

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

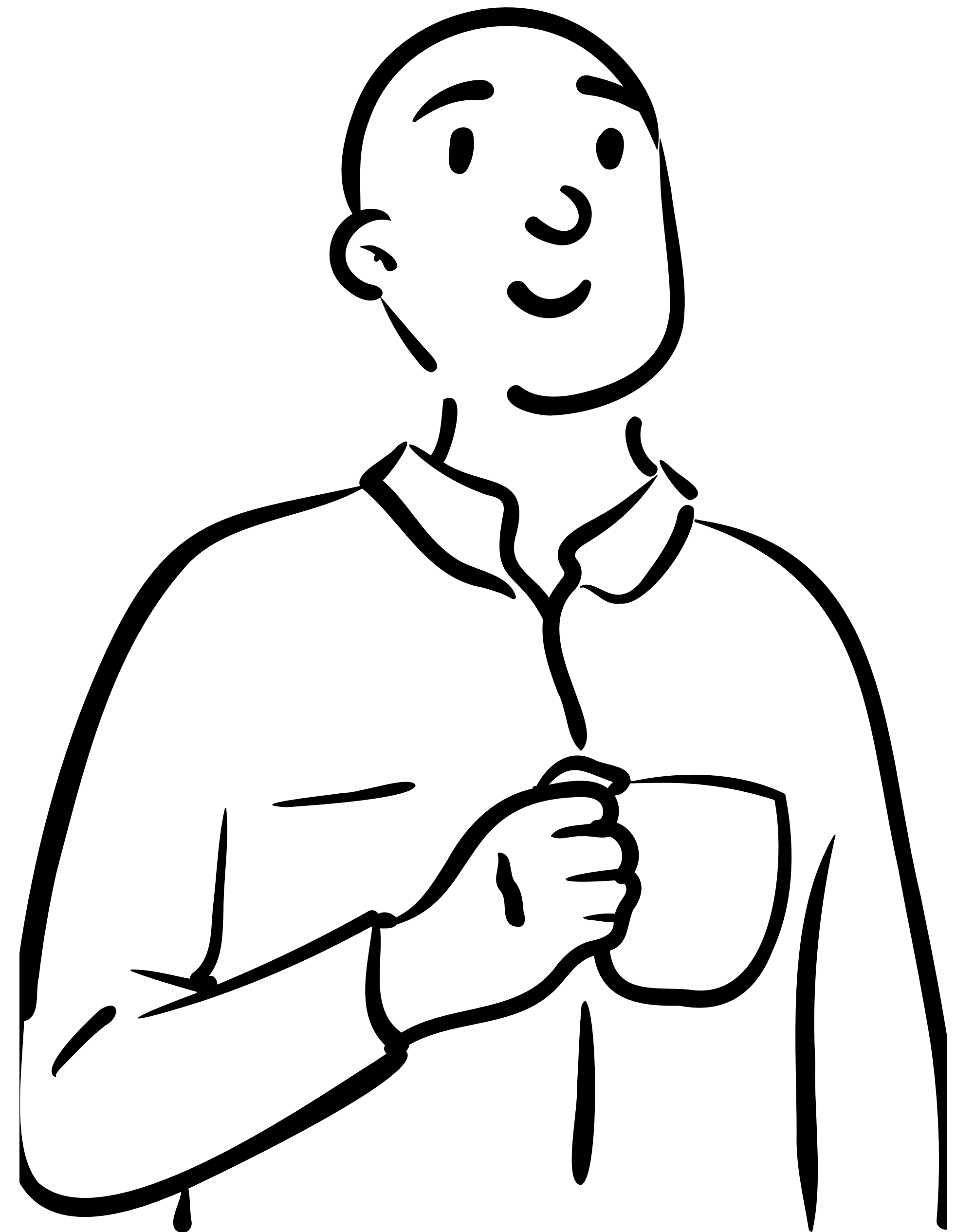
UNeedSecurity GmbH
Managed Security Service Provider



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

verinice

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



Agenda



Gegenstand



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



C5 Katalog,
Compliance am Beispiel von M365



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-Verordnung.



vorhandenes Sicherheitsmanagement

Sie haben ein ausgebautes Sicherheitsmanagement 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 akzeptiert, 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

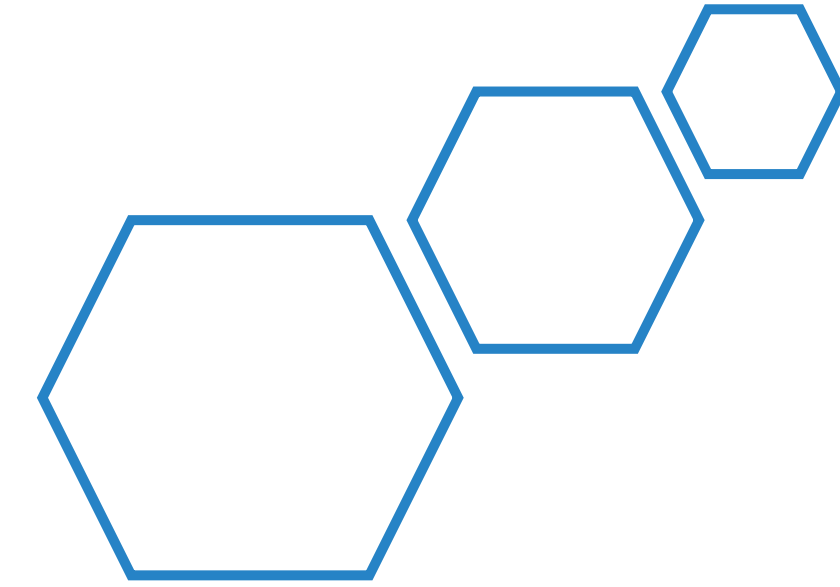
Effizienz durch regelbasierte Automatisierung
Minimierung der Dokumentation

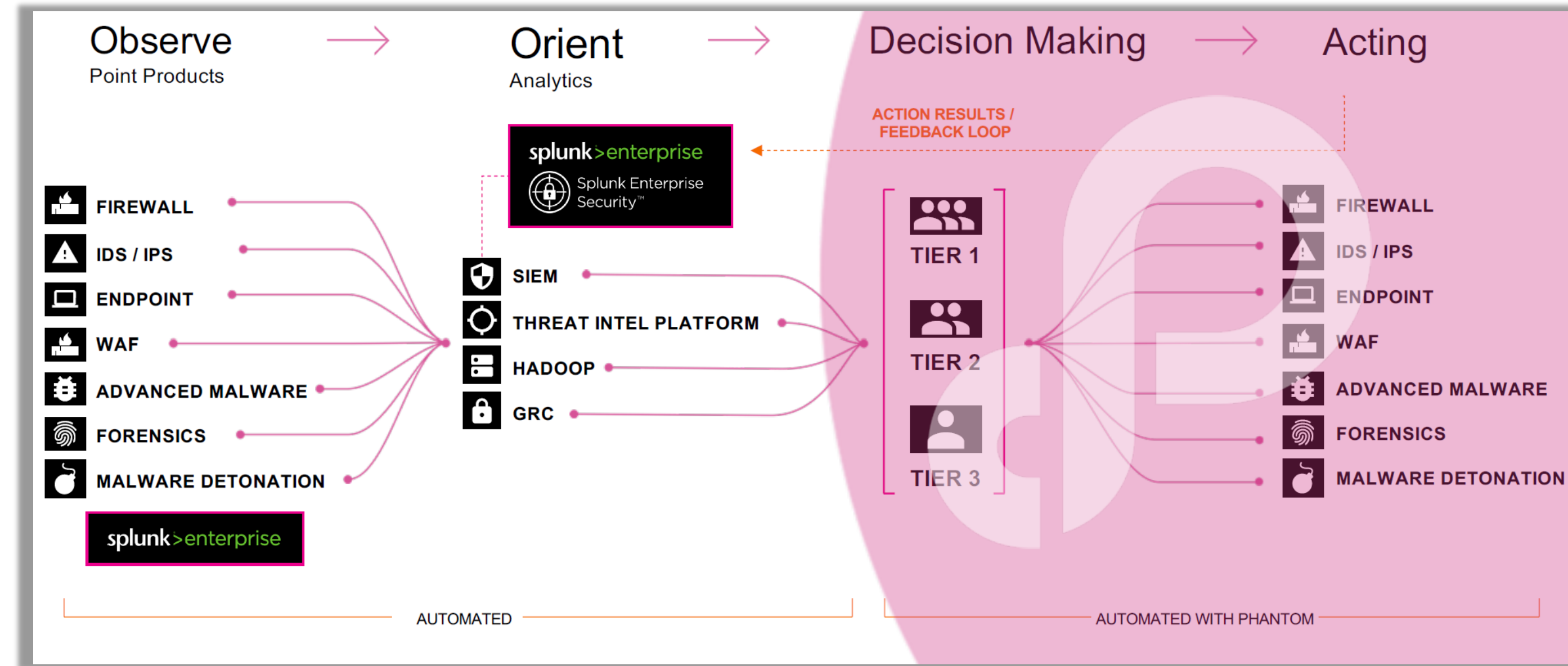
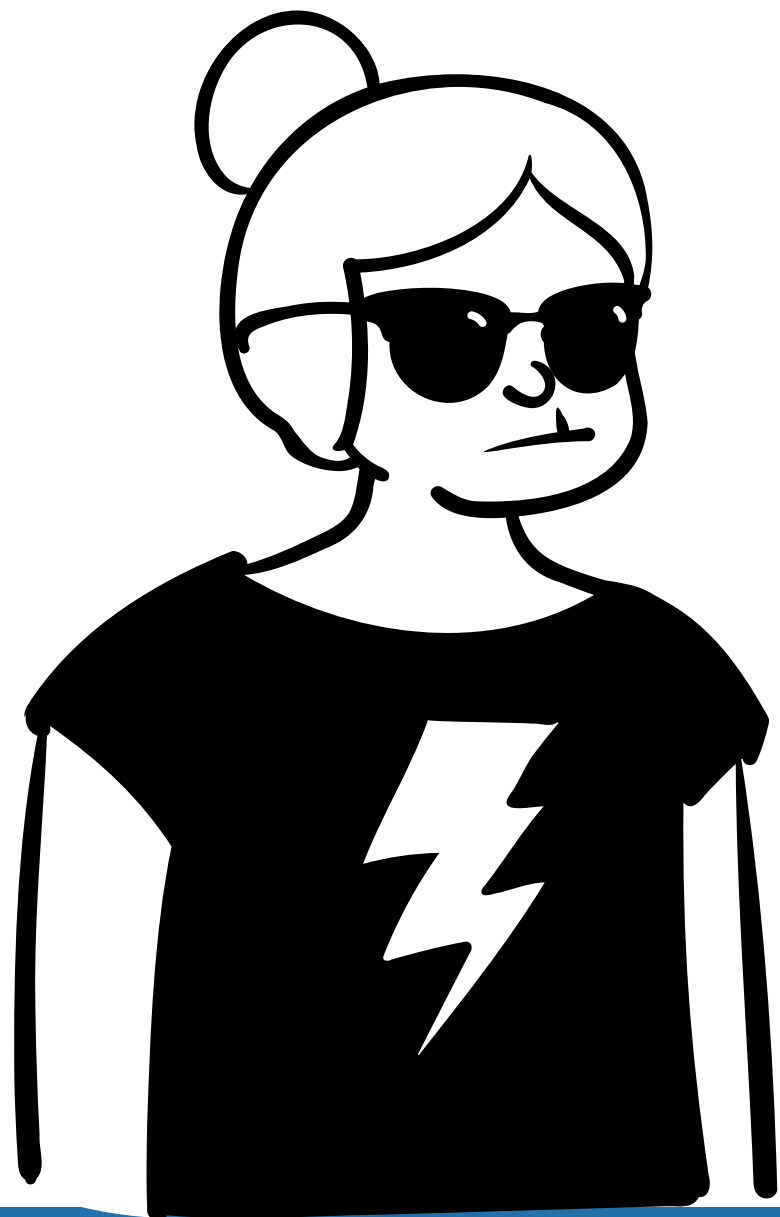


Stärkung der Datenschutzbeauftragten Stärkung des CISO

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



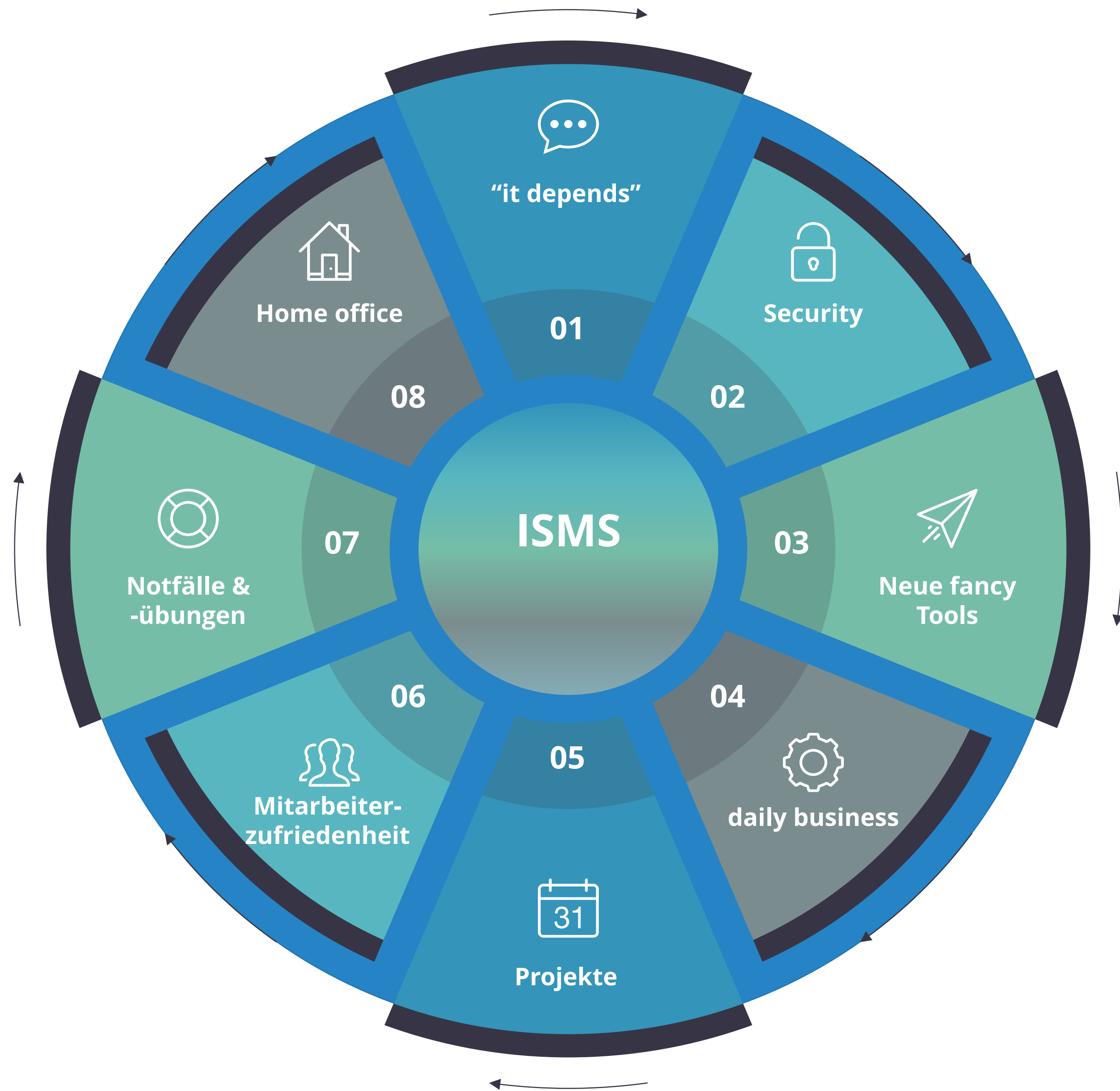




Quelle: splunk



On premise vs. (managed) clouds



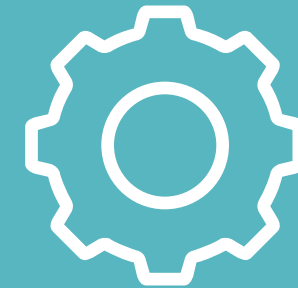
verinice als Steuerungs-instrument

Open Source Gedanke nutzen

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

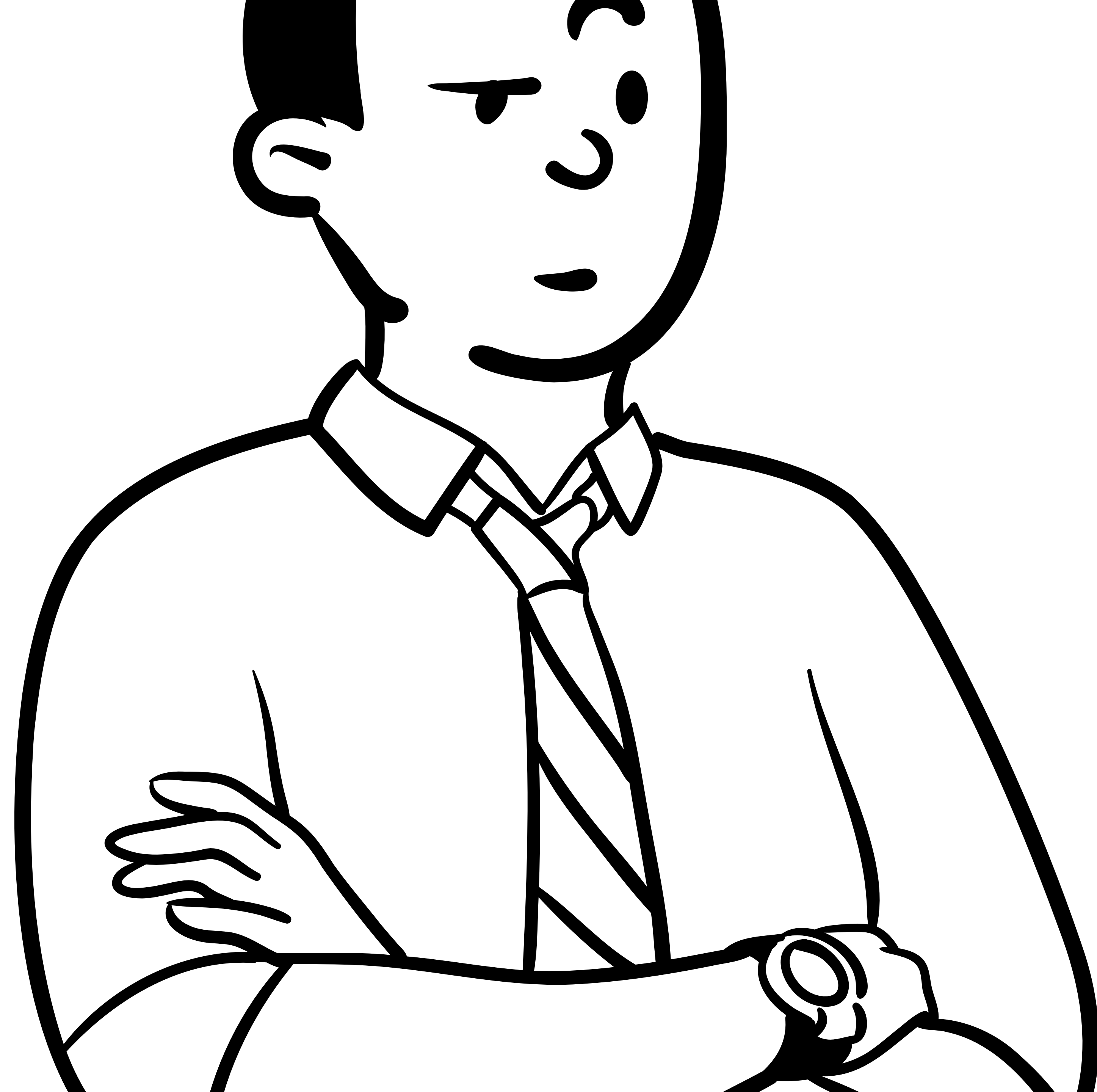
Idee: über die festgestellten Optimierungsempfehlungen wird das Sicherheitsniveau rechtzeitig angehoben, bevor es zu Ausfällen und Sicherheitsvorfällen kommt.

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 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

Grundlage für die Anforderungen an Cloud-Anbieter

Kontrollpflicht über Zertifizierungen

Nutzung der EU Standard Contracts als Vorlage

The screenshot displays the Verinice.PRO application window. On the left, a tree view shows the 'Kriterienkatalog Cloud Computing C5:2020 [ITGS-C5]' structure, with '6.17 PSS Produktsicherheit [ITGS-C5]' expanded to show 'PSS-01 Leitlinien und Empfehlungen für Cloud-Kunden'. The main area shows the details for 'PSS-01 Leitlinien und Empfehlungen für Cloud-Kunden'. The 'Identifizier' field contains 'PSS-01' and the 'Titel' field contains 'Leitlinien und Empfehlungen für Cloud'. The 'Vorgehensweise' is set to 'unbearbeitet'. The 'Beschreibung' field is empty. The 'Tags' field contains 'KontinuierlichePrüfung:teilweise'. The 'Dokument' field has an 'Ändern...' button. The 'Letzte Änderung' is '26.05.2020'. The 'Release' field is empty. The 'Änderungstyp' field has an 'Ändern...' button. The 'Änderungsdetails' field is empty. The 'Vertraulichkeit' checkbox is checked. The 'Integrität' checkbox is checked. The 'Verfügbarkeit' checkbox is checked. The 'Umsetzung' section shows 'Aus Maßnahme ableiten' as an unchecked checkbox, 'Umsetzungsstatus' as 'unbearbeitet', and 'Umsetzung bis' as '26.05.2020'. The 'Revision' section shows 'Letzte Revision am' as '26.05.2020'. The 'Bemerkungen' field is empty. The 'Objektbrowser' on the right shows the 'Basiskriterium' and 'Zusatzkriterium' sections.

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.

Art und Umfang der bereitgestellten Informationen orientieren sich am Bedarf sachverständigen Personals der Cloud-Kunden, die Vorgaben zur Informationssicherheit machen, diese umsetzen oder die Umsetzung überprüfen (z.B. IT, Compliance, Interne Revision). Die Informationen in den Leitlinien und Empfehlungen für die sichere Nutzung des bereitgestellten Cloud-Dienstes adressieren insbesondere die folgenden Aspekte, soweit diese für den Cloud-Dienst anwendbar sind:

- Anleitungen bezüglich der sicheren Konfiguration
- Informationsquellen zu bekannten Schwachstellen und Aktualisierungsmechanismen
- Fehlerbehandlungs- und Protokollierungsmechanismen
- Authentisierungsmechanismen;
- Rollen- und Rechtekonzept, inkl. risikobehafteter Kombinationen
- Dienste und Funktionen zur Administration des Cloud-Dienstes durch privilegierte Benutzer.

Die Informationen werden so gepflegt, dass sie für den bereitgestellten Cloud-Dienst in der für die produktive Nutzung vorgesehenen Version anwendbar sind.

Zusatzkriterium

-

Ergänzende Informationen

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.

Responsibility		SaaS	PaaS	IaaS	On-prem
Responsibility always retained by the customer	Information and data	Customer	Customer	Customer	Customer
	Devices (Mobile and PCs)	Customer	Customer	Customer	Customer
	Accounts and identities	Customer	Customer	Customer	Customer
Responsibility varies by type	Identity and directory infrastructure	Shared	Shared	Customer	Customer
	Applications	Microsoft	Shared	Customer	Customer
	Network controls	Microsoft	Shared	Customer	Customer
	Operating system	Microsoft	Microsoft	Customer	Customer
Responsibility transfers to cloud provider	Physical hosts	Microsoft	Microsoft	Microsoft	Customer
	Physical network	Microsoft	Microsoft	Microsoft	Customer
	Physical datacenter	Microsoft	Microsoft	Microsoft	Customer

■ Microsoft
 ■ Customer
 ▤ Shared

Kontroll- und Steuerungsmöglichkeiten

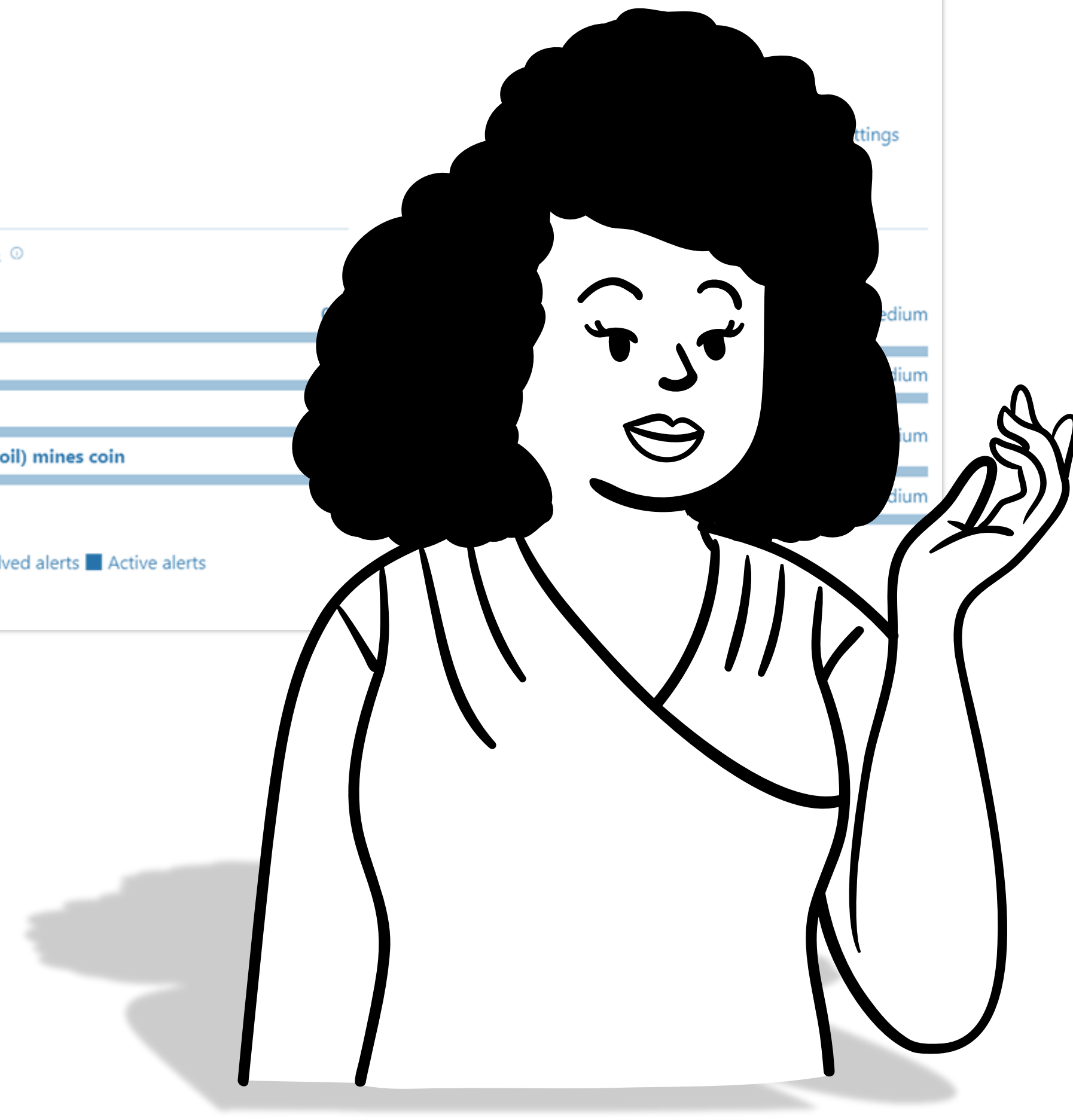
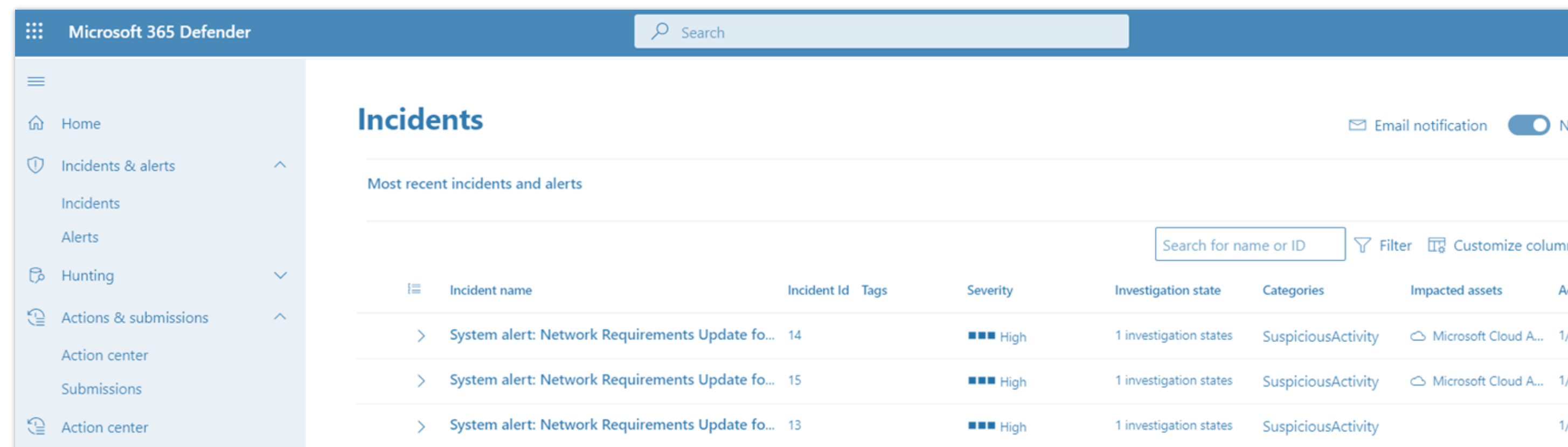
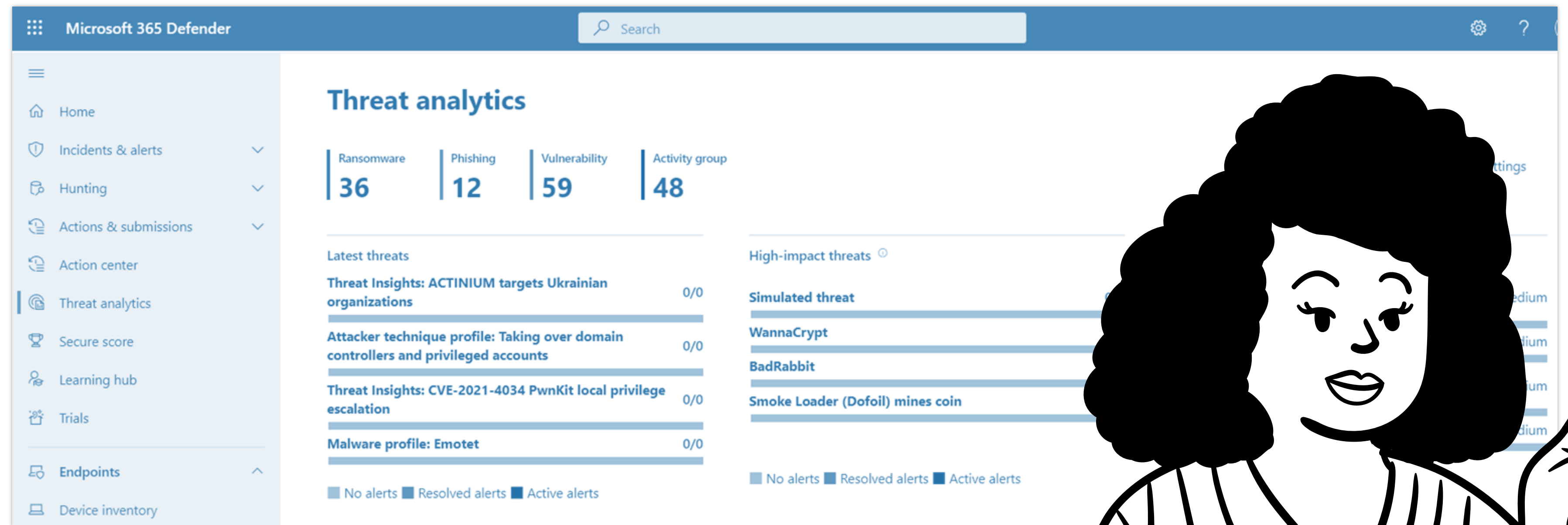
Alerts

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

Eclipse – 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/creating-powershell-script-via-java?forum=winserverpowershell>

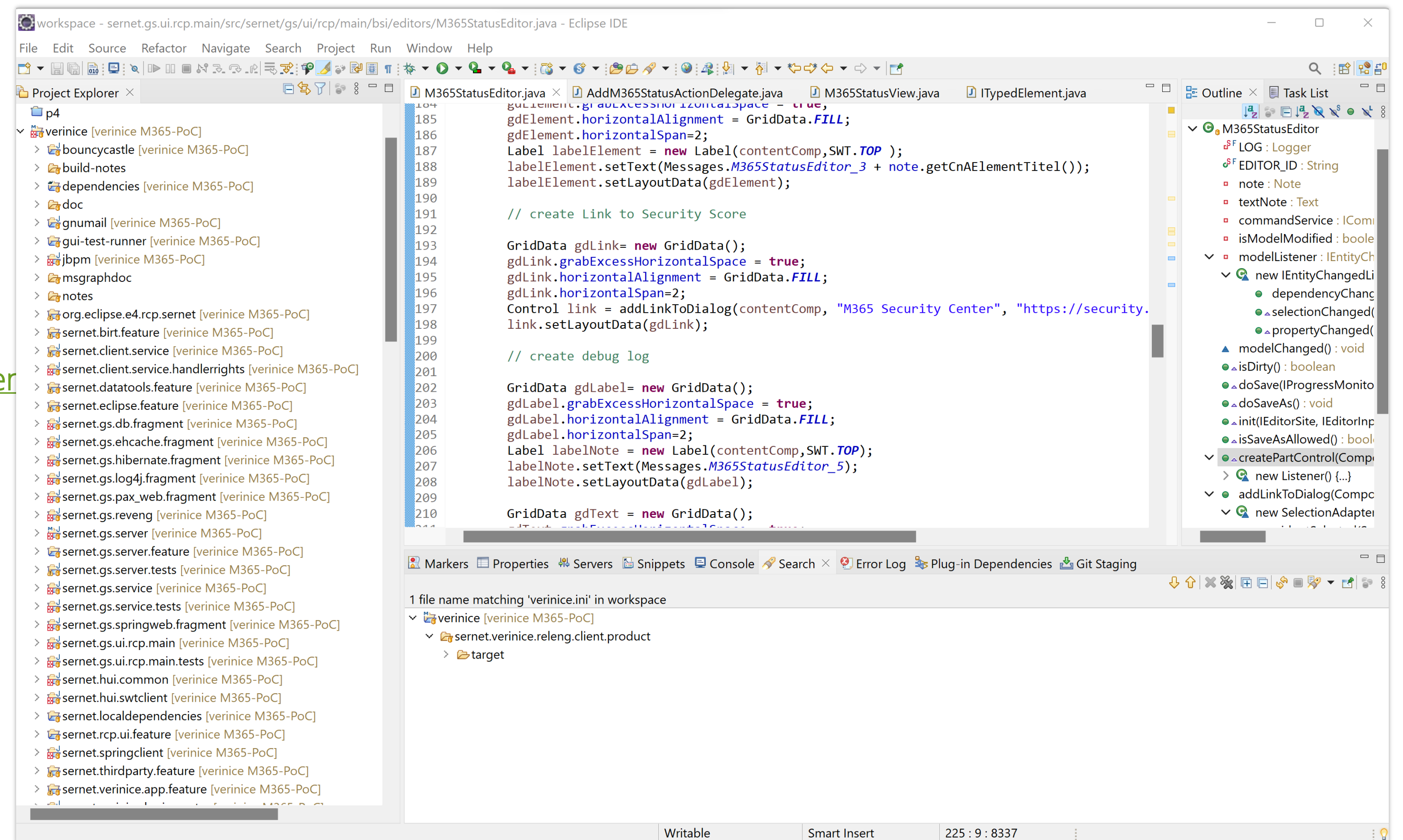
executing-powershell-script-via-java?

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@unneedsecurity.com



unneedsecurity.com

