Globeteam A/S

Continuous Security Improvement (CSI)

02.11.2021 I Peder Lind Sørensen

GLOBETEAM

“You can’t claim TRUST, you have to earn TRUST”

- Satya Nadella, Microsoft

“We have to treat privacy as a human right. We have to have end-to-end cybersecurity built into technology. We have to have both a set of ethical principles that guide our AI, but most importantly we have to translate that into engineering practices that are there, that are part of everyday engineering.”

Globeteam Continuous Security Improvement

KNOWLEDGE

AGILITY / FLEXIBILITY

TRUST

These are the most important ingredients in a relationship between us and our customers

GLOBETEAM

Globeteam Continuous Security Improvement

GLOBETEAM CONTINUOUS SECURITY IMPROVEMENT IS AN EFFECTIVE AND PRAGMATIC SERVICE BUILD ON TOP OF THE MICROSOFT TRUSTED CLOUD. ENSURING HIGHEST VALUE OF THE SERVICES THAT MICROSOFT HAS ALREADY INTEGRATED IN THEIR CLOUD PLATFORM

Globeteam Continuous Security Improvement is a service based on standard tools from the Microsoft cloud platform, to support customers in the space between their in- or outsourced ”Security Operation Center (SOC)” and their needs for agile and continous security improvement.

Globetam Continuous Security Improvement is a service that, besides using the standard tools from Microsoft’s Cloud platform, takes advantage of Microsoft’s yearly investments of 1 billion USD and more than 3.500 security experts focusing on analysis and development of Microsoft security solutions.

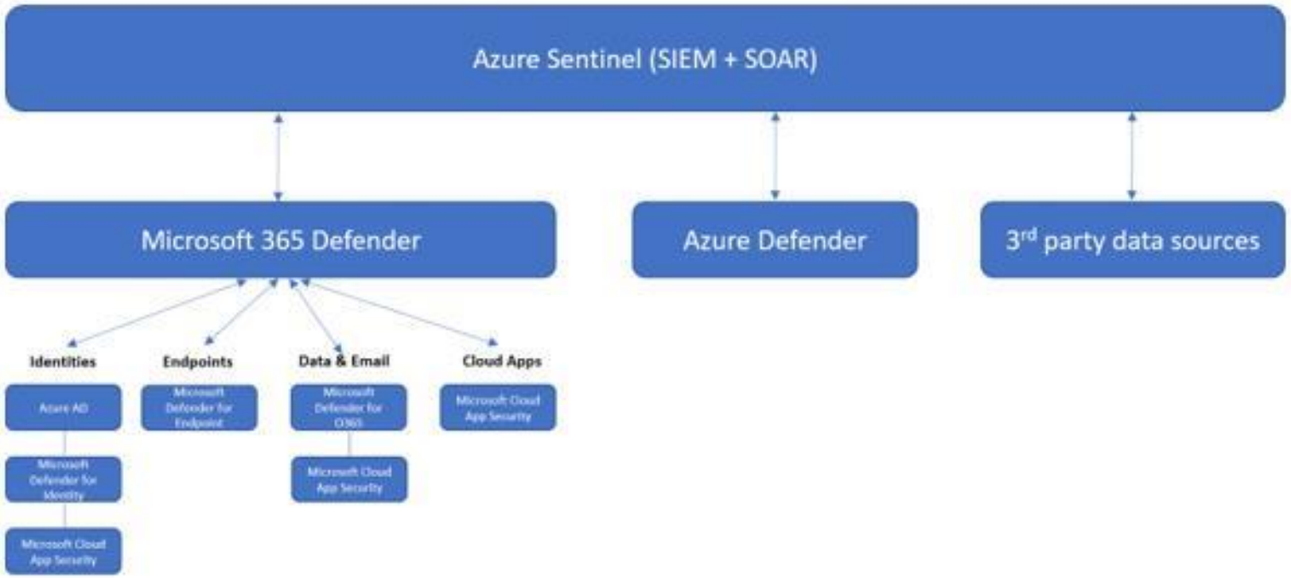
Globetam Continuous Security Improvement is a service that is updated and optimized automaticaly, based on the more than 6 billion securitysignals (users, endpoints, etc.) that Microsoft analyze every day in their operationcenters

Globeteams Continuous Security Improvement

GLOBETEAMS CONTINUOUS SECURITY IMPROVEMENT IS BASED ON MICROSOFT 365 E5, MICROSOFT SECURITY CENTER AND AZURE SENTINEL

Tools in Globeteams Continuous Security Improvement

- Azure Sentinel
- Azure Defender
- Microsoft 365 Security Center (Microsoft 365 Defender)
  - Defender for Identities
  - Defender for Endpoints
  - Defender for Office365
  - Microsoft Cloud App security



The platform uses the Microsoft Security components that the customer has already bought or implemented.

Ideally Azure Sentinel is the entry portal to all information and the monitoring platform that collects security related data from all of the tools in the service.

Globeteam Continuous Security Improvement – Managed Security Services Cycle

PROTECT

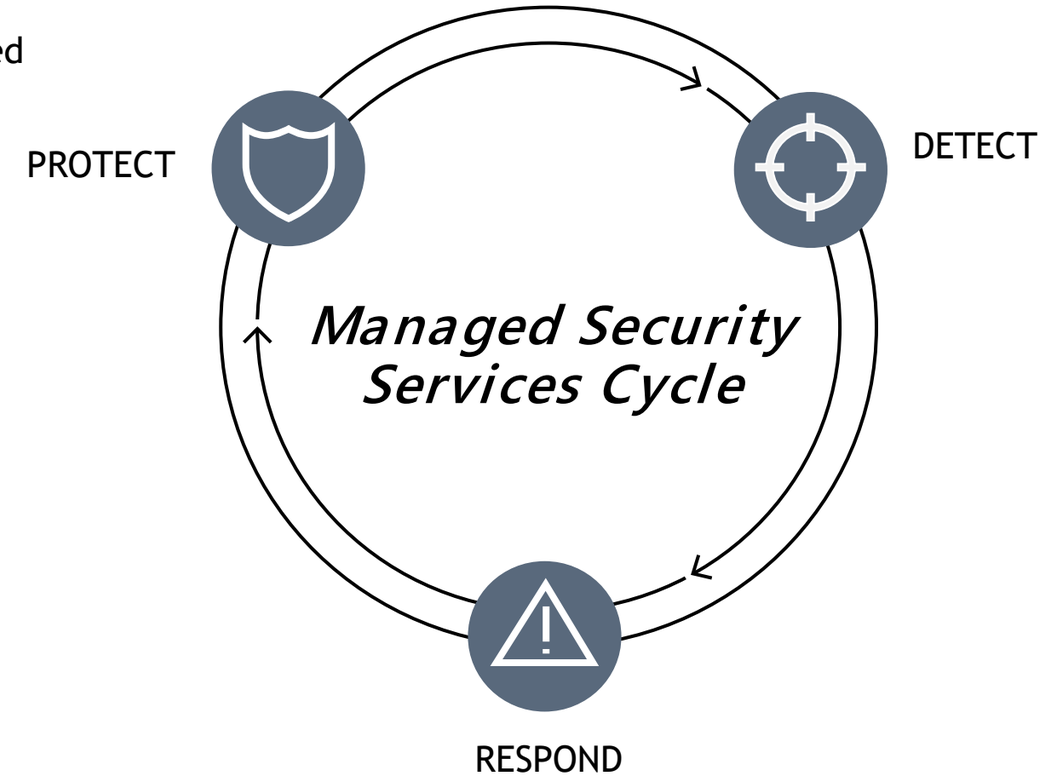
- We proactively protect by leveraging Microsoft services and tools in cooperation with our customers
- We monitor the environment and provides a bi-weekly report over proposed changes and current security issues.
- In joint effort with threat intelligence from Microsoft and data from our customers, we provide an insight into current and emerging threats

DETECT

- We use standard Microsoft 365 E5, Azure services and loganalytics to proactively detect threath, anormalities and behavioral changes together with the customers existing security operation.

RESPOND

- We use built-in AI and automation tools from Microsoft 365 to respond to alarms/incidents
- We proactively respond with increased awareness to anormalities, increased severities that arises within the security community, based on Services cycle

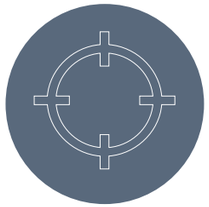


Globeteam Continuous Security Improvement – Managed Security Services Cycle

PROTECT

- Protection and continuous security optimization, including:
  - Utilize Microsoft Intelligent Security Graph and combine with data from customers Security Center
  - Optimization of dashboards and report for customer stakeholders
  - Suggest adjustment/changes on security measures
  - Mitigate alert overload, reduce false positives

OPTIONAL - Initiate campaigns, jointly with customer, to increase security and user awareness on security measures (phising-campaign, bruteforce attacks, etc.)



DETECT

- Detection and continuous security optimization, including:
  - Analyze collected logs, dashboards, reports for anormalities (beyond Microsoft suggestions if applicable and/or relevant)
  - Assess and evaluate security related actions suggested by Microsoft and/or the customers SOC vendor
  - Leverage security data from Security Center and Security Graph to proactively Detect and respond to threats, anomalities and/or changes
  - Report bi-weekly to customer on issues identified, anormalities and suggest security initiatives

RESPOND

- Respond to security matters, including:
  - Proactively responce to security attacks, incidents, severities, threats, anormalities and breaches aligned with the customer
    - Can be combined with a Response agreement that gives access to highly skilled consultants with an SLA for response
  - Act and evaluate on security related measures and issues suggested by Microsoft and/or SOC team

OPTIONAL - Proactively respond to major incidents – jointly with the customer and their SOC team.

Globeteam Continuous Security Improvement – Managed in customer environment

We are in this together

”Continous Security Improvement” is a service by Globeteam in co-operation with the customer. This means that customer can have an active role in operation and get knowledge insight from the solution.

Full transparency and flexible operation mode

”Continous Security Improvement” is based on the customers existing environment, which means no data are moved out of the customers environment. This ensures full transparency and flexibility for the customer to take over more operation over time.

Leveraging existing Microsoft software

”Continous Security Improvement” leverages the customers existing Microsoft licenses and no extra license cost are required. This ensures the highest value of the existing Microsoft solution and ensure a low TCO for the solution.

We start Baselining the specific customer solution

OUR KNOWLEDGE WORKING WITHIN THE SECURITY INDUSTRY, HAS TOUGHT US THAT CUSTOMERS NEEDS FOR REPORTING AND THEIR OPERATIONAL SETUP AND NEEDS ARE DIFFERENT. THAT'S WHY WE START WITH A BASELINE PERIOD.

01

Enable connectors and filter un-relevant information

02

Creating baseline for ”non-severe” alarms and incidents

03

Response workflow for 10 most frequent incidents suitable for self-remediation

04

Creating reporting format and dashboards for stakeholders

Continuous Security Improvement Economy

Continuous Security Improvement - Economy

Task	Implementation price	Monthly price	Comments
Implement Azure Sentinel, Azure Security center and Microsoft 365 security components	xx.xxx,-		Estimate from workshops
Initial Baselining (2 month)	xx.xxx,-		
Continuous Security Improvement Service (3 month cyclus – re-evaluate)		*xx.xxx,-	The price and service will be re-evaluated every 6 month, to potentially harvest on the improvements from the last period.
C-level advisory		xx.xxx,-	optional

* Estimated price – will depend on baselining decisions.

All prices are in DKR, excl. VAT

Globeteams Continuous Security Improvement - C-level advisory

Monthly reporting to c-level

Monthly meeting with C-level to advise customer about the overall security picture and where the customer can proactively invest to increase their IT security resilience

GLOBETEAM

GLOBETEAM A/S
Telefon +45 70 26 29 70
info@globeteam.com
www.globeteam.com

VIRUM
Virumgårdsvej 17A
DK-2830 Virum

VEJLE
Innovations Allé 3
DK-7100 Vejle