yourICT.

Security in der Cloud

Was haben Ritterrüstung und Burggraben damit zu tun?

Fermin Sanchez
Teamleiter Workplace und Server Engineering

Markus Rieder
CIO

Agenda

Was Sie heute erwartet

- Einleitung
- Klassische IT vs Modern Workplace
- Live-Demo
- Azure Information Protection (AIP)
- Data Loss Prevention (DLP)
- Insider Risk Management

Econis AG

Ihr Experte für IT-Outsourcing Lösungen

Schweizer Technologie- und Dienstleistungsunternehmen (gegründet 1997)

Erbringung von sicheren, innovativen und geschäftskritischen ICT-Infrastruktur- und Multi-Cloud-Services

Geschäftssitz Dietikon (ZH)

Niederlassung Lyss (BE)

~ 80 Mitarbeiterinnen und Mitarbeiter

50 davon im technischen Bereich (Implementation, Betrieb und Support)

5 Auszubildende

ISO/IEC 27001:2013 zertifiziert

Klassische IT

Klassischer Ansatz: Eigenes Datacenter
oder Private Cloud in der Schweiz

Sobald die Daten die Firma verlassen
(zum Beispiel Mail), gibt es keine Kontrolle mehr

Zugriff erfolgt aus der Firma und/oder
mit firmeneigenen Geräten

Wenig Kollaboration mit Externen

Sharing mit Externen in der Regel per E-Mail

Modern Workplace

Daten können in Public Cloud liegen

Das Teilen von Daten mit Externen gewinnt an Bedeutung

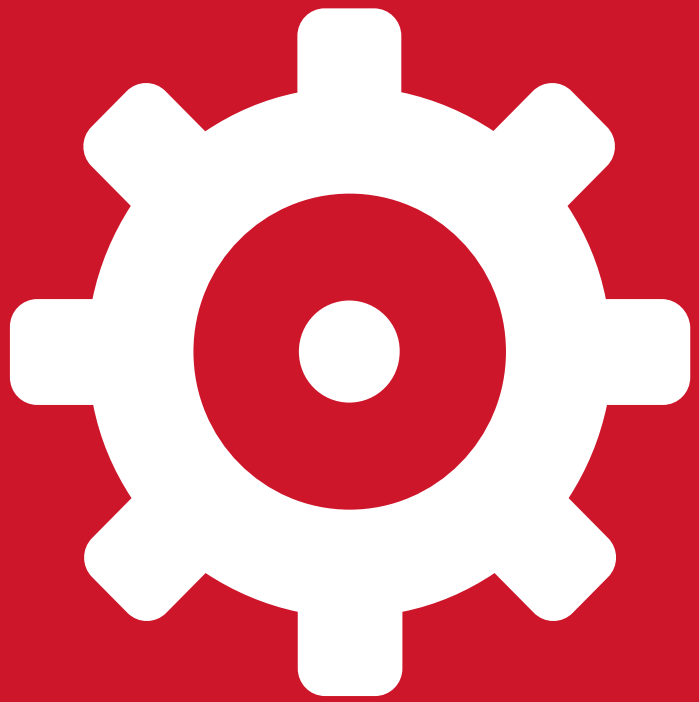
Es werden unterschiedliche Geräte, teils BYOD, eingesetzt

Kontrolle der Daten in den Dokumenten
gewinnt an Bedeutung

Data Loss Prevention (DLP) verhindert das Teilen und den Verlust von sensitiven Daten

DLP und Verschlüsselung (AIP) sind integrale Bestandteile

Live-Demo
Technologien



Exchange

Azure Information Protection

Data Loss Prevention

Live-Demo
Beispiel

Szenario – Schutz einer E-Mail und sensitiver Daten

Versuch 1

Weiterleiten an private Mailadresse (x.y@bluewin.ch)
Kein Erfolg, da das Weiterleiten an eine externe Adresse nicht zulässig ist.

Versuch 2

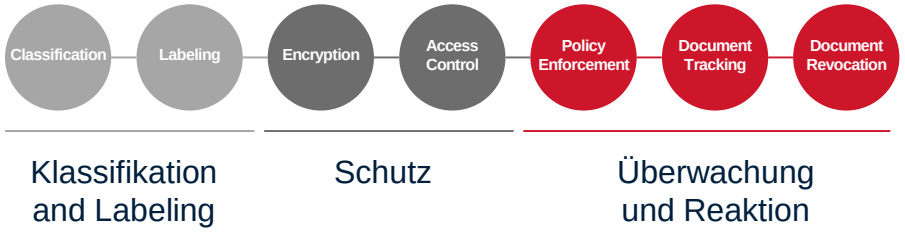
Versand einer e-Patientendossier Nummer per Mail
Die e-Patientendossier Nummer wird vom System erkannt. Eine DLP Regel verhindert das Versenden an Externe ohne Angabe eines Grundes.

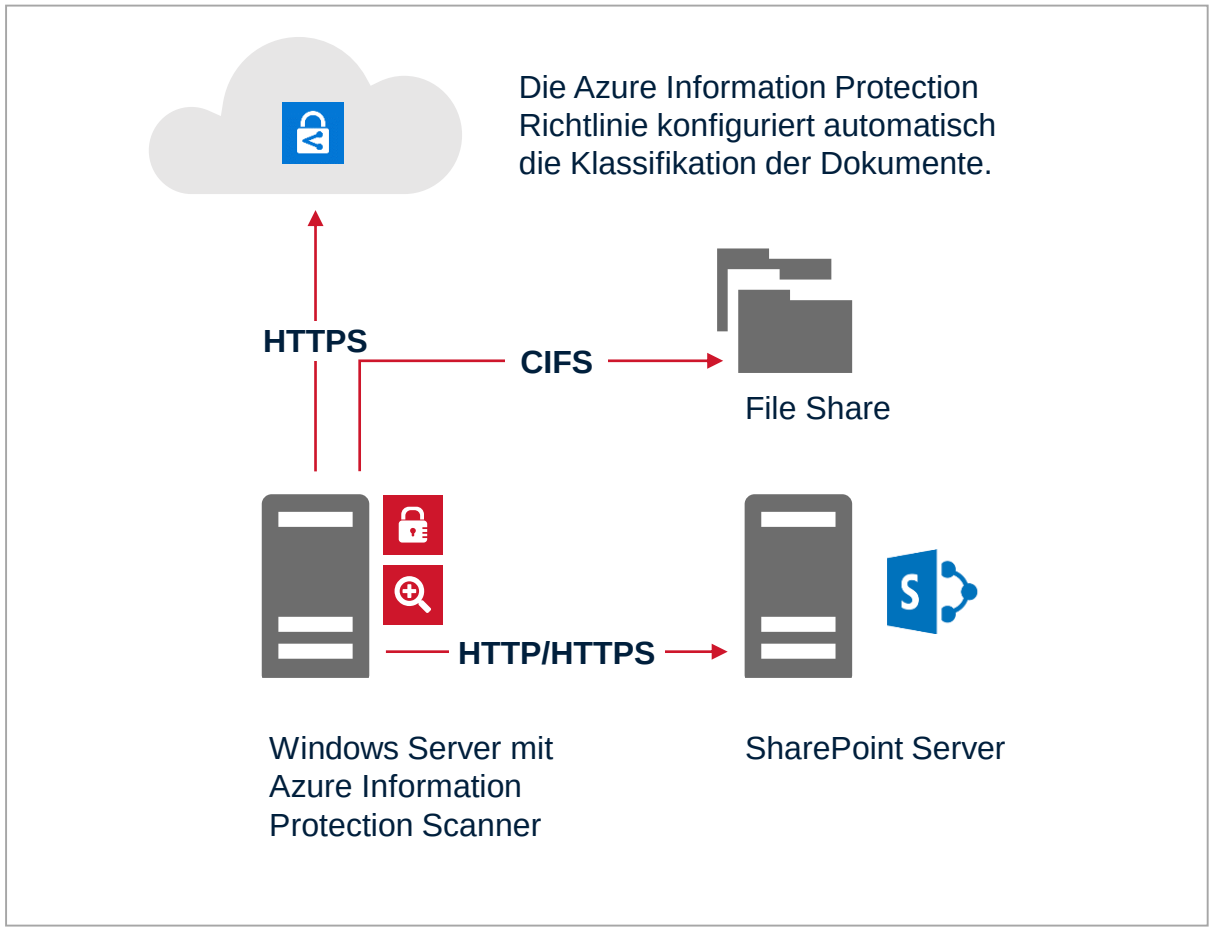
Azure Information Protection (AIP)

Architektur AIP

Mit AIP schützen wir die Daten, damit sie nicht in falsche Hände geraten.

Dokumente oder E-Mails werden nach dem Tagging verschlüsselt, unabhängig davon, wohin sie gehen.





Azure Information Protection (AIP)

Vorgehen für die Implementation von AIP

Planen

- Scope definieren
- Daten klassifizieren und Label definieren
- Richtlinien definieren

Bauen

- Richtlinien implementieren und Pilot durchführen
- Ereignisberichte aktivieren und Auswirkungen beurteilen
- Finetuning durchführen
- Mitarbeiter Awareness steigern

Aktivieren

- Aktivieren von AIP in der gesamten Organisation
- Kontinuierliches anpassen basierend auf Ereignisreports

Azure Information Protection

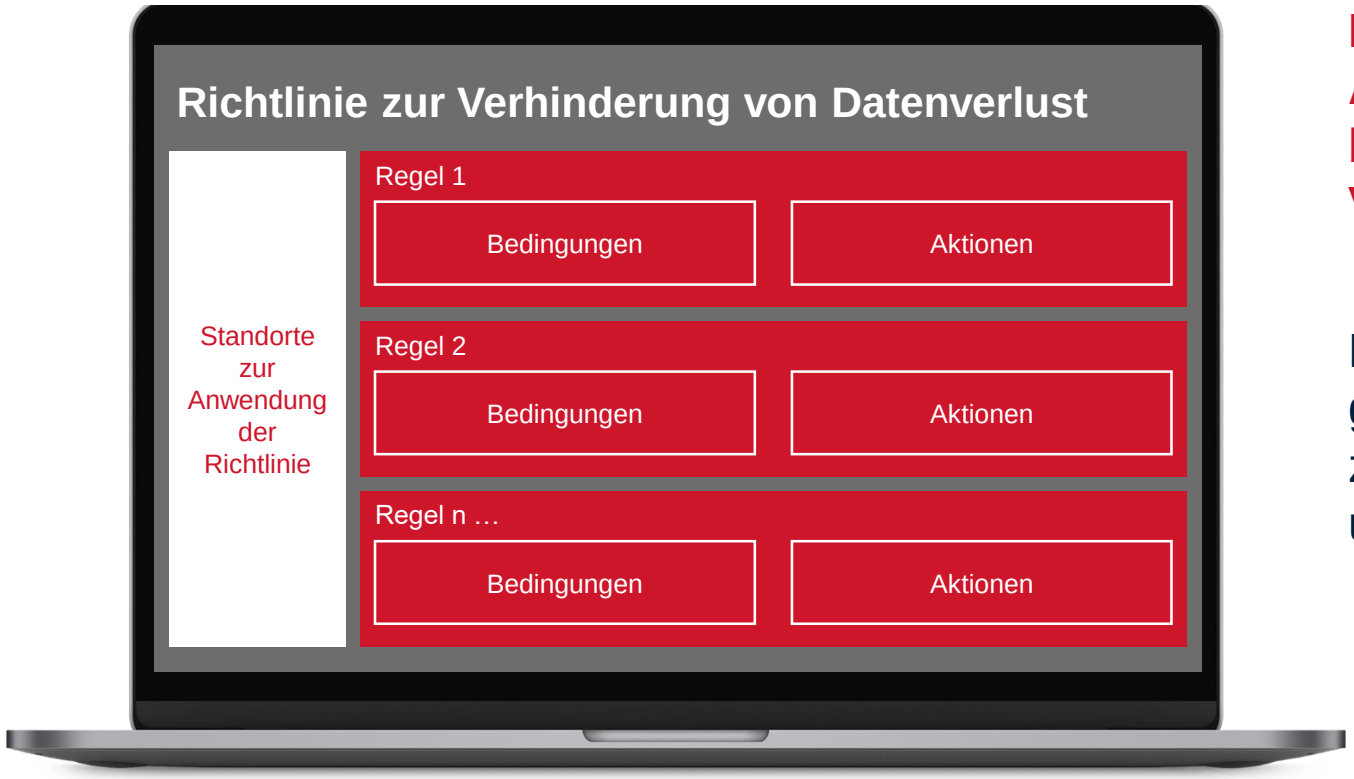
Wichtigste Features und benötigte Lizenzen

Feature	AIP für Office 365 *)	AIP P1	AIP P2
Schutz von Exchange, SharePoint und OneDrive for Business und MS Office Dokumenten	x	x	x
Eigene Templates	x	x	x
Erweiterung auf on-premises Exchange/SharePoint	x	x	x
Office 365 Message Encryption	x	x	x
AIP Erweiterung auf iOS, Mac OS, Android		x	x
Schutz anderer Dokumentformate		x	x
Manuelle, Standard und manuelle Klassifikation		x	x
RM Connector für die Klassifizierung von on-premises Dateien auf Windows File Servern		x	x
Dokument Tracking und Revozierung		x	x
Automatische Klassifizierung			x
Integration von AIP Labels mit Outlook S/MIME Verschlüsselung			x
Verhindern von "Oversharing" in Outlook			x
AIP Scanner zum automatischen Klassifizieren, Labeling und Schutz von on-premises Dateien			x

*) = In Office 365 **Enterprise** E3 und höheren Lizenzen enthalten

Data Loss Prevention (DLP)

Richtlinien Editor

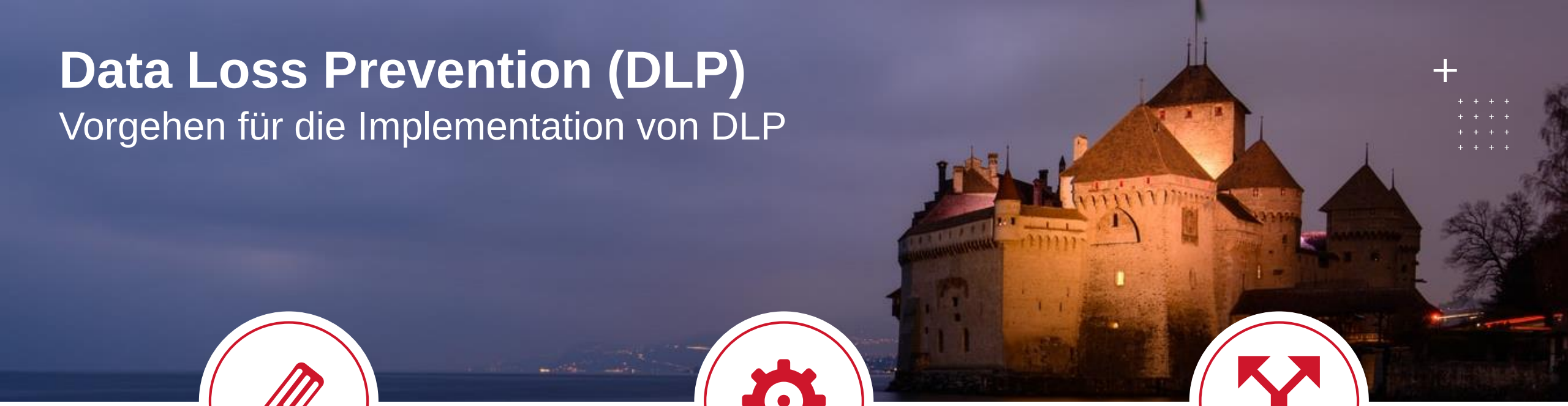


Mit DLP setzen wir Compliance Anforderungen um. Wir haben im Standard bereits viele Compliance-Kataloge zur Verfügung (z.B. HIPAA, Finma, GxP etc.).

Diese Anforderungen sind als einzelne Regeln gespeichert und in einer DLP-Richtlinie zusammengefasst, um die Verwaltung und die Berichterstellung zu vereinfachen.

Data Loss Prevention (DLP)

Vorgehen für die Implementation von DLP



Planen

- Scope definieren
- Start mit Templates
- Spezifische Richtlinien definieren

Konfig. und anpassen

- Richtlinien umsetzen und “Notify Mode” aktivieren, Pilot starten
- Ereignisberichte auswerten und Auswirkungen beurteilen
- Finetuning basierend auf “false positive” Ereignissen

Aktivieren

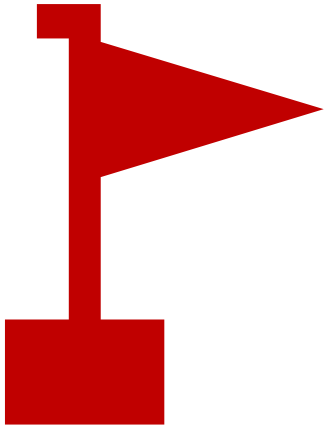
- Policies auf “enforce Mode” setzen (Scharfstellung)
- Kontinuierliches anpassen basierend auf Trendreports

Insider Risk Management

Erkennen interner Risiken

Mit Insider Risk Management von Microsoft 365 können sie interne Risiken minimieren, indem Sie riskante Aktivitäten in Ihrer Organisation erkennen, untersuchen und Massnahmen ergreifen können.

- Daten kontrollieren und schützen – an praktisch jedem Ort
- Insiderrisiken erkennen und beseitigen (Alert Dashboard)
- Relevante Daten schnell finden, verfolgen und übermitteln (e-Discovery)
- Vorschriften mühelos einhalten und Risiken eindämmen
- Fallbearbeitung (Investigate Dashboard)



Lizenzierung

Der Microsoft 365 E5 Compliance Plan steht Kunden zur Verfügung, die eine Lizenz für Microsoft 365 E3 oder für das Paket Office 365 E3 und Enterprise Mobility + Security E3 besitzen.

Insider Risk Management

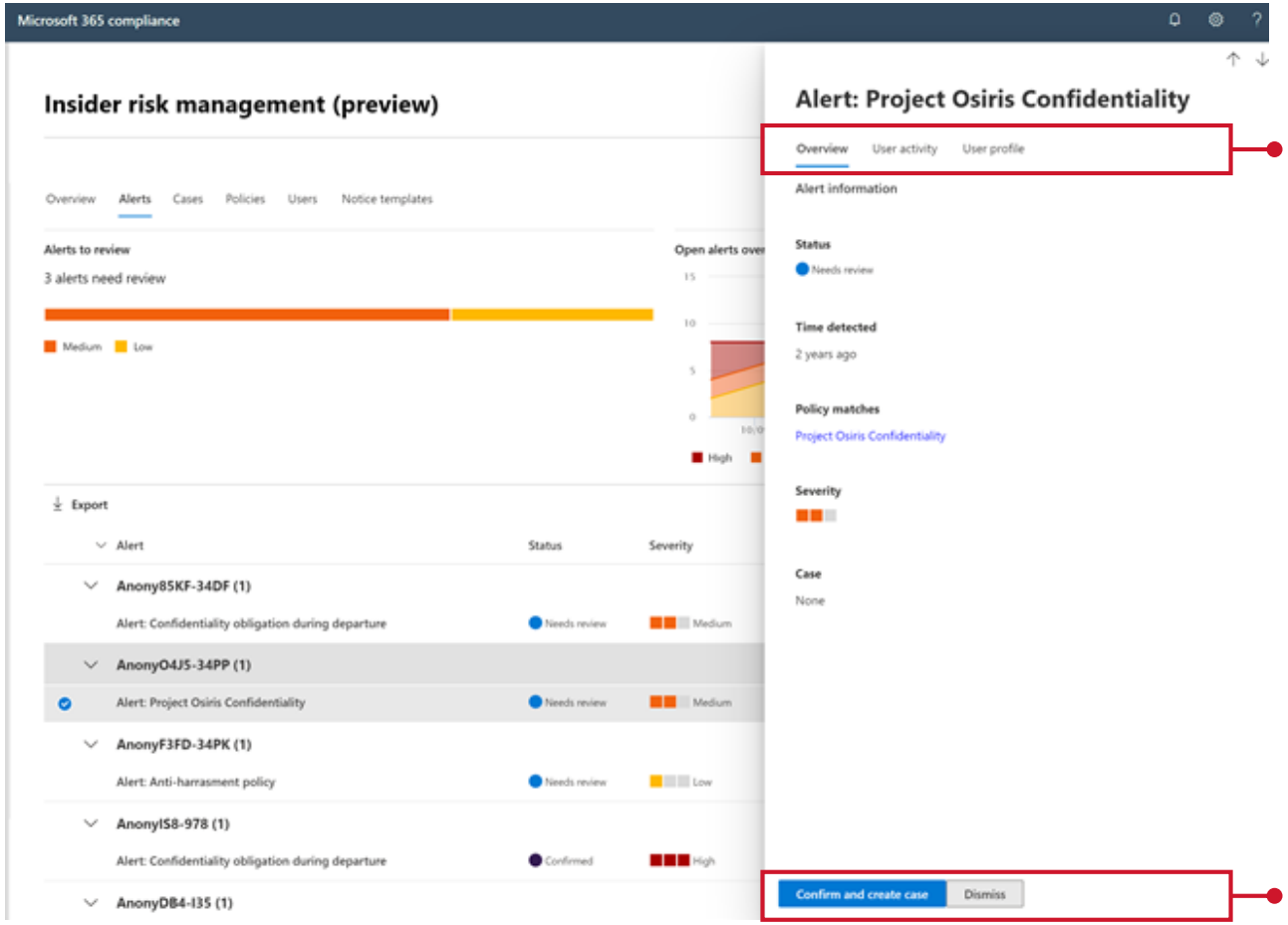
Insider Risk Management Workflow

Sie können aus den folgenden Richtlinienvorlagen auswählen

- Datendiebstahl von Mitarbeitern
- Datenlecks
- Beleidigende Sprache in E-Mails

Insider Risk Management

Alert Dashboard



Übersicht und User Aktivität einfach abrufbar

Schneller Case direkt aus dem Alert erstellen

Insider Risk Management

Vorgehen für die Implementation von Insider Risk Management

Planen

- Scope definieren
- Rollenkonzept definieren (Wer darf was in welchem Umfang)
- Richtlinien definieren

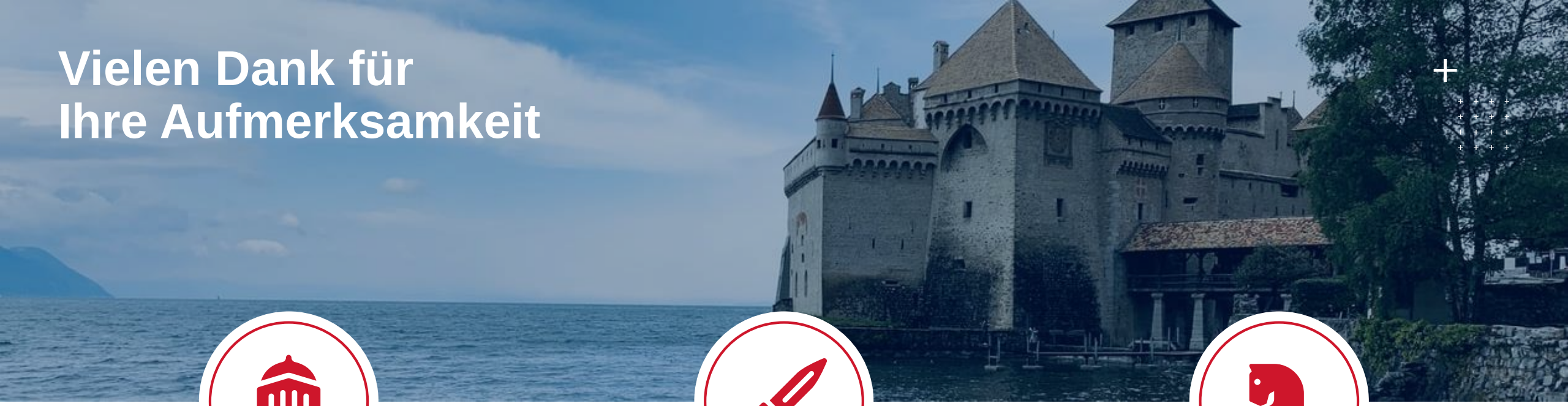
Konfig. und anpassen

- Pilot durchführen (Usergruppe)
- Ereignisberichte auswerten
- Finetuning basierend auf Ereignisberichte
- Gesamte Organisation informieren (Analyse von kritischen Aktivitäten)

Aktivieren

- Policies in der gesamten Organisation aktivieren
- Kontinuierliches anpassen basierend auf Auswertungen

Vielen Dank für Ihre Aufmerksamkeit



Haben Sie Fragen?