u'need'security

Cloud Compliance in verinice

M365 Compliance Manager

... sonst nichts.

(ISC)² CODE OF ETHICS

UNeedSecurity wird als Firma nach den Werten des (ISC)² Code Of Ethics geführt. Der Wertekanon besteht aus folgenden, grundlegenden Auffassungen:

Der Schutz der Gesellschaft, des Gemeinwohls, des notwendigen öffentlichen Vertrauens und der Infrastruktur ist unser erstes Ziel.

Dies wird durch ehrenhaftes, ehrliches, gerechtes, verantwortungsbewusstes Handeln auf legaler Grundlage erreicht.

Im Alltag ist es unsere Pflicht, sorgfältige und kompetente Dienstleistungen für die Auftraggeber zu erbringen,

Wir bringen den Berufsstand voran und schützen seinen Ruf.

Christian Breitenstrom

Z80 Hardware 1986, Informatik 1994. Entwicklung von Point of Sales Anwendungen für Deichmann (C++), später Internet Anwendungen in Java, Python, Eclipse
Security Engineer
IT-SiBe, Auditor

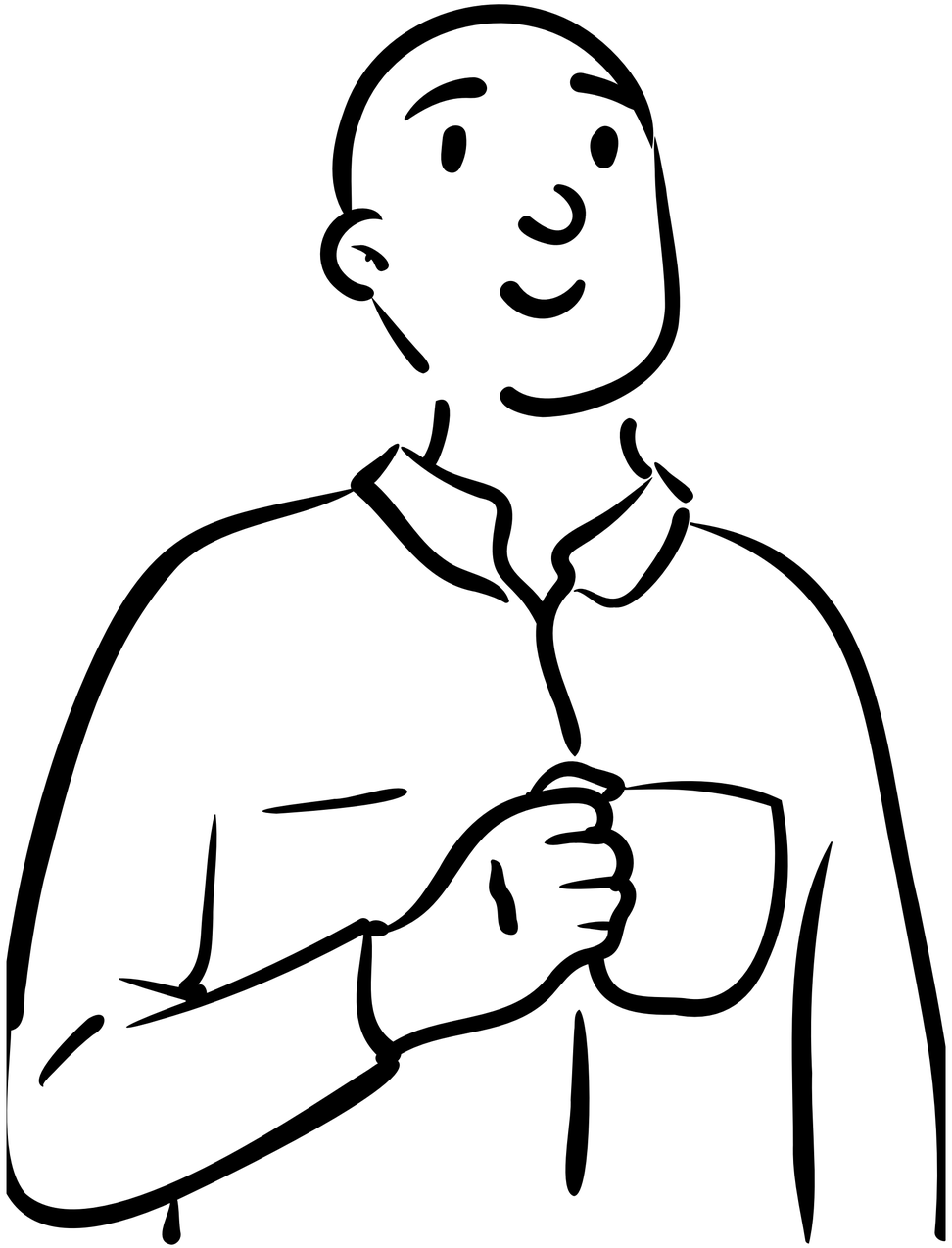
UNeedSecurity GmbH

Managed Security Service Provider

Public Sector, IT Dienstleister, Finance, Energy (KRITIS)

verinice

User seit ~2011
Partner seit 2020
(Entwickler) seit 2022



Agenda

1 **Gegenstand**

2 **Beitrag zur verinice.XP demo or die**

11 **C5 Katalog,**
Compliance am Beispiel von M365

12 **Implementierungsdetails &**
DANKSAGUNG

Zielgruppe(n)

Sie nutzen Cloud Services für Ihre Geschäftsprozesse und...

Compliance

Sie unterliegen Compliance Kriterien z.B. der DSGVO, der BAFIN und der KRITIS-Verordung.

vorhandenes Sicherheitsmanagement

Sie haben ein ausgebautes Sicherheitsmangement auf Basis einer verinice Instanz. Sie haben keine Angst vor Automatisierung, weil Sie so Ihre tägliche Arbeitslast im Griff haben.

Kostensteuerung

Ihre Geschäftsprozesse dulden keine Verletzung der Sicherheitsziele. Sie arbeiten mit Metriken, um Ihre Risiken informiert und kostenbewusst zu minimieren.

Kontinuierliche Verbesserung

Sie haben die Herausforderung aktzeptiert, ständig besser werden zu müssen, um mit den wachsenden Gefahren Schritt halten zu können.

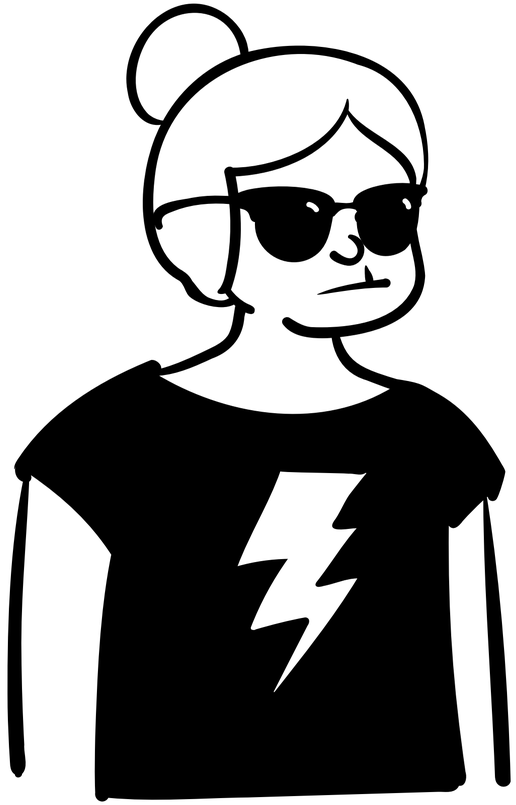
Gegenstand

Transparenz

Institutionen benötigen eine solide Grundlage um einen wirksamen Schutz gegen Cyberangriffe zu erreichen

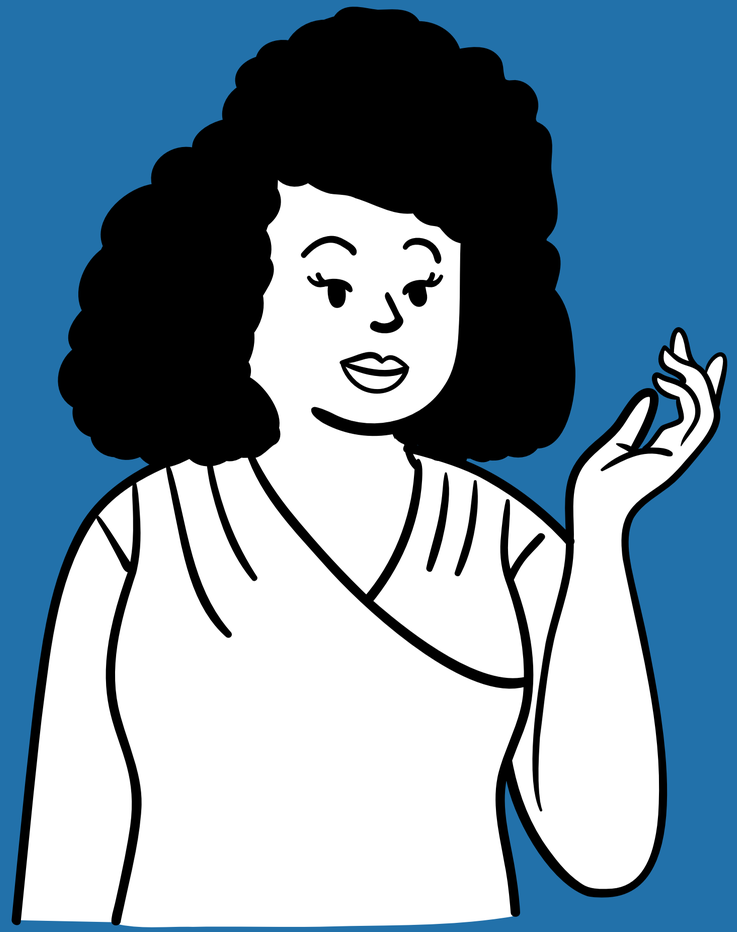
Automatisierung

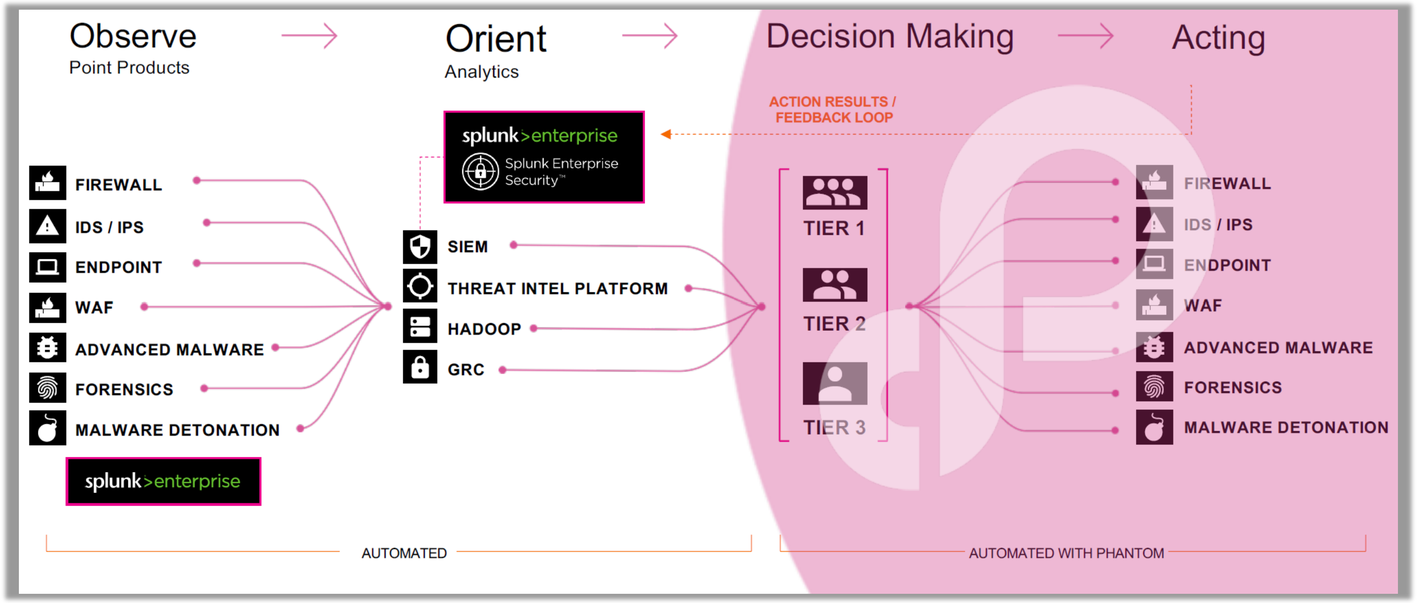
Effizienz durch regelbasierte Automatisierung
Minimierung der Dokumentation



Stärkung der Datenschutzbeauftragten
Stärkung des CISO

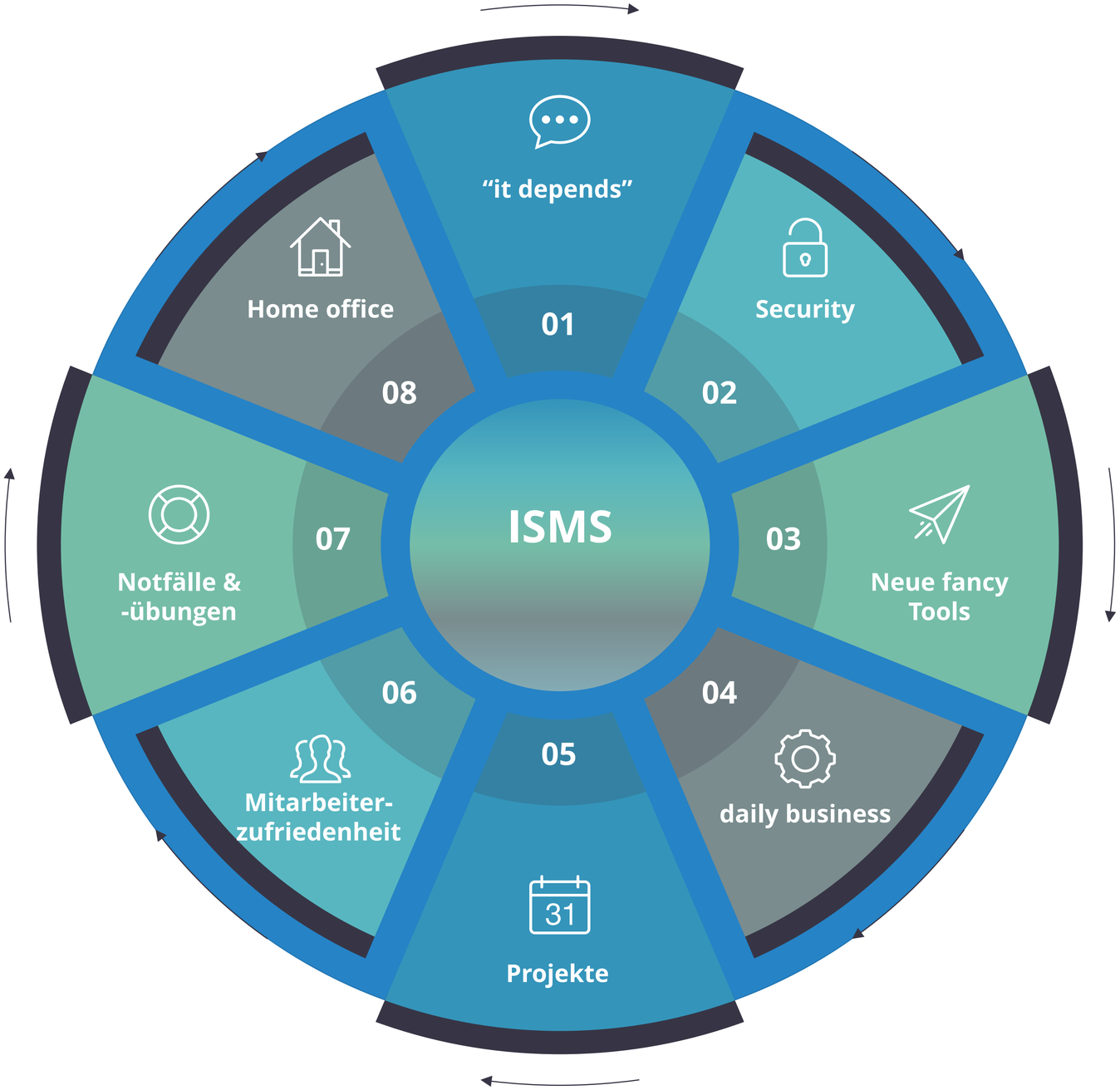
Kommunikationshilfen der Cloud Anbieter nutzen
Erprobte Metriken als Basis für kontinuierliche Verbesserung





Quelle: splunk

On premise vs. (managed) clouds



verinice als Steuerungs-instrument

Open Source Gedanke nutzen

Idee: über die vorhandenen, eher konstanten Cloud-Schnittstellen werden Metriken abgeholt, die in das tägliche Risikobarometer einfließen.

Idee: über die festgestellten Optimierungsempfehlungen wird das Sicherheitsniveau rechtzeitig angehoben, bevor es zu Ausfällen und Sicherheitsvorfällen kommt.

Let's go!

demo or die

Eclipse RCP mit Zugriff auf Microsoft Graph API per Powershell
(alternative Cloud Services möglich)

Transparenz

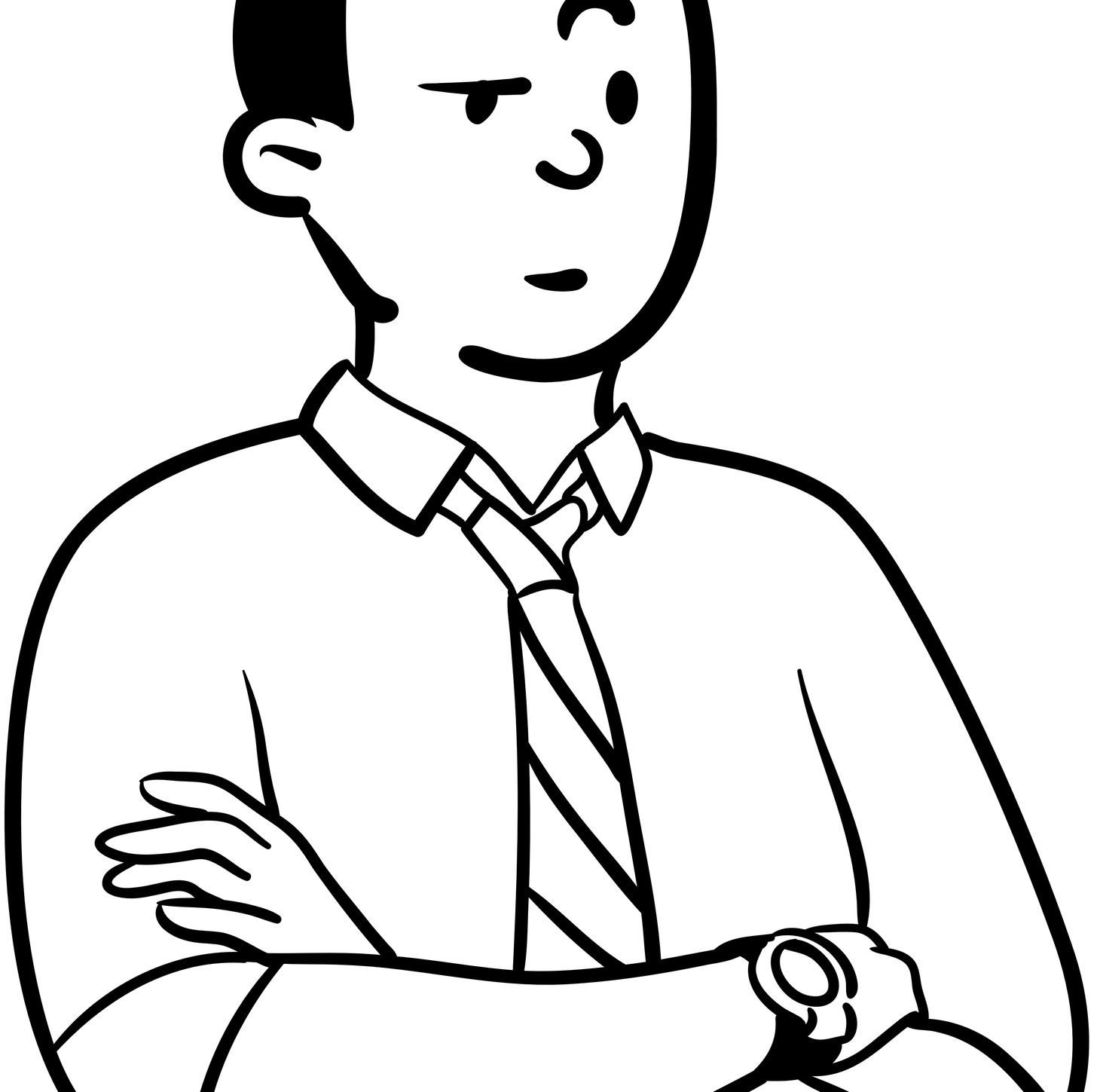
IST-Zustand kann jederzeit abgefragt werden
Empfehlungen für IT auf Basis von best practices
Alerts & Incidents

Automatisierung

Effizienz durch regelbasierte
Automatisierung

Stärkung der Datenschutzbeauftragten
Stärkung des CISO

Kommunikationshilfen der Cloud Anbieter nutzen,
über Reifegrade und Risikobarometer argumentieren



Inhalte des C5 Kataloges

Microsoft

Microsoft Corporation—Office 365 Germany

Report on Controls at Service Organization Relevant to Security, Availability, Processing Integrity, and Confidentiality (SOC 2), and Cloud Computing Compliance Controls Catalogue (C5)

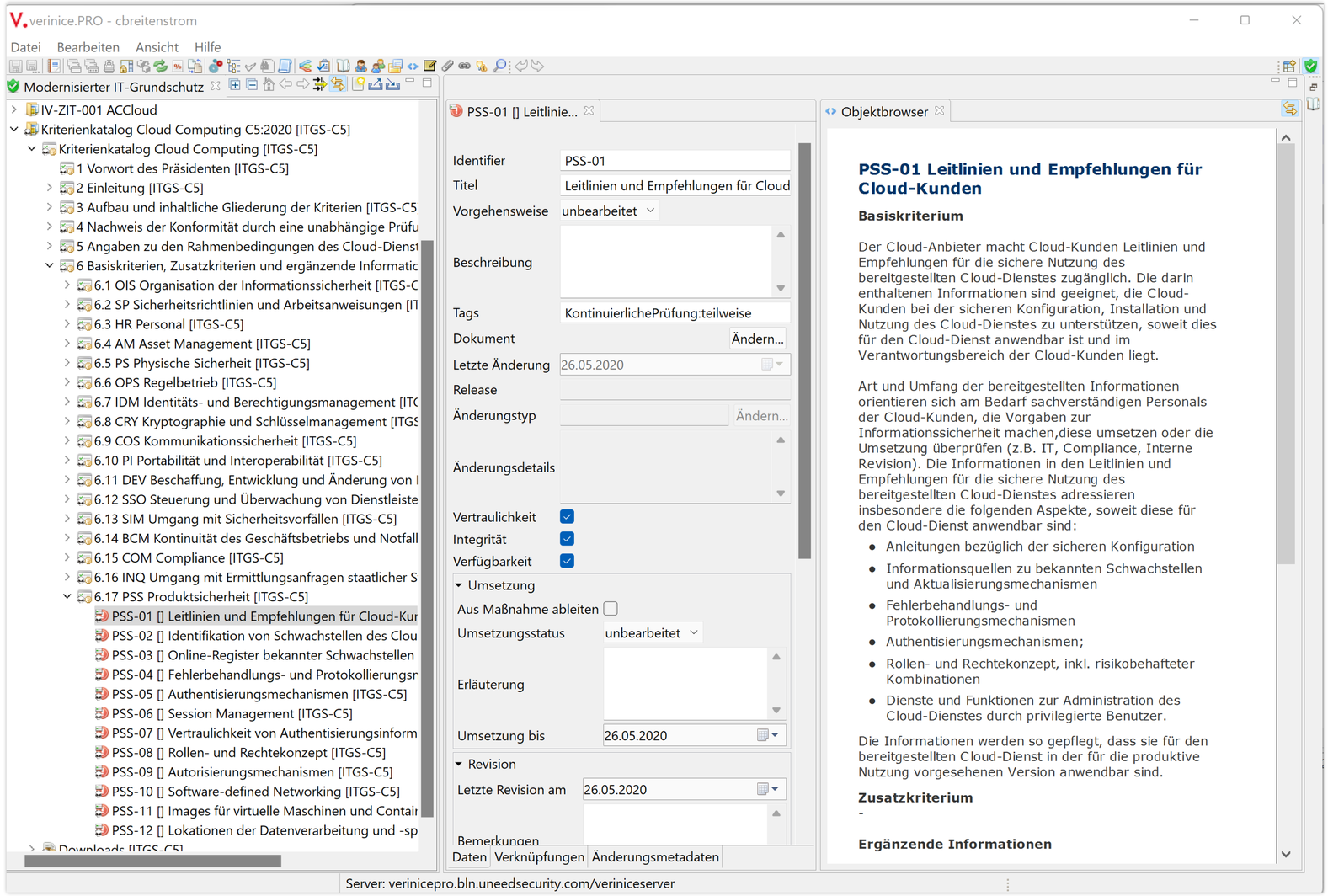
October 1, 2019, through September 30, 2020

Gegenstand sind Cloud Service Anbieter

<u>Grundlage für die Anforderungen an Cloud-Anbieter</u>

Kontrollpflicht über Zertifizierungen

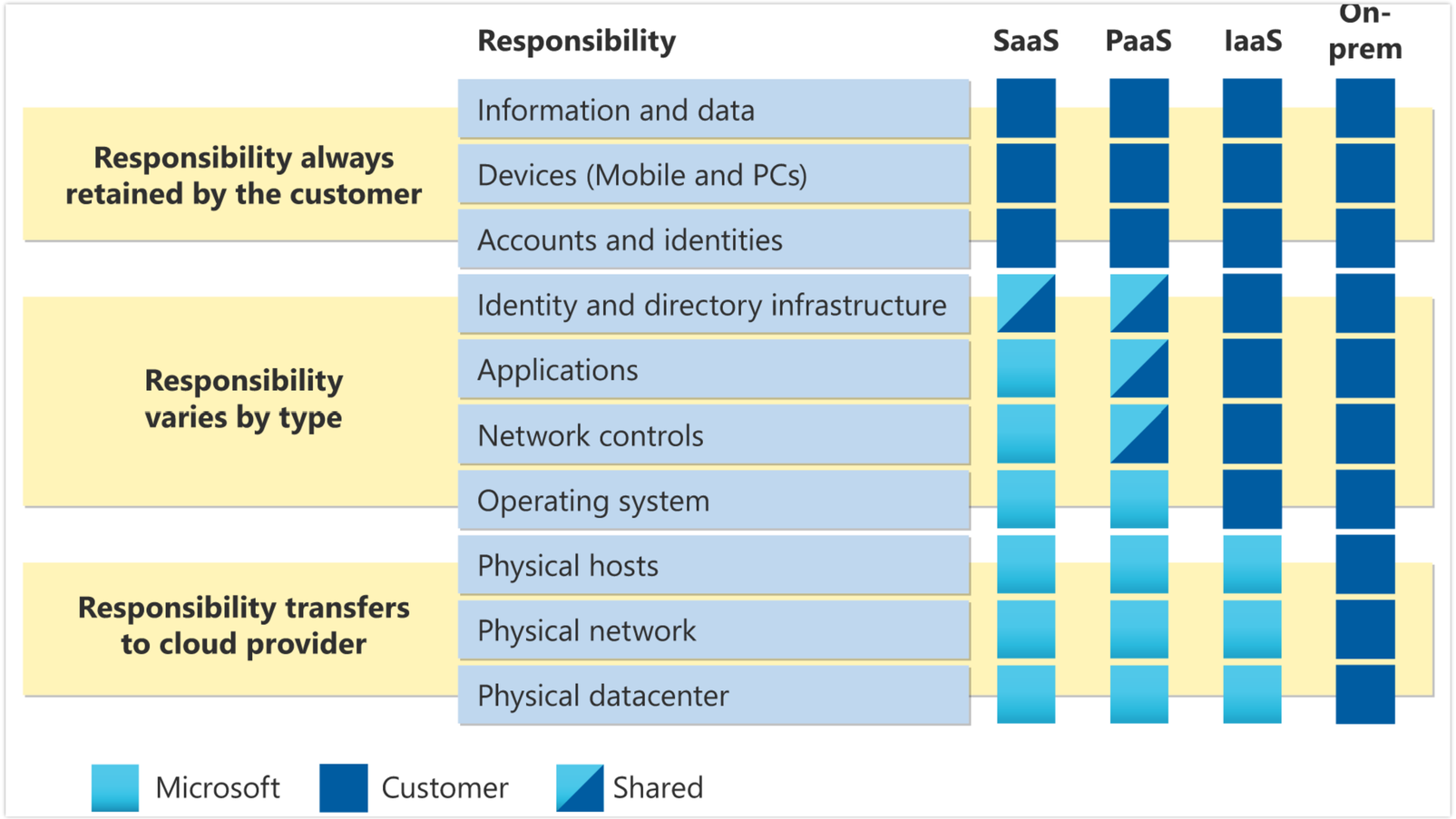
Nutzung der EU Standard Contracts als Vorlage



Shared Responsibility

PSS-01 Leitlinien und Empfehlungen für Cloud-Kunden
Basiskriterium

Der Cloud-Anbieter macht Cloud-Kunden Leitlinien und Empfehlungen für die sichere Nutzung des bereitgestellten Cloud-Dienstes zugänglich. Die darin enthaltenen Informationen sind geeignet, die Cloud-Kunden bei der sicheren Konfiguration, Installation und Nutzung des Cloud-Dienstes zu unterstützen, soweit dies für den Cloud-Dienst anwendbar ist und im Verantwortungsbereich der Cloud-Kunden liegt.



Kontroll- und Steuerungsmöglichkeiten

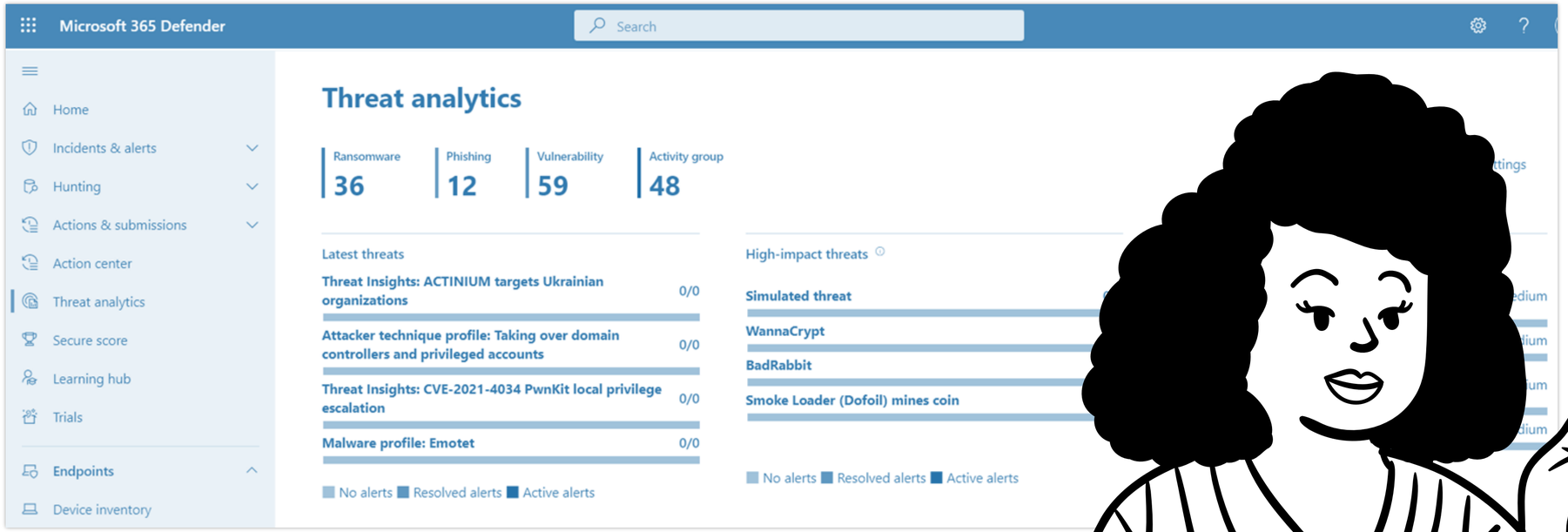
Alerts

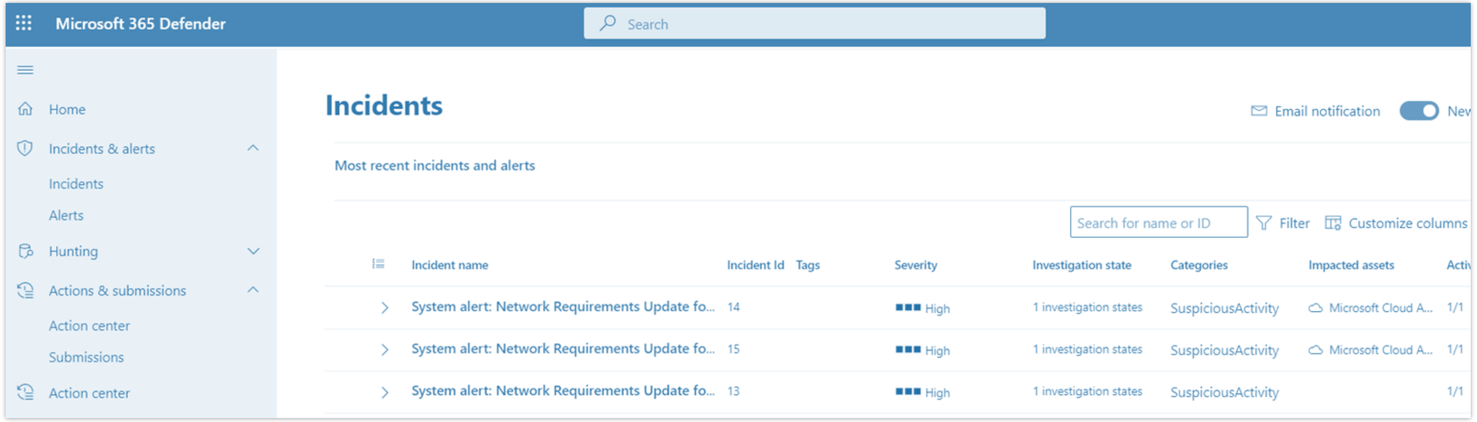
Schwachstellen

Optimierungsempfehlungen

Aufgaben

Risikoakzeptanz





die Implementierung

Open Source … kompiliert tatsächlich! https://forum.verinice.com/t/so-klappt-die-kompilierung-der-1-23-0/1577

PoC Sourcen in https://github.com/cb13579/verinice.git Branch M365-PoC

Build Prozess (mvn) ca. 6 min auf ThinkPad P50

Ecplipse – mvn plugin hat immer noch Schwierigkeiten

Optionen für die Anbindung an Azure

Microsoft: Azure Toolkit for Eclipse? Zeitrahmen zu eng.

Authentifizierung MSAL -> registrierte App

Datenmodellierung

Datenmodell nicht erweitert worden, M365 Status wird als „Note“ abgespeichert

Client

Zugriff auf ISMS Team eingeschränkt, WebOberfläche bei VEO ist an der Zeit.
Anbindung an SIEM Dashboards wäre hilfreich

Danksagung

Isaac Newton famously observed that “if I have seen further it is by standing on the shoulders of giants.”

Firma sernet ☺

https://adoptium.net/ - OpenJDK Binaries

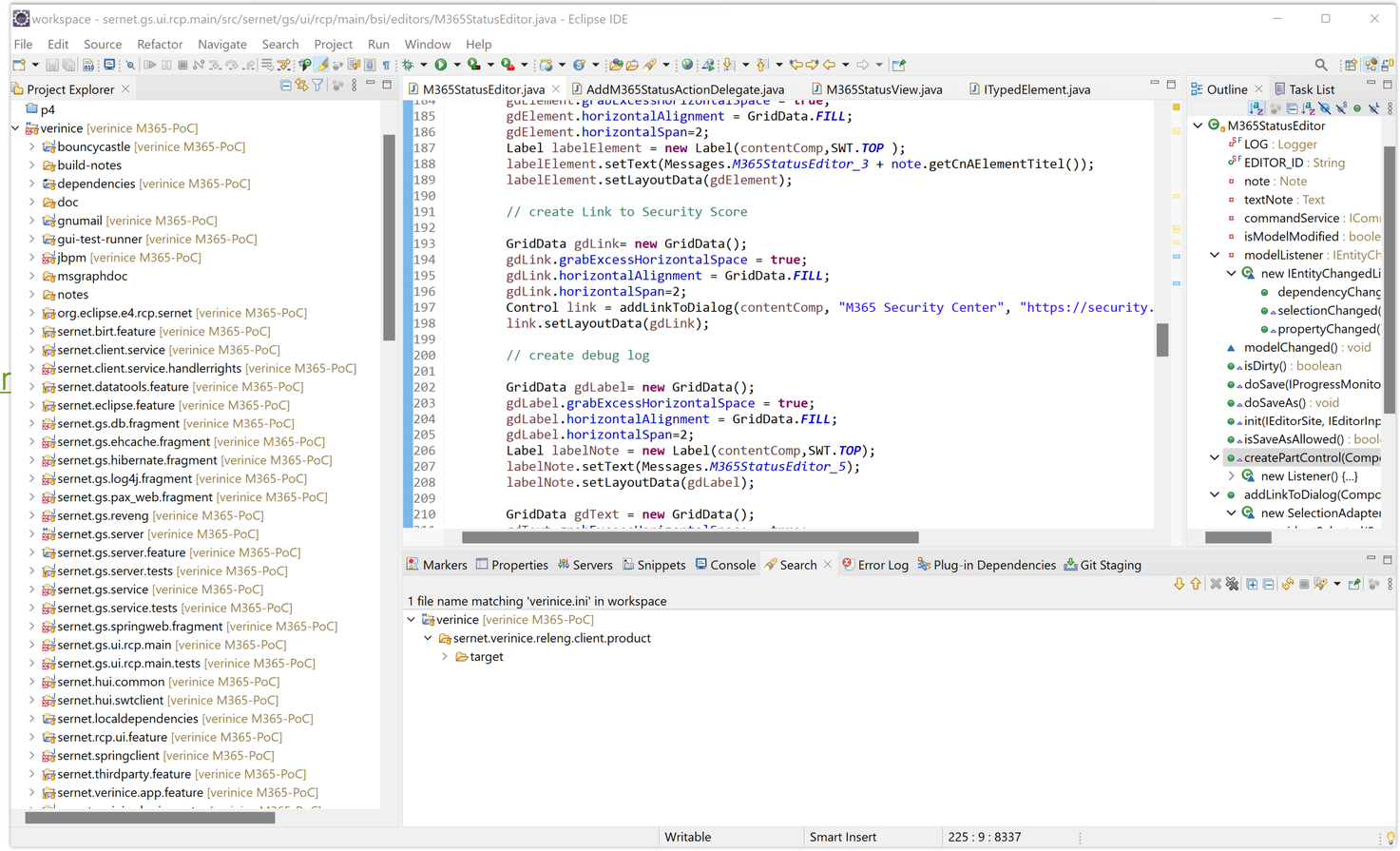
vogella GmbH
Tutorials zu Eclipse RCP
https://www.vogella.com/tutorials/EclipseJobs/article.html

Nicola Suter, Workplace engineer @baseVISION.
MSAL (Microsoft Authentication Library)
https://tech.nicolonsky.ch/explaining-microsoft-graph-access-toker

Microsoft:
https://github.com/microsoftgraph/msgraph-sdk-java

Brian A T
Beitrag zur Ausführung von PowerShell von Java
https://social.technet.microsoft.com/Forums/office/en-US/d32537bd-0aef-440e-8760-6b3085390c37/executing-powershell-script-via-java?forum=winserverpowershell

Elliot Munro
Powershell Skript für Export des Secure Scores
https://gcits.com/knowledge-base/export-customers-microsoft-secure-scores-to-csv-and-html-reports/



Contact

0049 170 9637991

sales@uneedsecurity.com

uneedsecurity.com