Prezentace Sentinel - Rok Informatiky - Telč

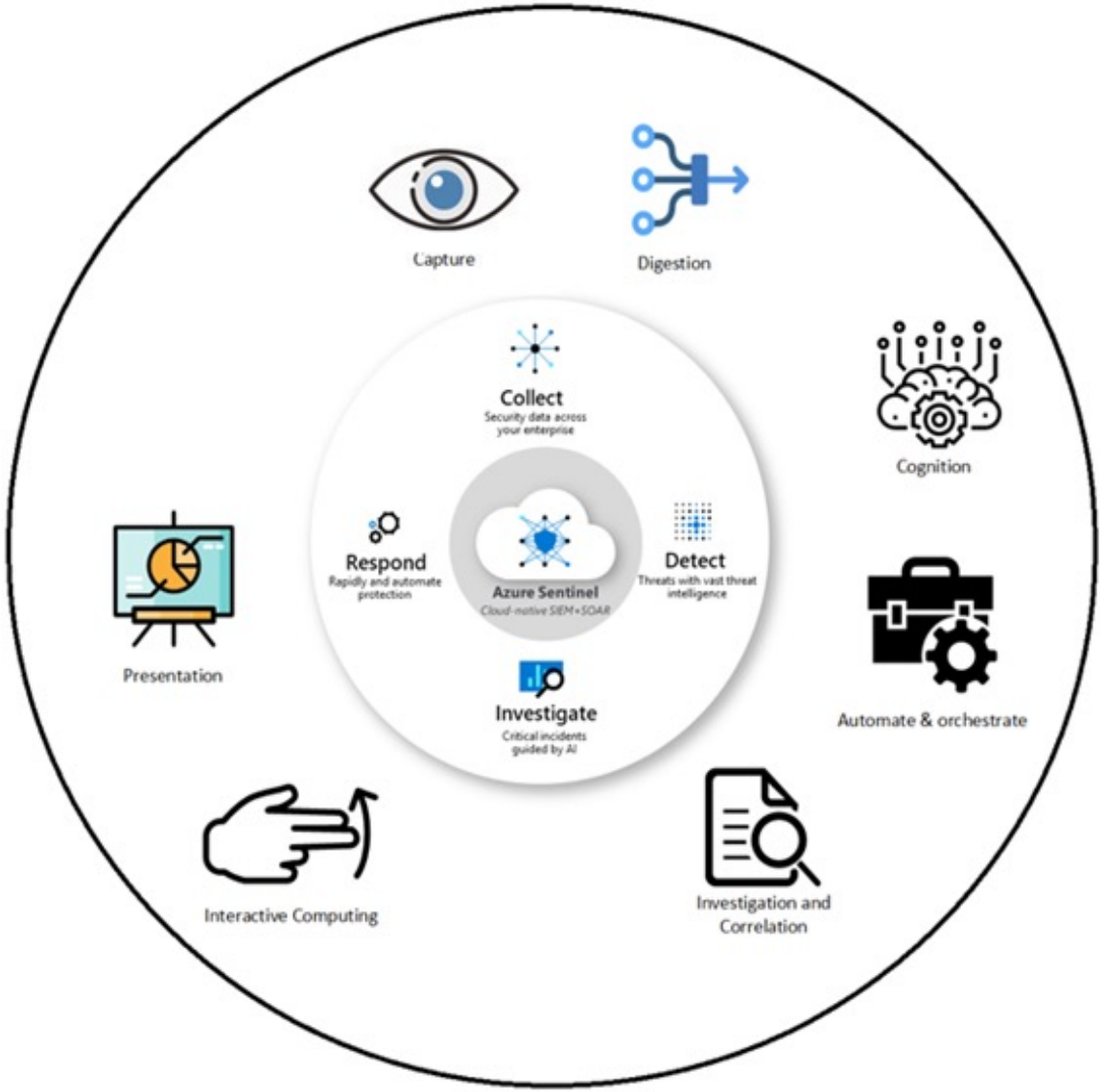
Absolutní bezpečnost prostředí s řešeními Defender & Sentinel

Microsoft Sentinel

Miroslav Toman
1. 6. 2023

Ochrana & Reakce

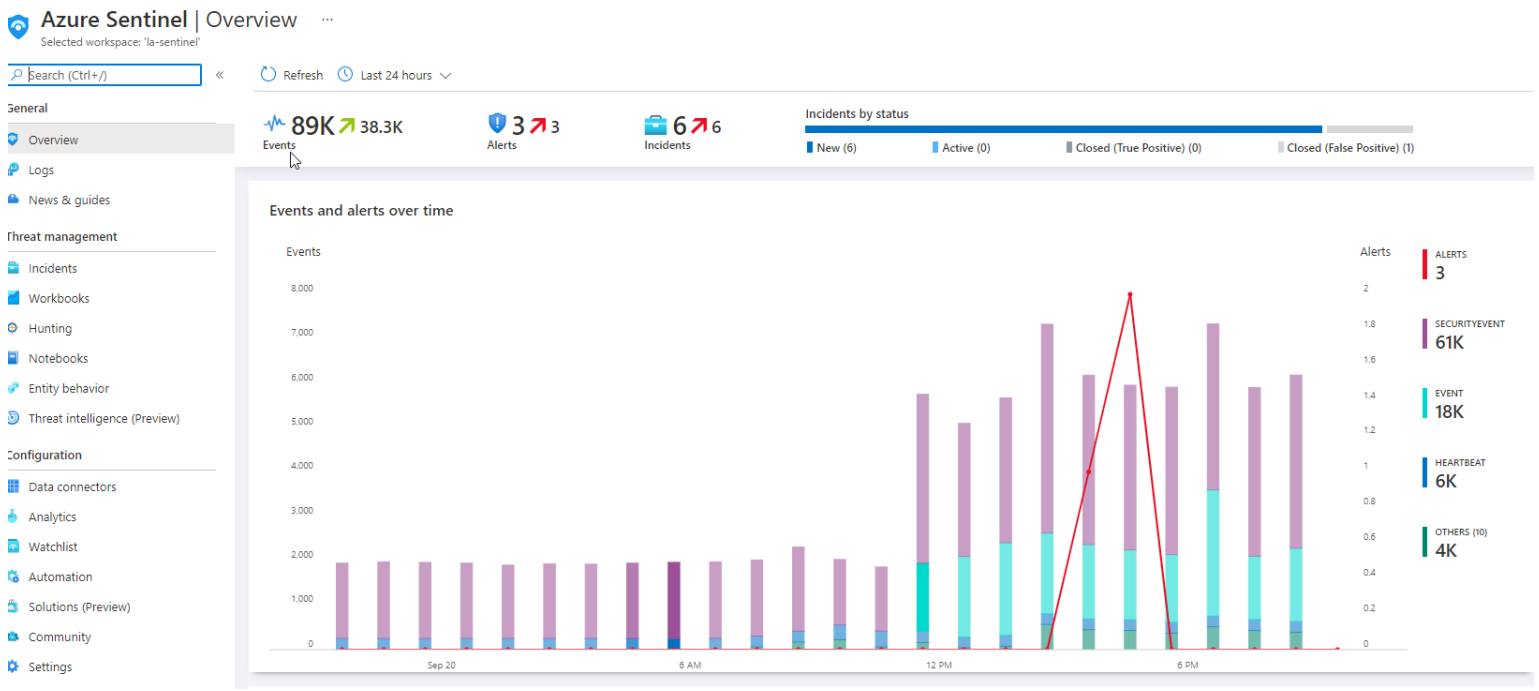
- Čelíme **hrozbám**, při kterých útočníci využívají sofistikované nástroje, které maximalizují návratnost investice (ROI).
- Vývoj **ochranných nástrojů** jede paralelně vedle vývoje automatizovaných nástrojů na útočení.
- Je potřeba si uvědomit, že ne všechny **útoky** dokážeme **efektivně odrazit**, je potřeba mít vyvážené financování do prevence, detekce a odezvy.
- Pomocí **pokročilé analytiky** Sentinel pomáhá filtrováním různých typů signálů doporučit na bližší analýzu právě ty, kterým je potřeba věnovat zvýšenou pozornost.



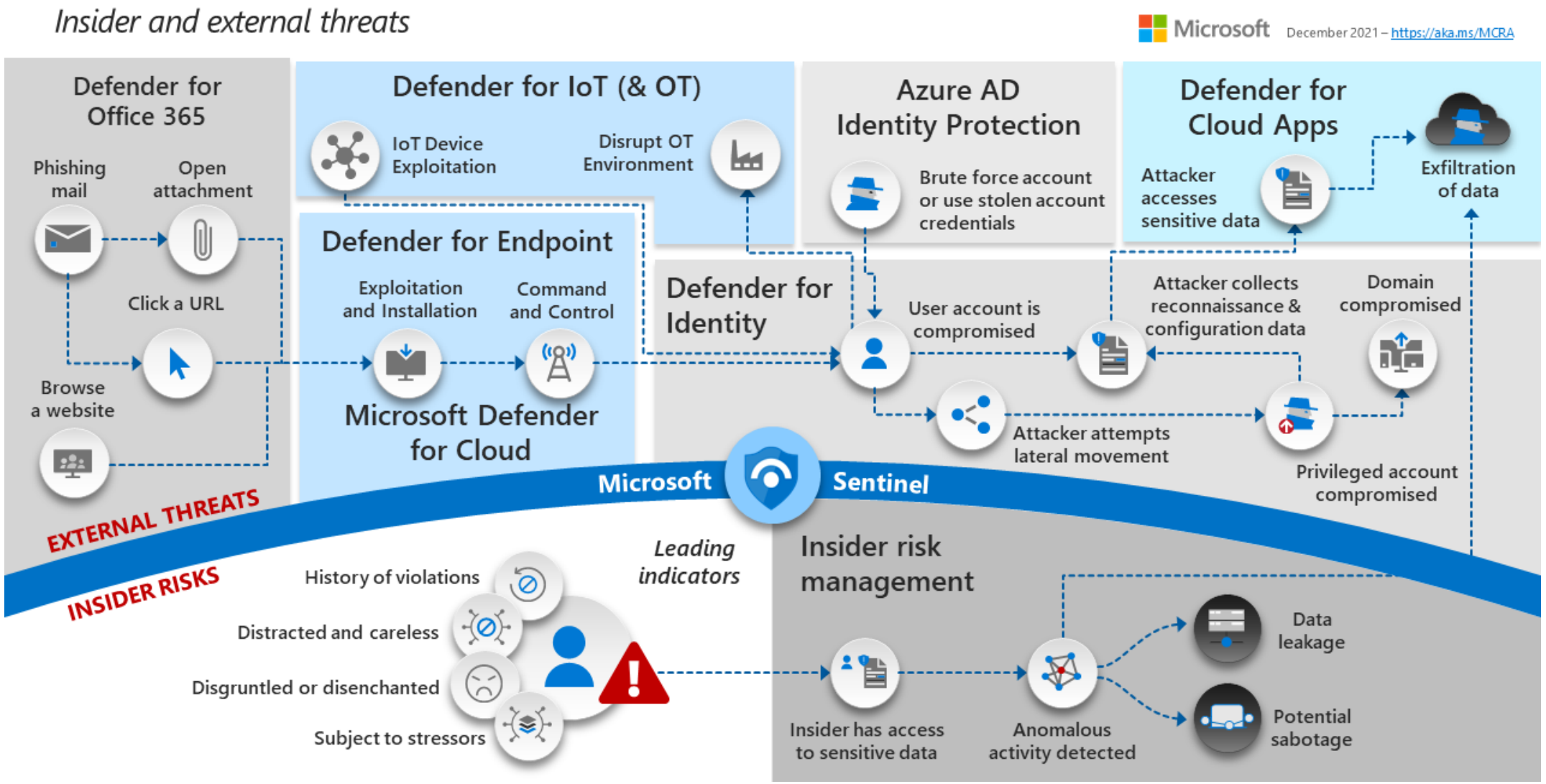
Představení služby

Představení služby Sentinel

- **SIEM pro cloudové prostředí** (cloud native SIEM)
- **SOAR & XDR v reálném čase**
- **Bezpečnostní doporučení** dle zkušeností Microsoftu z provozu globálního cloudového prostředí
- **SaaS**
- **Auto-scaling**
- **Data ingestion**
- **AI & ML features**
- **Logic Apps & EventHub integration**
- **Human and AI cooperation**
- **Reporting**

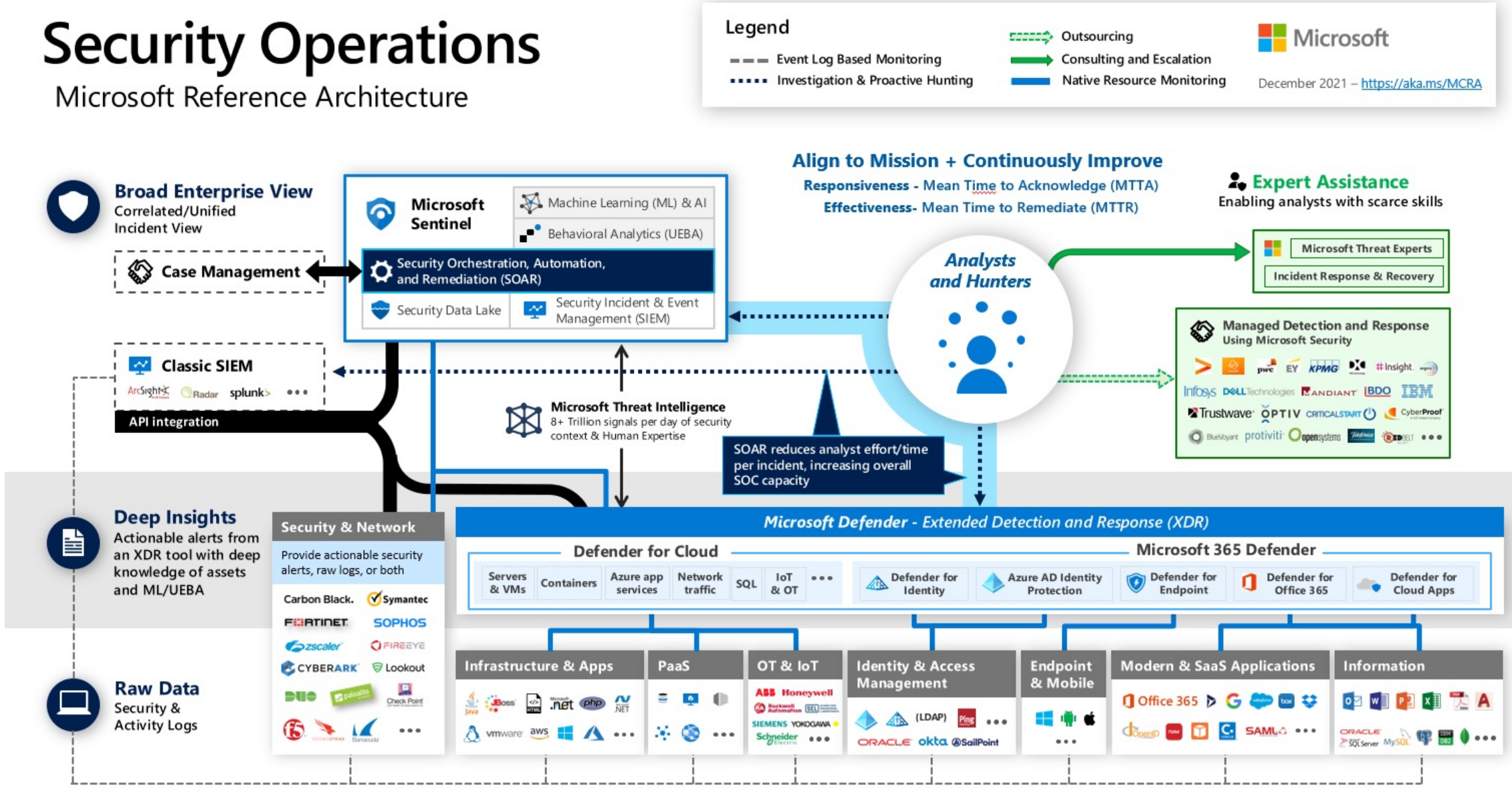


Představení služby Sentinel



Security Operations

Microsoft Reference Architecture



Klíčové vlastnosti

Sběr dat v cloudovém měřítku – napříč všemi uživateli, zařízeními, aplikacemi a infrastrukturou, a to jak na místě, tak ve více cloudech.

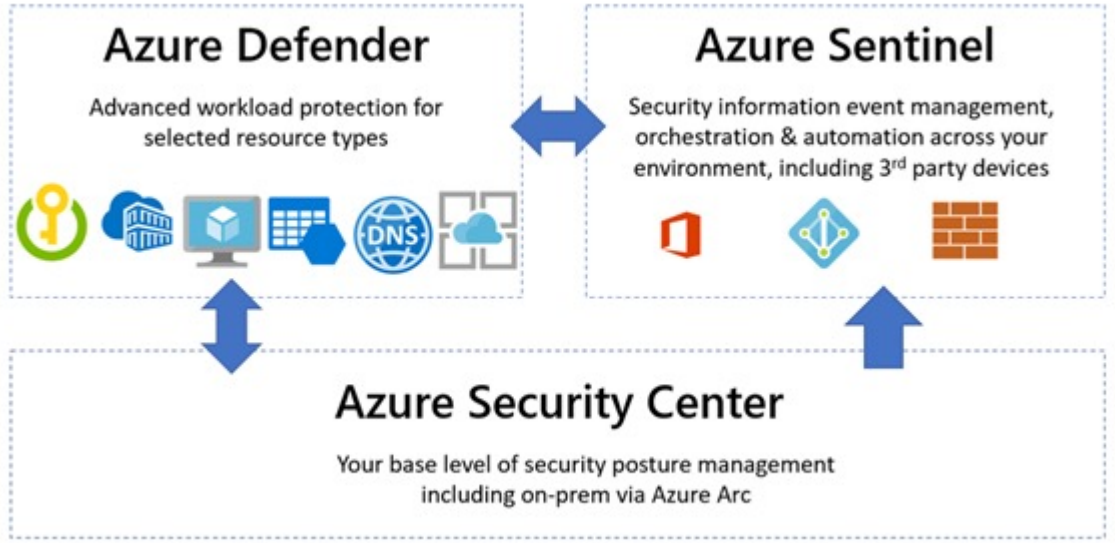
Detekce dříve odhalených hrozeb a minimalizace falešných poplachů pomocí analytiky a jedinečného zpravodajství o hrozbách od společnosti Microsoft.

Prozkoumání hrozeb pomocí umělé inteligence a hledání podezřelé aktivity ve velkém, využití desítky let práce v oblasti kybernetické bezpečnosti ve společnosti Microsoft.

Rychlá reakce na incidenty pomocí vestavěné orchestrace a automatizace běžných úkolů.

Konkrétní příklady

- Kontrola přístupu uživatelů k firemním dokumentům
- Změna typu uživatele teamu
- Vytvoření privilegovaného uživatele
- Přihlášení z nestandartních zemí v rychlém sledu
- Export privátních klíčů ADFS serveru
- Credentials dumping & privilege escalation
- Deploying EXE souborů prostřednictvím DC řadičů
- Detekce nových globálních hrozeb



Technické detaily

Technické detaily

- Postaveno na robustním systému uložení a analýzy logů – služba Log Analytics
- Využit jazyk KQL (Kusto Query Language), který umožňuje úpravu připravených dotazů.
- Předpřipravené šablony pro analýzu dat dle zkušeností Microsoftu i komunity uživatelů Sentinelu (GitHub)
- Nástroje pro reaktivní (Alerty) i proaktivní (Workbooky, Hunting) analýzu
- Microsoft i výrobci SW mohou přidávat vlastní konektory (např. SAP, výrobci firewallů, antivirů)
- Microsoft Graph API

Licence & Cena

Licence & Cena

Free Trial

- Vyzkoušejte Microsoft Sentinel na prvních 31 dní zdarma. Microsoft Sentinel lze povolit bez dalších nákladů na pracovním prostoru Azure Monitor Log Analytics, s výhradou omezení uvedených níže.
- Nové pracovní prostory mohou bezplatně zpracovat až 10 GB dat protokolu za den po dobu prvních 31 dnů. Během 31denního zkušebního období jsou prominuty jak poplatky za příjem dat Log Analytics, tak poplatky za Microsoft Sentinel. Na tuto bezplatnou zkušební verzi se vztahuje limit 20 pracovních prostorů na jednoho tenanta Azure.
- Stávající pracovní prostory mohou povolit Microsoft Sentinel bez dalších nákladů. Během 31denního zkušebního období jsou prominuty pouze poplatky za Microsoft Sentinel.
- Použití nad tyto limity bude účtováno podle cen uvedených na této stránce. Poplatky související s dalšími funkcemi pro automatizaci a zavedením vlastního strojového učení jsou během bezplatné zkušební verze stále platné.

Licence & Cena

Výhoda Microsoft Sentinel pro zákazníky Microsoft 365 E5, A5, F5 a G5

Zákazníci Microsoft 365 E5, A5, F5 a G5 a Microsoft 365 E5, A5, F5 a G5 Security mohou získat datový grant až 5 MB na uživatele/den ke zpracování dat Microsoft 365. Mezi zdroje dat zahrnuté v této nabídce patří:

- Azure Active Directory (Azure AD) sign-in a audit logs
- Microsoft Cloud App Security shadow IT discovery logs
- Microsoft Information Protection logs
- Pokročilá hunting data Microsoft 365

Chcete-li pracovat s daty přihlášení z AAD, musíte mít Úroveň AAD P1, která je dodávána s licencemi E3.

Licence & Cena

Data connectors per AAD license

AAD P1	AAD P2	AAD Free
Azure Active Directory	Azure Active Directory Identity Protection	Azure Activity

Data connectors per M365 license

M365 A3, E3, G3	M365 A5, E5, G5	Microsoft 365 Defender eligible license
Office 365	Microsoft 365 Defender	Microsoft Defender for Cloud
	Microsoft 365 Insider Risk Management	Microsoft Defender for Endpoint
	Microsoft Defender for Office 365	Microsoft Defender for Office 365

Licence & Cena

Tier	Microsoft Sentinel Price	Log Analytics Price	Total Price	Effective Per GB Price[1]	Savings Over Pay-As-You-Go
Pay-As-You-Go	$2.60 per GB-ingested	$2.99 per GB	$5.59 per GB	$5.59 per GB	N/A
100 GB per day	$130 per day	$252.84 per day	$382.84 per day	$3.83 per GB	32%
200 GB per day	$234 per day	$474.72 per day	$708.72 per day	$3.55 per GB	37%
300 GB per day	$338 per day	$696.60 per day	$1,034.60 per day	$3.45 per GB	38%
400 GB per day	$433.33 per day	$908.16 per day	$1,341.49 per day	$3.36 per GB	40%
500 GB per day	$520 per day	$1,115.85 per day	$1,635.85 per day	$3.28 per GB	41%
1,000 GB per day	$1,014 per day	$2,193 per day	$3,207 per day	$3.21 per GB	43%
2,000 GB per day	$1,924 per day	$4,282.80 per day	$6,206.80 per day	$3.11 per GB	44%
5,000 GB per day	$4,550 per day	$10,384.50 per day	$14,934.50 per day	$2.99 per GB	47%

Problematika	ZoKB, VoKB	Minimální technické řešení od MS	Optimální technické řešení od MS
Ochrana koncových zařízení	§12 Řízení přístupu §14 Zvládání kybernetických bezpečnostních událostí a incidentů §18 Bezpečnost komunikačních sítí §21 Ochrana před škodlivým kódem	Intune Microsoft Defender for Endpoint/Servers P1 Microsoft Defender for Office 365 P1	Intune Microsoft Defender for Endpoint/Servers P2 Microsoft Defender for Office 365 P2 DLP for Endpoints
Ochrana informací	§10 Řízení provozu a komunikací §22 Zaznamenávání událostí infomačního a komunikačního systému, uživatelů a administrátorů	Office365 DLP Information Protection	Office365 DLP DLP for Endpoints Information Protection
Ochrana vícefaktorovou autentizací	§12 Řízení přístupu §19 Správa a ověřování identit	Azure Active Directory P1	Azure Active Directory P2
Logování událostí	§22 Zaznamenávání událostí infomačního a komunikačního systému, uživatelů a administrátorů	Intune, Azure Active Directory P1	Intune, Azure Active Directory P2

Problematika	ZoKB, VoKB	Minimální technické řešení od MS	Optimální technické řešení od MS
Vyhodnocování událostí - SIEM	§14 Zvládání kybernetických bezpečnostních událostí a incidentů §22 Zaznamenávání událostí infomačního a komunikačního systému, uživatelů a administrátorů §24 Sběr a vyhodnocování kybernetických bezp. událostí	MS Sentinel	MS Sentinel
Ochrana proti ATP hrozbám	§14 Zvládání kybernetických bezpečnostních událostí a incidentů §21 ochrana před škodlivým kódem §23 detekce kybernetických bezpečnostních událostí §24 Sběr a vyhodnocování kybernetických bezp. událostí §25 Aplikační bezpečnost	Microsoft 365 Defender Microsoft Defender for Endpoint/Servers P1 Microsoft Defender for Office 365 P1 Microsoft Defender for Identity Microsoft Defender for Cloud Apps	Microsoft 365 Defender Microsoft Defender for Endpoint/Servers P2 Microsoft Defender for Office 365 P2 Microsoft Defender for Identity Microsoft Defender for Cloud Apps
Nástroje pro řízení přístupů a identit (včetně mobilních zařízení)	§12 Řízení přístupu §19 Správa a ověřování identit §20 řízení přístupových oprávnění §21 ochrana před škodlivým kódem §25 aplikační bezpečnost	Intune Azure Active Directory P1	Intune Azure Active Directory P2

Národní Program Obnovy pro KYBEZ	§ Vyhlášky 82/2018	§ Vyhlášky NIS2 - vyšší povinnosti	Oblast/Produkt
Pořízení antiviru, Endpoint protection, a obdobných řešení,	§12 Řízení přístupu §14 Zvládání kybernetických bezpečnostních událostí a incidentů §18 Bezpečnost komunikačních sítí §21 Ochrana před škodlivým kódem	§14 Řízení přístupu §15 Zvládání kybernetických bezpečnostních událostí a incidentů §19 Bezpečnost komunikačních sítí §24 Vyhodnocování kybernetických bezpečnostních událostí	Microsoft 365 Defender Microsoft Defender for Endpoint/Servers P1 a P2 Microsoft Defender for Office 365 P1 a P2
Pořízení a implementace nástroje pro analýzu a monitoring síťového provozu,	§14 Zvládání kybernetických bezpečnostních událostí a incidentů §22 Zaznamenávání událostí infomačního a komunikačního systému, uživatelů a administrátorů §24 Sběr a vyhodnocování kybernetických bezp. událostí	§15 Zvládání kybernetických bezpečnostních událostí a incidentů §23 Zaznamenávání událostí §24 Vyhodnocování kybernetických bezpečnostních událostí	MS Sentinel
Pořízení a implementace nástroje pro Multifaktorovou autentizaci,	§12 Řízení přístupu §19 Správa a ověřování identit	§14 Řízení přístupu §19 Bezpečnost komunikačních sítí §20 Správa a ověřování identit §21 Řízení přístupových oprávnění	Azure Active Directory P1 a P2 Intune
Pořízení a implementace nástroje pro LogManagement,	§22 Zaznamenávání událostí infomačního a komunikačního systému, uživatelů a administrátorů	§23 Zaznamenávání událostí	MS Entra, Intune, AAD P1
Pořízení a implementace nástroje pro SandBoxing,	§14 zvládání kybernetických bezpečnostních událostí a incidentů §21 ochrana před škodlivým kódem §23 detekce kybernetických bezpečnostních událostí §24 Sběr a vyhodnocování kybernetických bezp. událostí §25 Aplikační bezpečnost	§15 Zvládání kybernetických bezpečnostních událostí a incidentů §22 Detekce kybernetických bezpečnostních událostí §24 Vyhodnocování kybernetických bezpečnostních událostí	Microsoft Defender for Office 365 P1 a P2

Národní Program Obnovy pro KYBEZ	§ Vyhlášky 82/2018	§ Vyhlášky NIS2 - vyšší povinnosti	Oblast/Produkt
Dodávka a implementace nástroje SIEM, služby SOC,	§14 Zvládání kybernetických bezpečnostních událostí a incidentů §22 Zaznamenávání událostí infomačního a komunikačního systému, uživatelů a administrátorů §24 Sběr a vyhodnocování kybernetických bezp. událostí	§15 Zvládání kybernetických bezpečnostních událostí a incidentů §23 Zaznamenávání událostí §24 Vyhodnocování kybernetických bezpečnostních událostí	MS Sentinel
Dodávka a implementace nástroje z kategorie Advanced Threat Protection,	§14 Zvládání kybernetických bezpečnostních událostí a incidentů §21 ochrana před škodlivým kódem §23 detekce kybernetických bezpečnostních událostí §24 Sběr a vyhodnocování kybernetických bezp. událostí §25 Aplikační bezpečnost	§15 Zvládání kybernetických bezpečnostních událostí a incidentů §22 Detekce kybernetických bezpečnostních událostí §24 Vyhodnocování kybernetických bezpečnostních událostí	Microsoft 365 Defender Microsoft Defender for Endpoint/Servers P1 a P2 Microsoft Defender for Office 365 P1 a P2 Microsoft Defender for Identity Microsoft Defender for Cloud Apps
Dodávka a implementace nástroje pro řízení přístupů a identit (PIM/PAM, atp.),	§12 Řízení přístupu §19 Správa a ověřování identit §20 řízení přístupových oprávnění §21 ochrana před škodlivým kódem §25 aplikační bezpečnost	§14 Řízení přístupu §20 Správa a ověřování identit §21 Řízení přístupových oprávnění §23 Zaznamenávání událostí	MS Entra (Azure Active Directory P1 a P2) MS Sentinel
Pořízení a implementace nástroje pro Mobile/Enterpise device management,	§12 Řízení přístupu §19 Správa a ověřování identit §20 řízení přístupových oprávnění §21 ochrana před škodlivým kódem §25 aplikační bezpečnost	§14 Řízení přístupu §19 Bezpečnost komunikačních sítí §20 Správa a ověřování identit §21 Řízení přístupových oprávnění	MS Entra (Azure Active Directory P1 a P2), Intune