AUTOMIZE®

*We bring people, business and technology closer together*

Gold Microsoft Partner

Microsoft

## AUTOMIZE MANAGED

# Security Operation Center


Birkemosevej 7c
DK-6000 Kolding

Høje Taastrup Blvd. 52-58
DK-2630 Taastrup

info@automize.dk
+45 7171 5353

automize.dk


servicenow Bronze Technology Partner

AUTOMIZE

*We bring people, business and technology closer together*

Gold Microsoft Partner

Microsoft

AUTOMIZE MANAGED

# Security Operation Center

## What is Managed SOC?

Managed SOC is the allocation of Dedicated resources for Identification (Detection) and Response to security threats in your IT environment. Which can be purchased for one or more security products from Microsoft. Furthermore, it gives your company clear agreements about actions in emergency situations.

With Automize managed security operations, you always have a professional partner to handle your company's IT security. Automize ensures that you get the full value of the Microsoft Defender products you have already paid for. If you use Defender services, we consolidate the alarms in Microsoft Sentinel, so that you not only have the products activated, but we take responsibility for the important alarms these products generate.

Our service covers services in Azure, Microsoft-365, Onprem, PCs and mobile phones so that you are secured in every possible way. Your IT security is never more secure than the weakest links.

24 hours a day, Automize delivers rapid and documented response to identified security threats.

Birkemosevej 7c
DK-6000 Kolding

Høje Taastrup Blvd. 52-58
DK-2630 Taastrup

info@automize.dk
+45 7171 5353

automize.dk

servicenow Bronze Technology Partner

AUTOMIZE

*We bring people, business and technology closer together*

Gold Microsoft Partner

Microsoft

AUTOMIZE MANAGED

# Security Operation Center

## Why should you switch to Managed SOC?

### PURPOSE

Rapid and documented identification and response to security threats.

### SERVICES

- Better technical support
- You will achieve a higher level of IT security in the areas that Automize are allowed to operate.
- 24/7 SLA so that you always are covered regardless of the time of day or week.
- Price per. unit, Enterprise service for SMB customers
- Opportunity to purchase resources to repair damage following cyber attacks

## How does Managed SOC Benefit You?

### PURPOSE

Automize makes the resources and knowledge available, no reliance on internal IT employees.

### SERVICES

- Minimize the risk of damage from cyber-attacks (Everyone gets attacked).
- Certified IT security experts at your disposal.
- Implementation of new and updated measurement points, which can contribute to stability and better reporting.
- Quick and documented identification and response to security threats.
- Security products, consolidation in Microsoft Sentinel and security incidents are handled in our central ITSM system from ServiceNow.

Birkemosevej 7c
DK-6000 Kolding

Høje Taastrup Blvd. 52-58
DK-2630 Taastrup

info@automize.dk
+45 7171 5353

automize.dk

servicenow Bronze Technology Partner

AUTOMIZE

*We bring people, business and technology closer together*

Gold Microsoft Partner

Microsoft

AUTOMIZE MANAGED

# Security Operation Center

## When is Managed SOC relevant to you?

- Regardless of the size of your business, Managed SOC is relevant to you. If you have to provide IT security yourself, it will be more expensive and your internal security team will be assigned tasks outside their area, which wastes valuable resources. At Automize, we are experts in IT security and focus exclusively on this aspect of your business.
- Managed SOC is not industry specific, IT security should always be a priority for any company if you want to have an overview of your IT security situation without dedicating internal resources.
- Automize offers Managed SOC on components and systems that cover Azure, Microsoft-365, Onprem and Multi Cloud.

## How can Automize help your business?

- Automize are experts in this area and have dedicated IT security expert consultants ready to monitor and operate your IT security so you can focus on the tasks that add value to your business.
- Automize have many years of experience with IT security and cloud products / services, we are also certified IT security experts and are at your disposal when you need it.
- By letting Automize take care of your IT security, you will have the opportunity to relocate your internal IT resources to be able to solve tasks that provide direct value for your company.

Birkemosevej 7c
DK-6000 Kolding

Høje Taastrup Blvd. 52-58
DK-2630 Taastrup

info@automize.dk
+45 7171 5353

automize.dk

servicenow Bronze Technology Partner

AUTOMIZE

*We bring people, business and technology closer together*

Gold Microsoft Partner

Microsoft

AUTOMIZE MANAGED

# Security Operation Center

## Alert-based SOC

### PURPOSE

Handling security incident alarms from a given service.

### SERVICES

- Detection of security incidents (**Detect in NIST security framework**) from the following reference **list**.
- Creation of security incident based on the incident process described in Processes and procedures - incident management. Incident priority is defined, based on the severity of the incident in the individual threat management service.
- Responds to the identified security incident. (Respond in NIST security framework)
  *- Analyzes the identified incident so that scope can be assessed and appropriate mitigation can be performed.*
  *- Mitigates the incident based on agreed powers.*
  *- Escalation to customer security officers.*
- Configuration and maintenance of integration between the threat management services selected in the agreement and the Supplier's serviceNow.

## Customer obligations

- The customer ensures that the supplier has access to managed systems.
- Licenses for Thread management software purchased on components.
- Definition of the Supplier's powers in connection with security incidents.
- Recovery activities in connection with damage from incidents with possible involvement of the supplier.

*The supplier can not be held responsible for changes made by the threat management service provider which affect the integration.*

Birkemosevej 7c
DK-6000 Kolding

Høje Taastrup Blvd. 52-58
DK-2630 Taastrup

info@automize.dk
+45 7171 5353

automize.dk

servicenow Bronze Technology Partner

AUTOMIZE

*We bring people, business and technology closer together*

Gold Microsoft Partner

Microsoft

AUTOMIZE MANAGED

# Security Operation Center

| | | ServiceDesk | Onboarding | Alert based SOC |
|---|---|---|---|---|
| **DATACENTER SERVICES** | | | | |
| 1 | Microsoft Defender for servers | x | x | x |
| 2 | Microsoft Defender for SQL | x | x | x |
| 3 | Microsoft Defender for App Service | x | x | x |
| 4 | Microsoft Defender for Storage | x | x | x |
| 5 | Microsoft Defender for Kubernetes | x | x | x |
| 6 | Microsoft Defender for container registries | x | x | x |
| 7 | Microsoft Defender for Key Vault* | x | x | x |
| 8 | Microsoft Defender for Resource Manager | x | x | x |
| 9 | Microsoft Defender for DNS | x | x | x |
| 10 | Microsoft Defender for open-source relational databases | x | x | x |
| 11 | Azure firewall - Threat intelligence | x | x | x |
| 12 | Azure network watcher - Traffic Analytics (NSGs) | x | x | x |
| 13 | Microsoft Defender for IoT | x | x | x |
| **MICROSOFT 365 SERVICES** | | | | |
| 14 | Microsoft Defender for Endpoint | x | x | x |
| 15 | Microsoft Defender for Office | x | x | x |
| 16 | Microsoft Defender for Identity | x | x | x |
| 17 | Microsoft Defender for Cloud Apps | x | x | x |
| 18 | Azure AD | x | x | x |
| 19 | Azure Tenant | x | x | x |

Birkemosevej 7c
DK-6000 Kolding

Høje Taastrup Blvd. 52-58
DK-2630 Taastrup

info@automize.dk
+45 7171 5353

automize.dk

servicenow Bronze Technology Partner

AUTOMIZE

*We bring people, business and technology closer together*

Gold Microsoft Partner

Microsoft

# Choose the right partner

*Security in a new context with Microsoft Sentinel and Defender as key players, the same solution for small businesses as for large ones. The hackers do not differentiate on size.*

SecOps teams are constantly hammered with alarms, if you had to handle all these alarms yourself, you would not have time for anything else. Microsoft Sentinel enables us to easily collect data across your entire organization, from devices, to users, to applications located in any Cloud solution.

Using artificial intelligence, we quickly identify real threats and since it is based on the SaaS model, unlike traditional SIEM systems, one does not have to think about setup, maintenance and scaling.

**Click here to read more about Automize, as a provider of Security Operations Center!**

Businesses are bombarded with security threats daily. In the past, only large companies prioritized IT security, but with the large degree of automation, virtually all companies have to prioritize IT security as everyone is at risk of e.g. ransomware, where one's data is taken hostage and only released against payment.

At Automize, we can either actively contribute to your current security setup and deliver data to your SecOps team or we can take over the function 100%. Your business only needs to focus on your core areas and what it is set in the world to do. Our contribution will be to make sure your IT platform runs securely and by proactively making sure you are ready for the threats of the future.

Want to know more about Managed SOC and IT security with Automize, you can contact us here.

Birkemosevej 7c
DK-6000 Kolding

Høje Taastrup Blvd. 52-58
DK-2630 Taastrup

info@automize.dk
+45 7171 5353

automize.dk

servicenow Bronze Technology Partner