

Ontinue + A1

# Nonstop SecOps mit Microsoft Teams

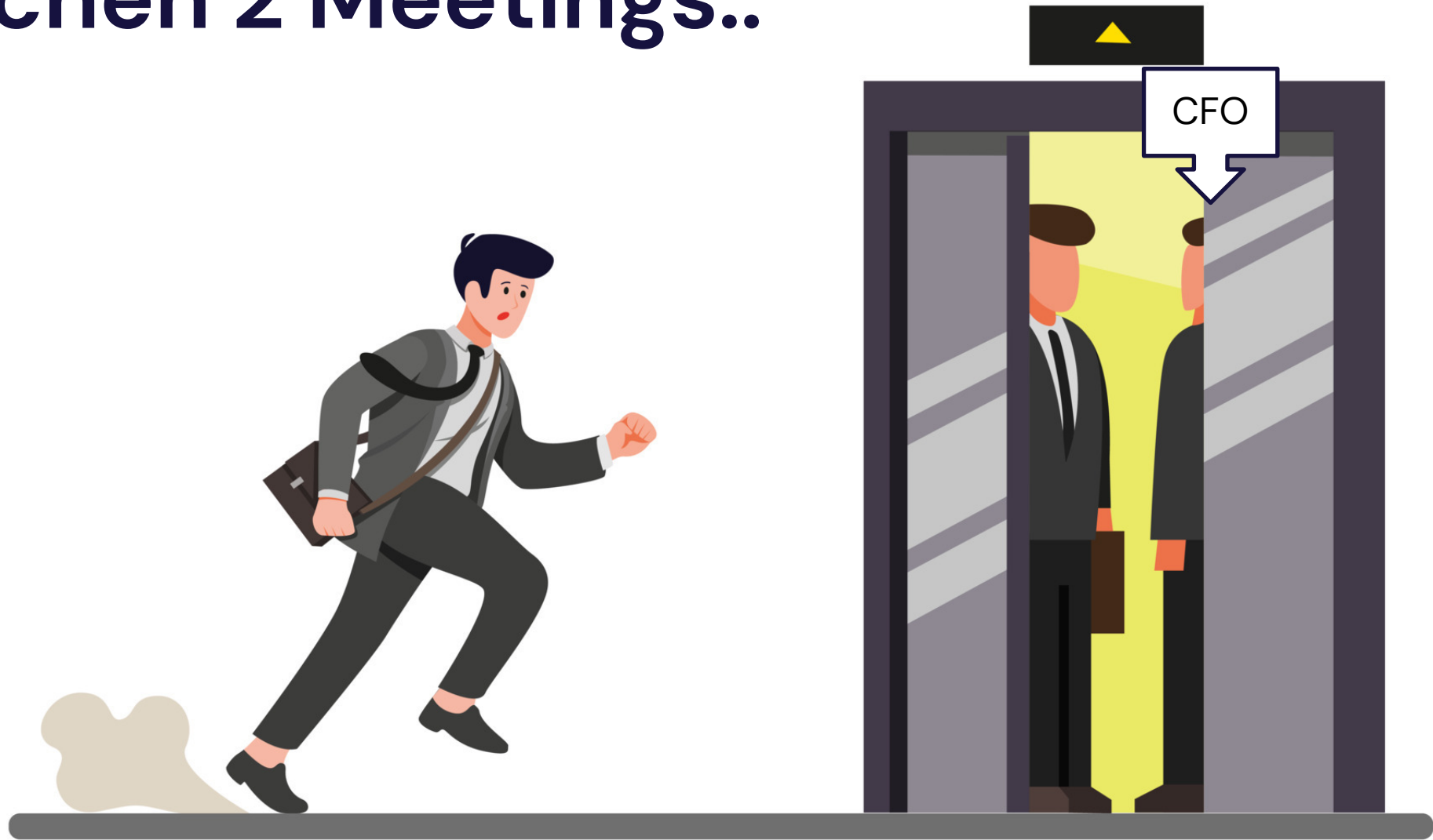


**Andrina Brun**  
Senior Cybersecurity Specialist



**Thierry Aubry**  
Senior Sales Executive

# Zwischen 2 Meetings..





## Ontinue Collaboration

Posts

ION Automate

2 more



**ION Bot** 4:42:10 PM

I am your personal assistant for understanding and optimizing your ION service. Enter your request in the prompt below.



**Anne Kirk** 4:42:20 PM

What are my sentinel costs?



**ION Bot** 4:42:31 PM

Your cost in the past month: 23,593.1 CHF.

Top Solutions in terms of cost:

- LogManagement: 18,903.4 CHF (80.1%)
- Security: 2,967.5 CHF (12.6%)
- AzureSentinel: 1,722.2 CHF (7.3%)

Top Data Types in terms of cost:

- CustomLog\_Firewall (LogManagement): 8,233.5 CHF (34.9%)
- CustomLog\_DnsInspection (LogManagement): 6,693.7 CHF (28.4%)
- Event (LogManagement): 3,905.8 CHF (16.6%)
- SecurityEvent (Security): 2,880.5 CHF (12.2%)
- DeviceProcessEvents (AzureSentinel): 1,202.9 CHF (5.1%)









ION Demo via Power Automate 16:41

## ION Cyber Defense Centre

Incident Title	Coffeext malware was prevented on one endpoint
Incident ID	<a href="#">1073</a>
Incident Severity	High
Incident Creation Time	06/13/2023 14:41:16
Security Product	Microsoft Sentinel
Entity Enrichment	<a href="#">File</a> 86fc70d24f79a34c46ef66112ef4756639fcad2f2d7288e0eeb0448ffab90428: Malicious

[View Full Entities](#)

- Block File Hash: 86FC70D24F79A34C46EF66112EF47566...
- Isolate Machine: Ontinue-WS-AA
- Restrict App Execution: Ontinue-WS-AA

Incident Closure ▼

Enter classification comment if incident closed

ION ENGAGE

[Submit](#)

[Dismiss](#)

Submit

# ION | Technologie



ION for Microsoft Teams

ION Defender Workbench

ION Data Science Mesh

ION Automate



Microsoft Sentinel



Microsoft Defender - Extended Detection and Response (XDR)

DEFENDER FOR CLOUD

Servers & VMs | Containers | Azure App Service | Network Traffic | SQL | IoT & OT

MICROSOFT 365 DEFENDER

Defender for Endpoint | Defender for Office 365 | Defender for Identity  
Azure AD Identity Protection | Defender for Cloud Apps

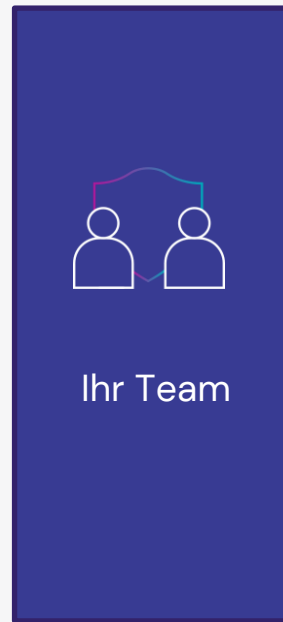
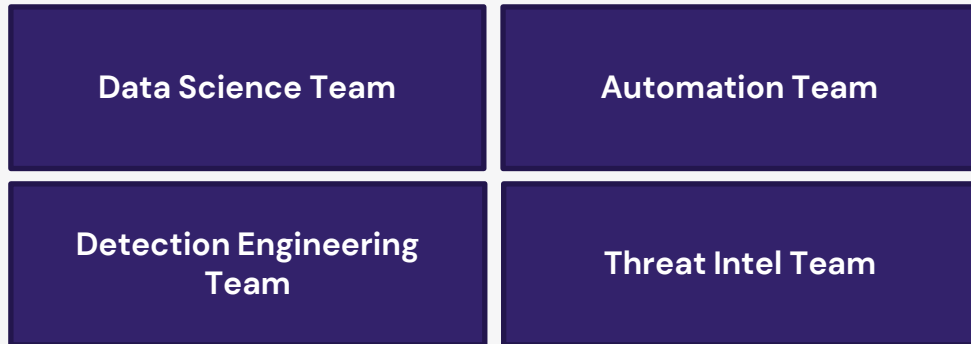
MULTI-CLOUD | MULTI-DEVICE

LEGACY CONTROLS

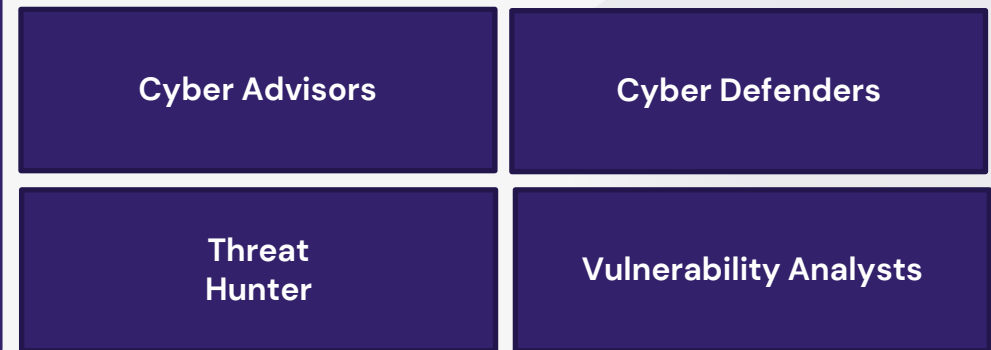
# ION | Menschen



Ontinue-Teams unterstützen  
SecOps mit Intelligence,  
Automatisierung und Technik



Für den täglichen  
Sicherheitsbetrieb sind die  
Ontinue-Teams verantwortlich



ION Cyber Defense Center





## Prevent

- Priorisieren und beraten bei Änderungen:
- Patching
- Konfiguration
- Prozess

## Detect

- Entdecken/Untersuchen/Priorisieren
- Warnungen und Signale von Microsoft übernehmen
- Bedrohungsnachrichten-Feeds kuratieren

## Assess

- Ihre Umgebung
- Schwachstellen
- Sicheres Ergebnis
- Vorfallshistorie
- Threat Hunting

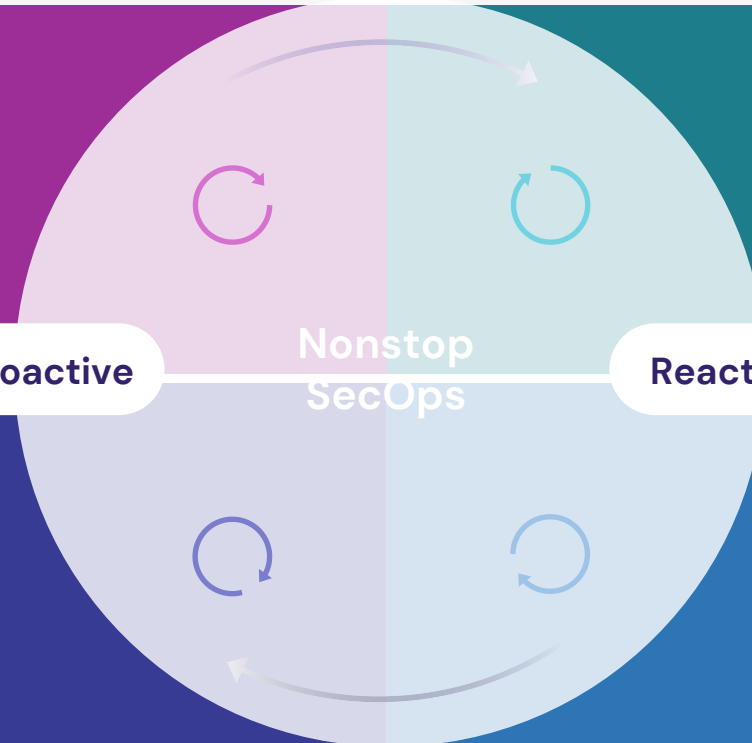
## Respond

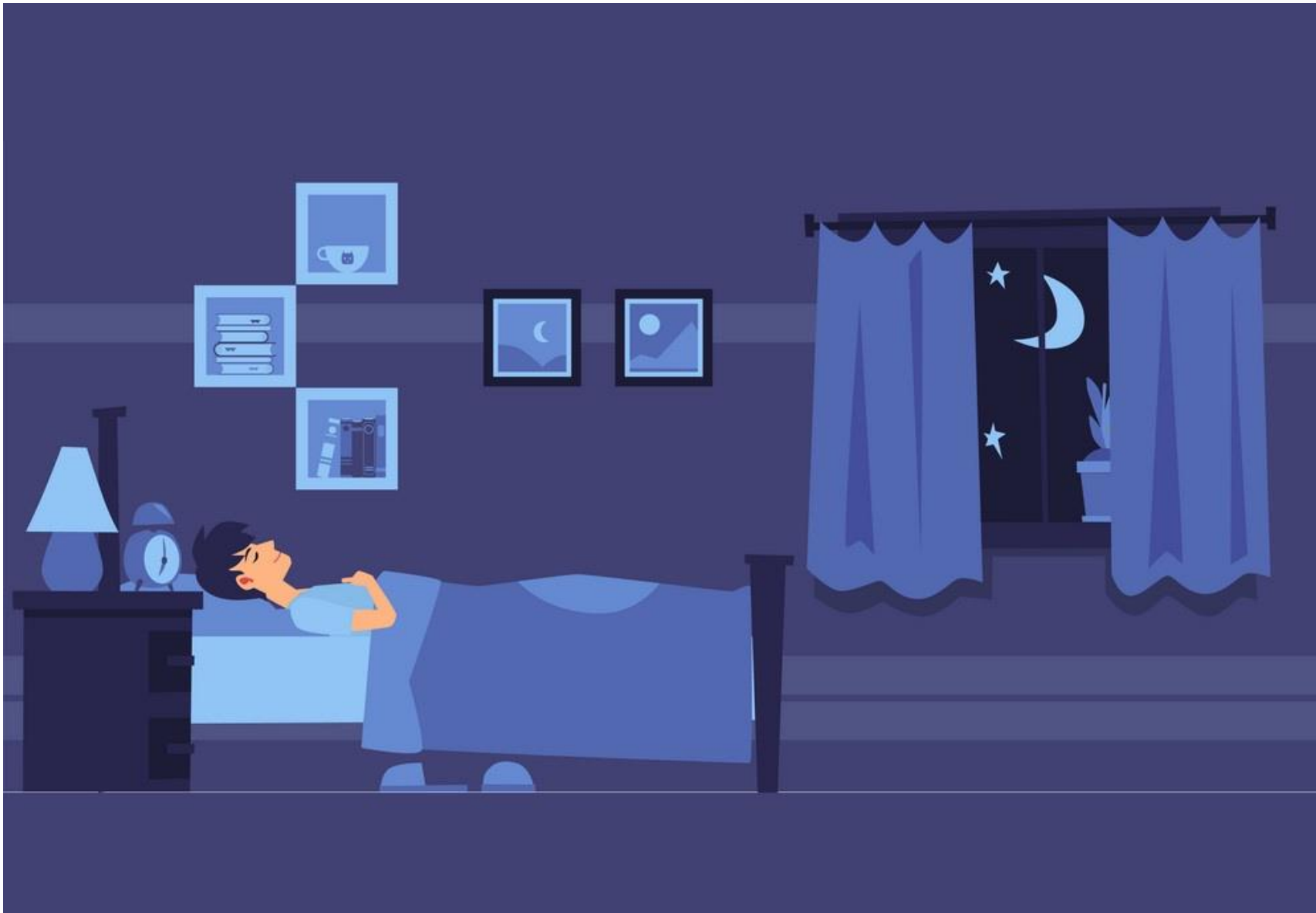
- Vorfälle priorisieren
- Antworten priorisieren
- Zusammenarbeiten
- Abhilfe schaffen

Proactive

Nonstop  
SecOps

Reactive





**Live Demo? Fragen?  
Kontaktieren Sie uns!**

Ontinue + **A1**