



Threat Investigation

myCloudDoor SOC analysts investigate potential cybersecurity incidents and provide measures and recommendations to mitigate them. Alerts are enriched with customer context information, which helps quickly identify the focus and scope of the threat.

Threat Hunting

The service performs proactive hunting for advanced threats, automating search rules and adapted to the customer's context.

RESPONSE



Incident Response

myCloudDoor SOC analysts activate the automations generated to respond efficiently to the incident, before it spreads. They are also working on the direct automation of many of them. The 24x7 incident response team remains active to respond and move in the event of an incident.

24x7 SOC

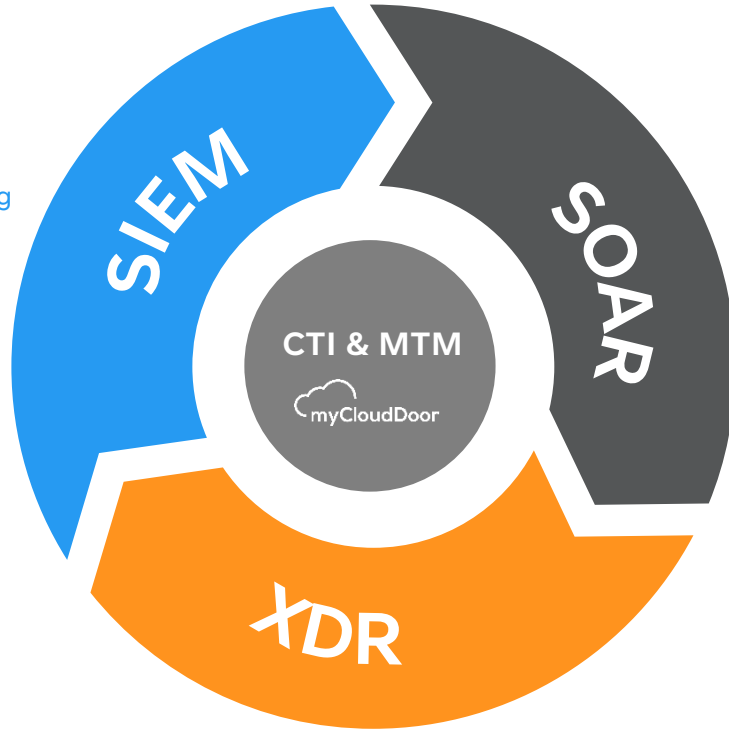
The SOC's 24x7 team is always available and accessible to communicate directly using a personalized Teams channel (chat or video), phone number, and email.



Managed Extended Detection and Response (MXDR)

Basic pillars of service. myCloudDoor MXDR platform

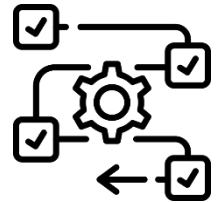
- Centralizing alerts
- Continuous Monitoring
- Threat detection



- Response
- Integrate platforms



People



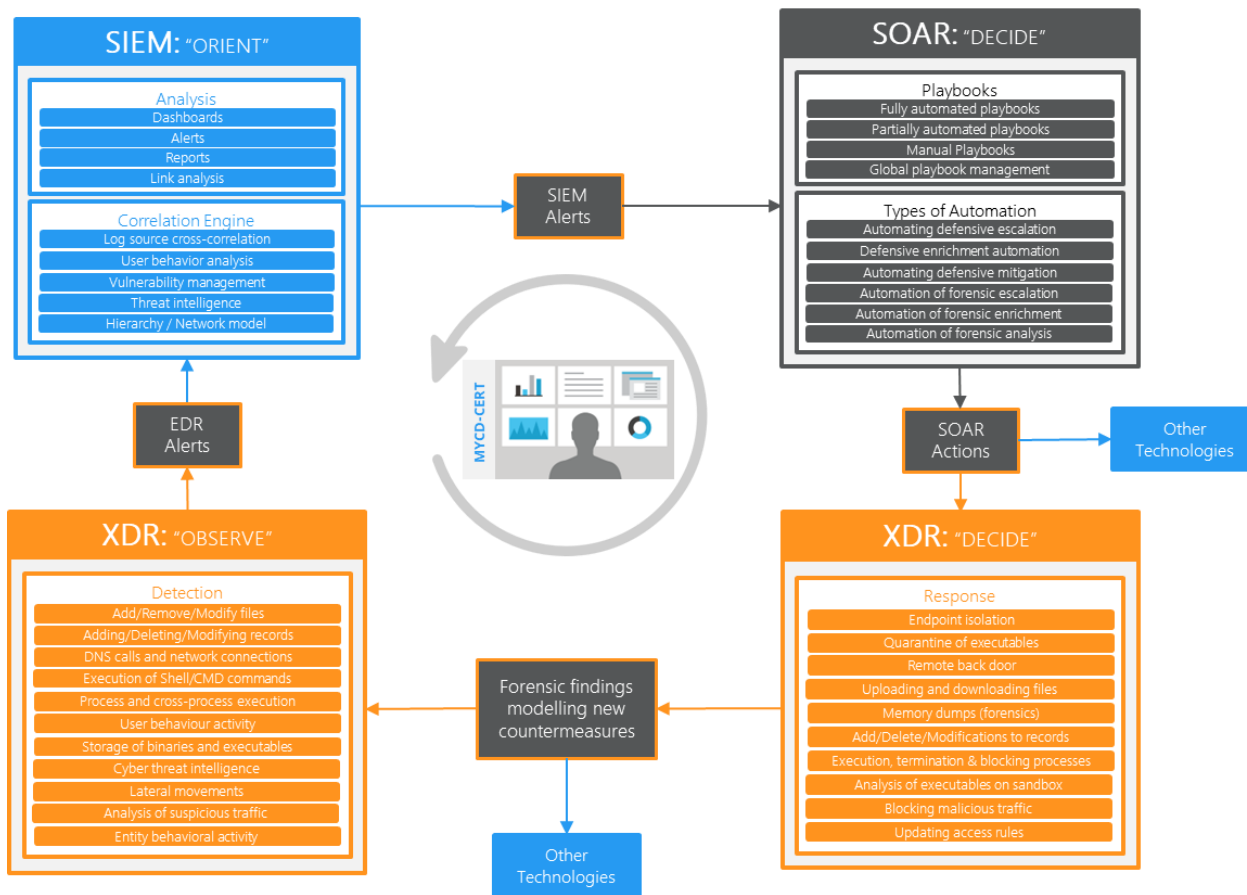
Processes

- Protect
- Threat detection
- Response
- Discover



Managed Extended Detection and Response (MXDR)

Our managed detection and response model approach



Managed Extended Detection and Response (MXDR)

Integrated cybersecurity platforms

SIEM

- Microsoft Sentinel
- myCloudDoor Data Collector
- myCloudDoor Threat Detector



SOAR

- Shuffle SOAR (MyCD own)
- Microsoft Logic Apps



XDR

- Microsoft Defender XDR (recommended)
- Any other XDR product (Palo Alto, CrowdStrike, etc.)



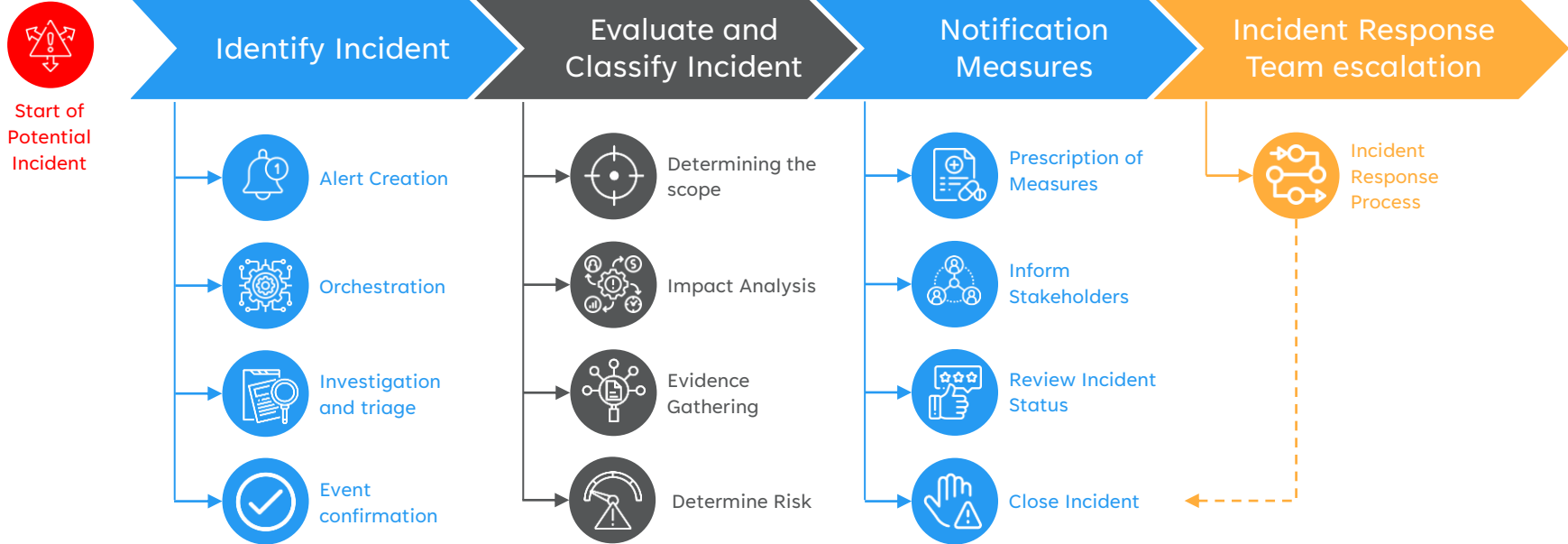
THREAT INTELLIGENCE

- myCloudDoor MITRE Threat Map (MTM)



Managed Extended Detection and Response (MXDR)

Cyber incident Management Process



Periodic Service Reports

MXDR monthly service report

myCloudDoor

MXDR Monthly Service Report
CLIENT

1 INTRODUCTION

This document compiles the results of last September of the SOC service provided by the Security Department to CLIENT.

The document has been organized in several different points, detailing the purpose of this document, classifying the security alerts according to the CCN STIC-817 and NIST SP 800-61 guidelines, status and statistics of the service, pending points and relevant facts of the service.

This report aims to provide an overview of the performance and effectiveness of the services provided by the myCloudDoor Security Operations Centre during the specified monitoring period. It will detail key activities, incidents handled, improvements implemented and any other relevant information.

2 EXECUTIVE SUMMARY

Following the go-live of the managed security service by myCloudDoor's SOC, a report is issued reflecting the evolution of the service during the month of September 2023.

During this period, the security service has managed a total of 315 potentially dangerous security alerts, among other tasks related to interactions with the CLIENT team. In addition, it should be noted that during this month no threat against the CUSTOMER's systems has materialized.

The history of alerts managed by the SOC MXDR service is shown below.




Month	Detected Alerts
January	183
February	139
March	92
April	106
May	223
June	224
July	315
August	313
September	309

CLIENT: MXDR monthly service report - September 9

myCloudDoor

MXDR Monthly Service Report
CLIENT

Security alert classification



Category	Number of Alerts
SECURITY POLICY	138
INTRUSIONS	122
OBTAINING INFORMATION	10
COMMITMENT OF INFORMATION	17
AVAILABILITY	2
HARMFUL CODE	10
ABUSIVE CONTENT	0
OTHERS	5

ILLUSTRATION 3. CLASSIFICATION OF ALERTS IN THE MONTH OF SEPTEMBER 2023 ACCORDING TO CCN-STIC-817

2.1 MAIN ALERTS

The alerts in the "Security Policy" category are due to the current configuration of the rules.

- Communications are detected with an external IP listed as a possible tracker, on a port used by P2PTV applications, the uninstallation of the program used is prescribed (Ticket in Jira Case # XXX).
- Internal IP making a connection to legitimate services, such as Google, Microsoft or Akamai Technologies, sending a large number of packets in a given period of time, but no malicious activity is detected (Case # XXX).

Alerts in the "intrusions" category are related to attacks received on CUSTOMER assets.

- Multiple intrusion attempts to exploit vulnerabilities in the CUSTOMER assets, the attacks received are analyzed and if the asset is vulnerable. Of all the threats detected, none have had an impact on the company (Case # XXX).
- Attempted access to CUSTOMER assets. A specific case is an attempt to access the Zabbix server via SSH. After investigation, it is detected that no access was gained, but that the version of OpenSSH used contains multiple vulnerabilities and the IT department is instructed to update the version used (Case # XXX).

In the "Information gathering" category, they are mainly:

CLIENT: MXDR monthly service report - September 12

myCloudDoor

MXDR Monthly Service Report
CLIENT

3 PENDING ACTIONS

The following are the pending actions to be carried out:

- Sophos Central was integrated into Microsoft Sentinel as a new source, also the alerts arrive by mail to the users to whom these notifications have been configured, but the interaction between the Internal Systems department and myCloudDoor SOC to mark as resolved the alerts in the Sophos Central console needs to be proceeded.
- Plan the date for the next periodic (monthly) vulnerability scan.

4 IMPROVEMENTS IMPLEMENTED

Detection Tool Enhancements:

Microsoft Sentinel use cases have been updated to improve early threat detection. New use cases are documented in CLIENT_Threat_Modeling_ver_2_1.pdf.

Staff Training:

A training session on advanced threat detection has been conducted to improve staff skills in identifying and responding to threats.

Optimization of Procedures:

Incident response procedures have been reviewed and optimized (version 3.2.1) to ensure faster and more efficient action.

5 RECOMMENDATIONS

Several attacks (attempts to exploit vulnerabilities which are not affected) and scans on the CLIENT's DMZ have been detected. It has been detected that these attacks are being carried out on the service. A study of the alerts associated with this asset was carried out, and it was observed that attacks are continually being carried out in an attempt to exploit vulnerabilities that this asset does not have. A list of attacking IPs was obtained and a Jira ticket (ID: XXXXXXXXXX) was drawn up so that the communications area could block these IPs. For the moment, no attack has had any impact, and due to the risk of a successful attack, it is recommended:

- Block future attacker IPs.

CLIENT: MXDR monthly service report - September 15

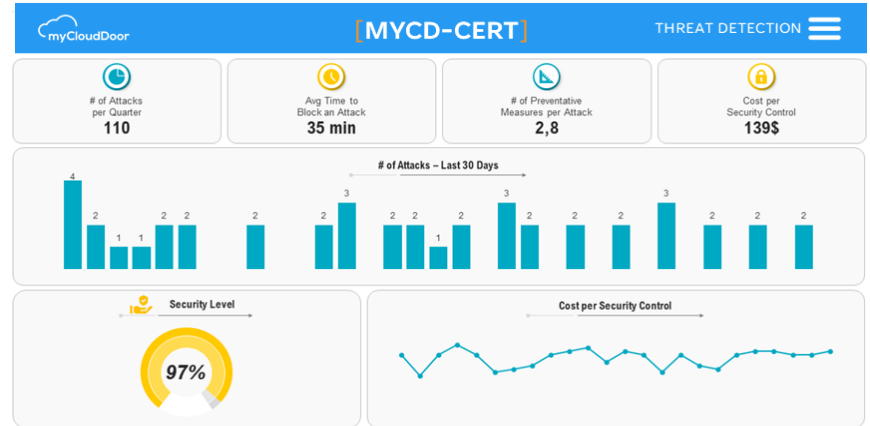
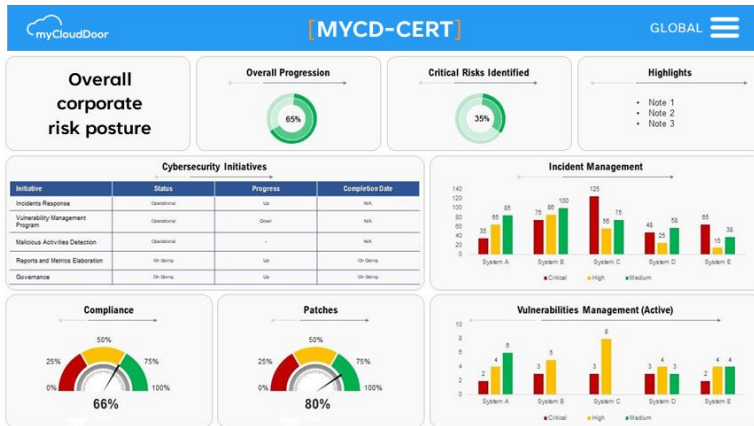


Service Tracking Dashboard

Fundamental tool for decision making and continuous improvement

The proposed cybersecurity service provides a **dashboard of indicators** and relevant information for the customer. In this way, it allows customers to consult the **evolution and status** of the service in **real time**.

The information offered is crucial to know the current situation and support the **continuous improvement** of corporate security and to involve the company's management in a **strategic vision** of security.



Comprehensive View - Decision-Making - Risk Management - Compliance - Continuous Improvement



Microsoft Sentinel (SIEM/SOAR) and Microsoft Defender XDR



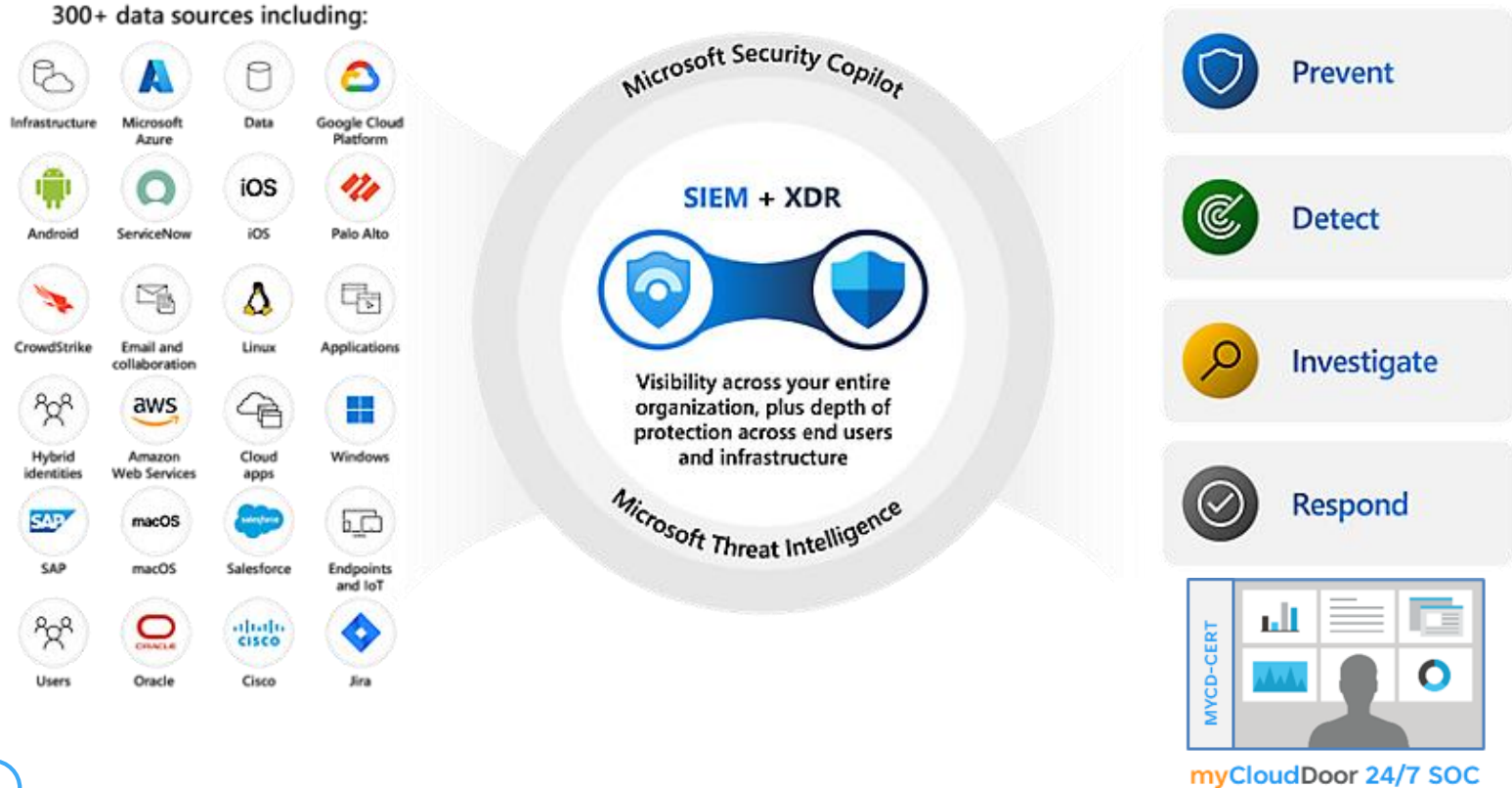
Microsoft Sentinel at the heart of our platform

Next-generation security platform with cloud technology and artificial intelligence



Microsoft Sentinel and Microsoft Defender

A perfect combination to combat cyber security threats



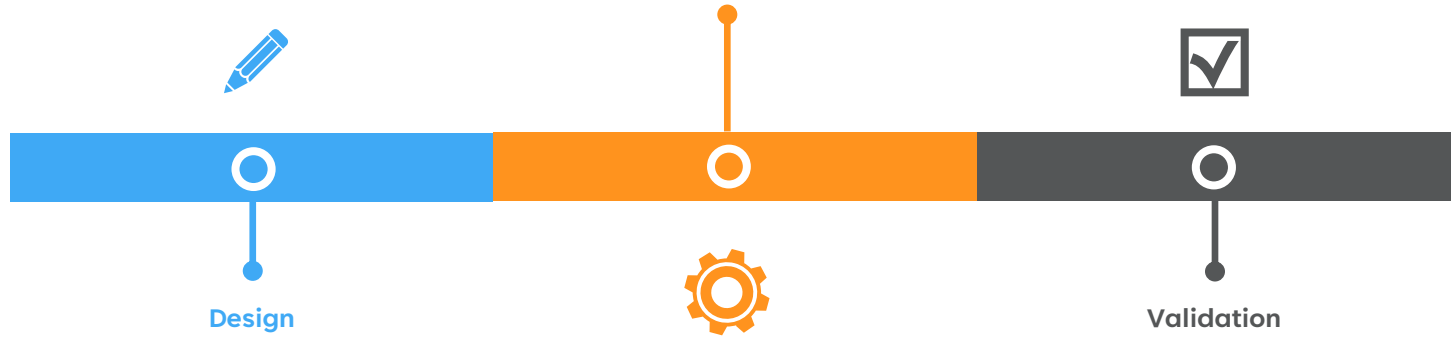


Microsoft Sentinel Deployment

Methodology: Implementation stages

Implementation

Once the environment has been designed and approved by the customer, our SIEM management and architecture specialists will carry out the implementation of the solution



Design

The myCloudDoor team will carry out an audit of the environment in order to develop a design that perfectly suits the needs of our client. In addition, using the FinOps methodology, an optimized environment will be designed to efficiently manage the costs of the solution.

Validation

With the implementation phase complete, it is crucial that everything works properly. To this end, an adversary simulation exercise will be carried out where each use case will be tested, and its correct operation will be confirmed.



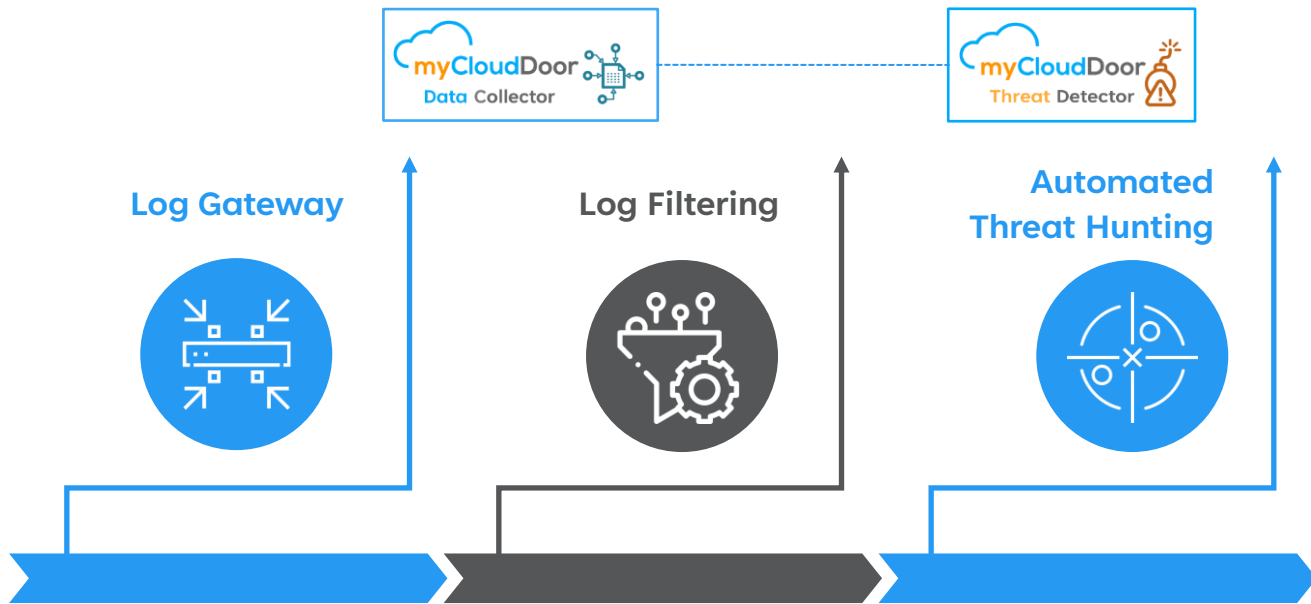
myCloudDoor Threat Detector





Managed Extended Detection and Response (MXDR)

myCloudDoor Threat Detector: Advanced threat hunting capabilities and log ingest efficiency



Collect

Collect events and logs from the necessary information sources.

Filter

Filter and select logs to redirect them to the appropriate database.

Hunt

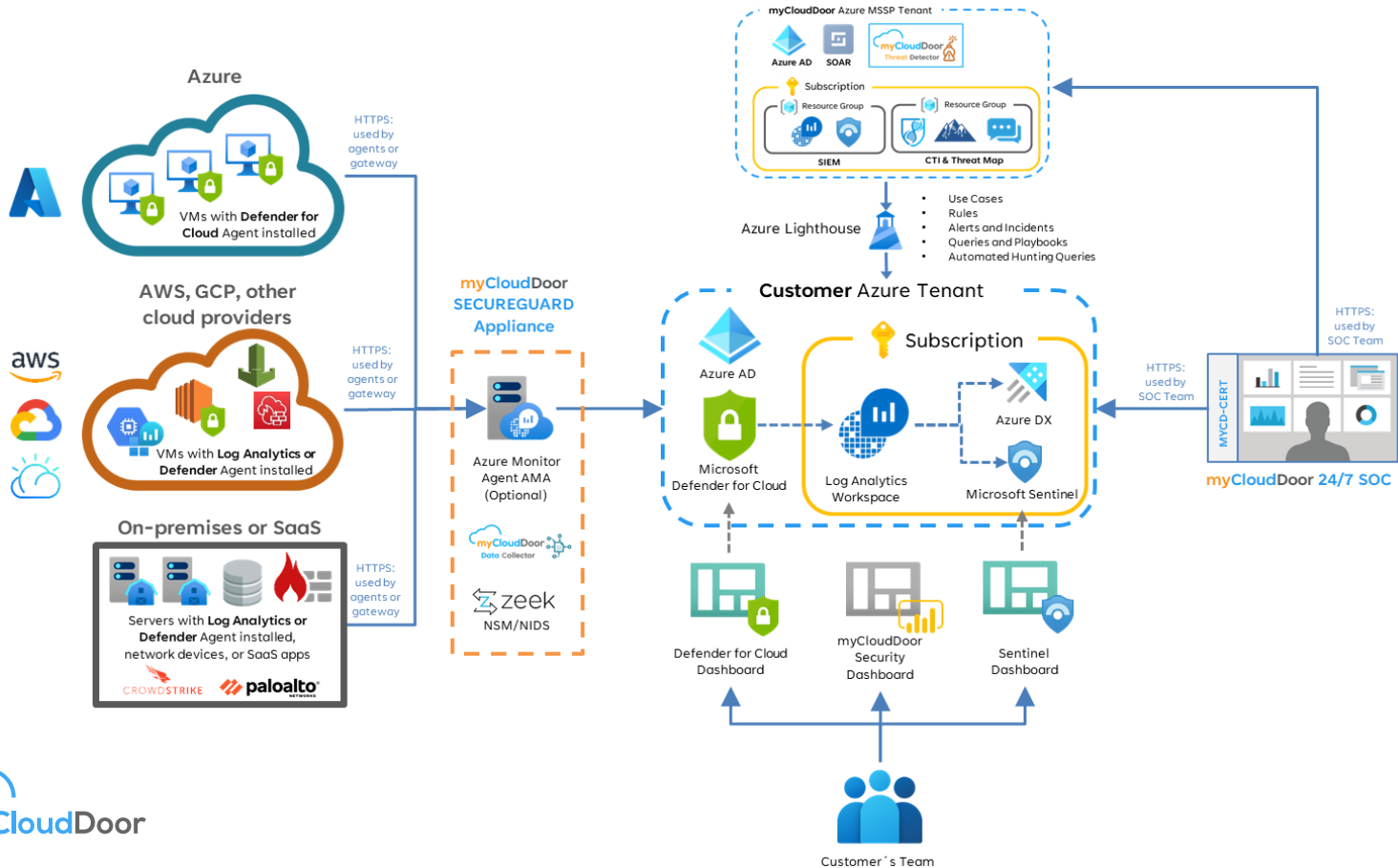
Launches automated threat hunting missions periodically.

Architecture for the MXDR service



Managed Extended Detection and Response (MXDR)

Detection and response platform architecture






24/7 Incident Response Service



24/7 Incident Response Service

Key elements of the service



Rapid Intervention Group



○ 24/7 availability and SLA measurement



○ Agile on-site deployment



○ Team of experts and specialists



○ Specialized equipment and tools



Crisis Committee



○ Leading the crisis. Guidance on decision-making



○ Mixed team composition



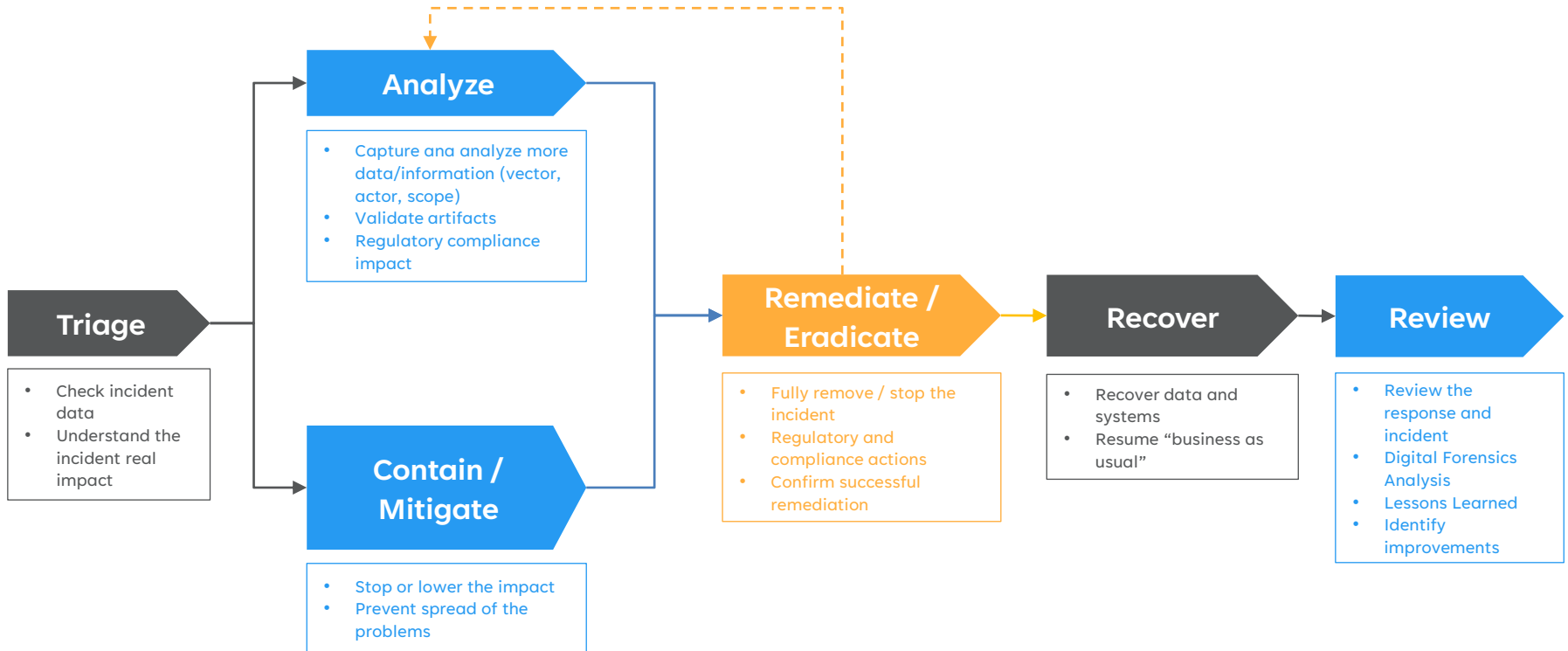
○ Negotiation and legal specialists



○ Dedicated videoconference rooms and resources

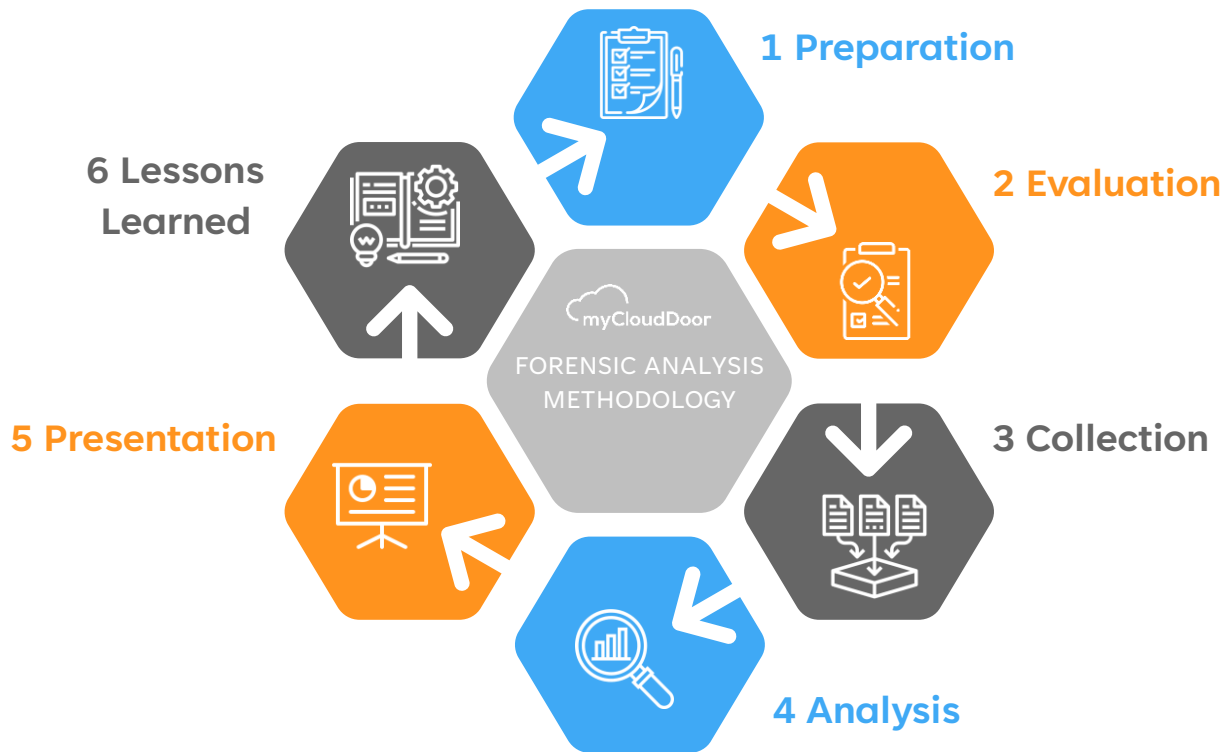
24/7 Incident Response Service

Incident Response Management Process



24/7 Incident Response Service

Methodology used for Digital Forensic Analysis



Deliverables

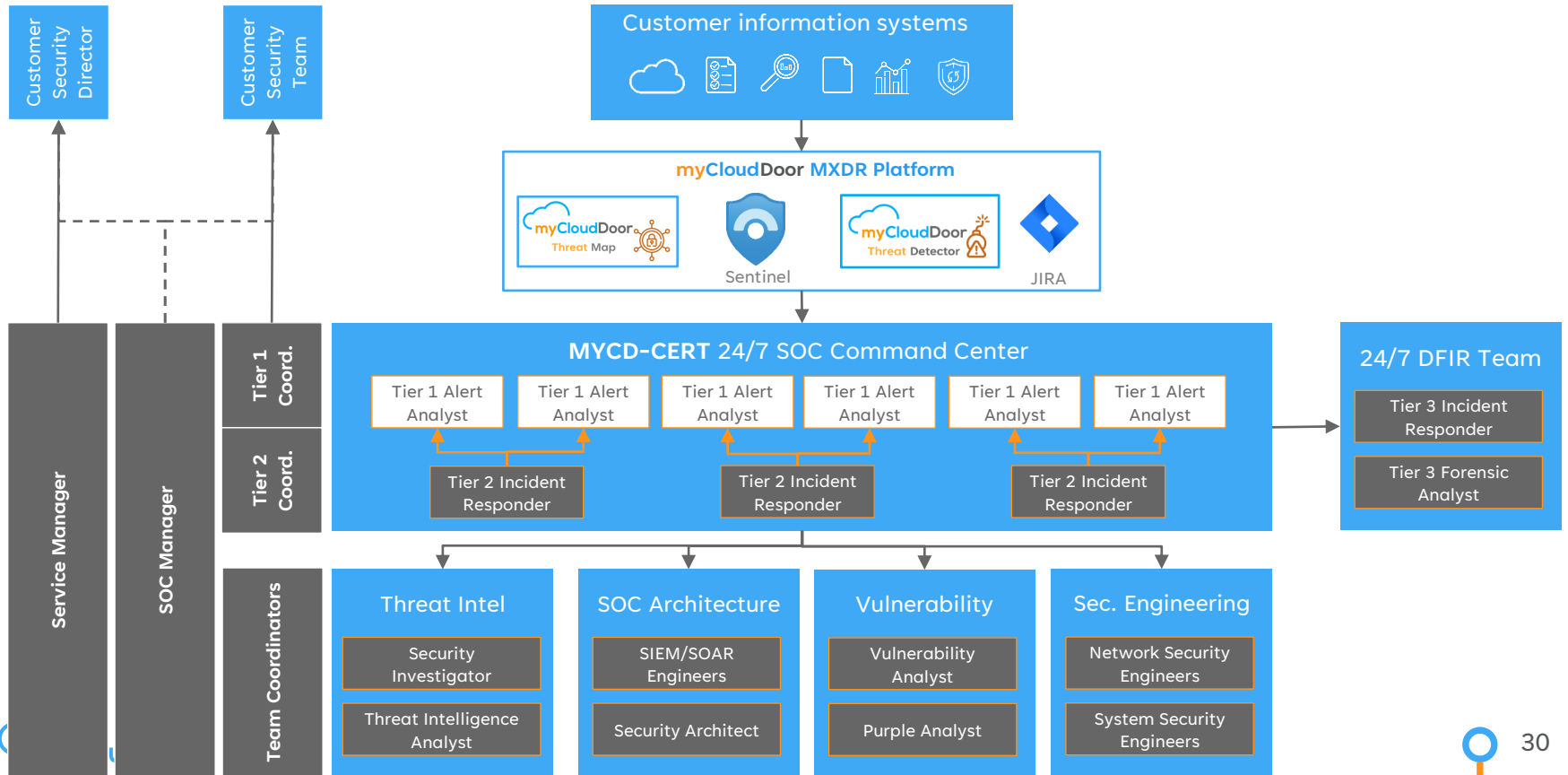
- Executive Summary
- Focus of the analysis
- General nature of the analysis
- Event Chain Timeframe
- Logical and/or deleted data
- Data leakage
- Keywords

Service organization and planning



Structure of the SOC service

Teams and Operating Model





Thanks



Creating future

THANKS



info@myclouddoor.com