Microsoft Azure

Microsoft Azure Sentinel

Simo Veinstein

Traditional SOC Challenges

Sophistication of threats

High volume of noisy alerts

IT deployment & maintenance

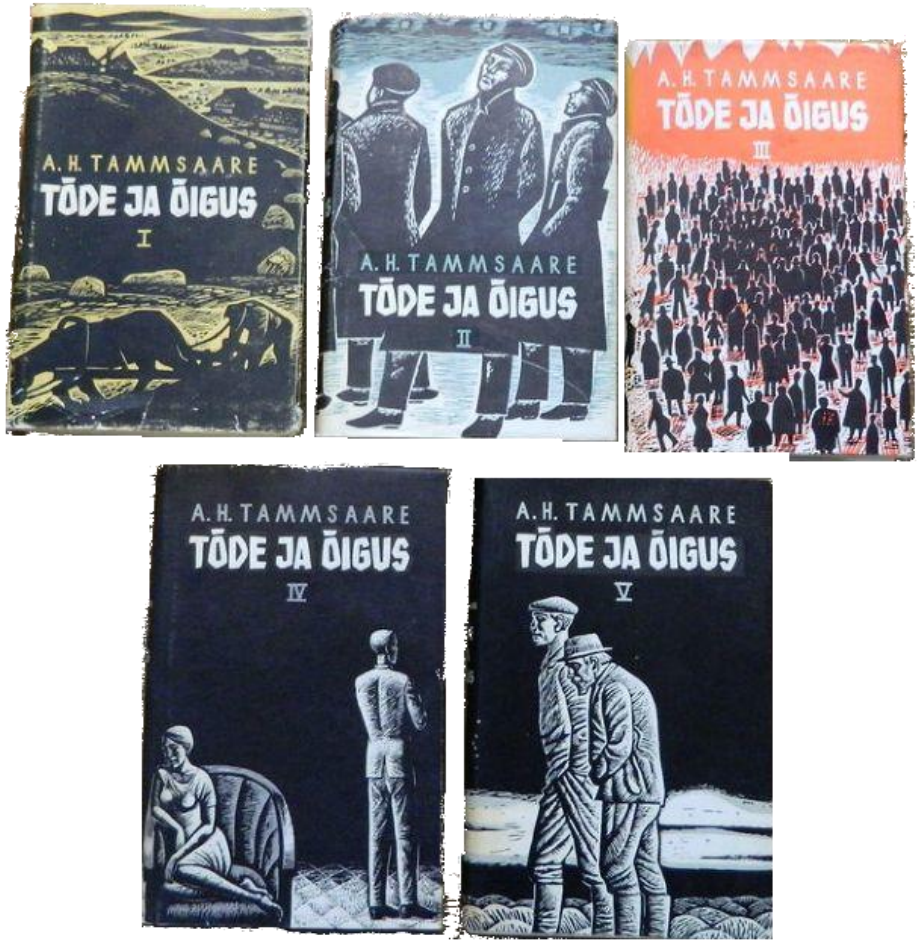
Rising infrastructure costs and upfront investment

Too many disconnected products

Lack of automation

Security skills in short supply

Mis on SIEM (Security Information Event Management) ?



Kuidas SIEM töötab?

Logid Outlooki, jagad OneDrive´is, isiklik telefon ettevõtte võrgus, Teams´ist allalaadimine

Kõik logid kogutakse kokku

Riskprofiilid kasutajatest

Ettearvatav käitumismuster

Azure Sentinel vs tavapärane SIEM

Puudub infrastruktuuri kulu ja esialgne suur investeering.

Puudub vajadus infrastruktuuri seadistada ja hooldada.

Lihtsasti skaleeritav.

Maksa selle eest mida kasutad.

Mida uut pakub Azure Sentinel?

Azure Log Analytics

100% pilvepõhine SIEM

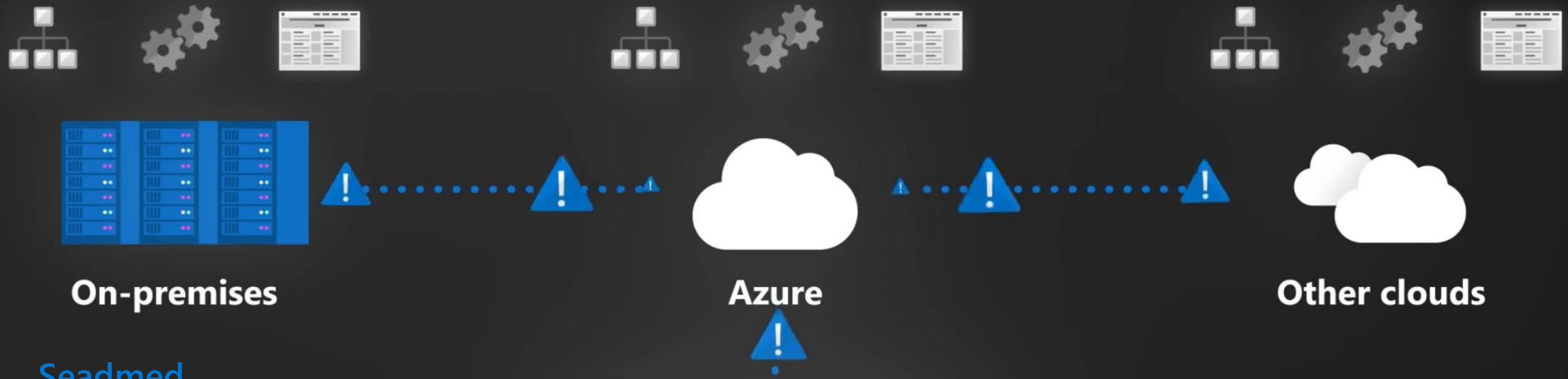
+

AI analüütikaks

+

SOAR – Security orchestration automation and response

Security Center



- Seadmed
- Kasutajad
- Rakendused
- Serverid
- Võrgud
- Erinevad pilved

Tuvasta ohud ja analüüsi logisid kiirelt AI abil

Masinõppe mudelid, mis põhinevad Microsofti pikaaegsel kogemusel.

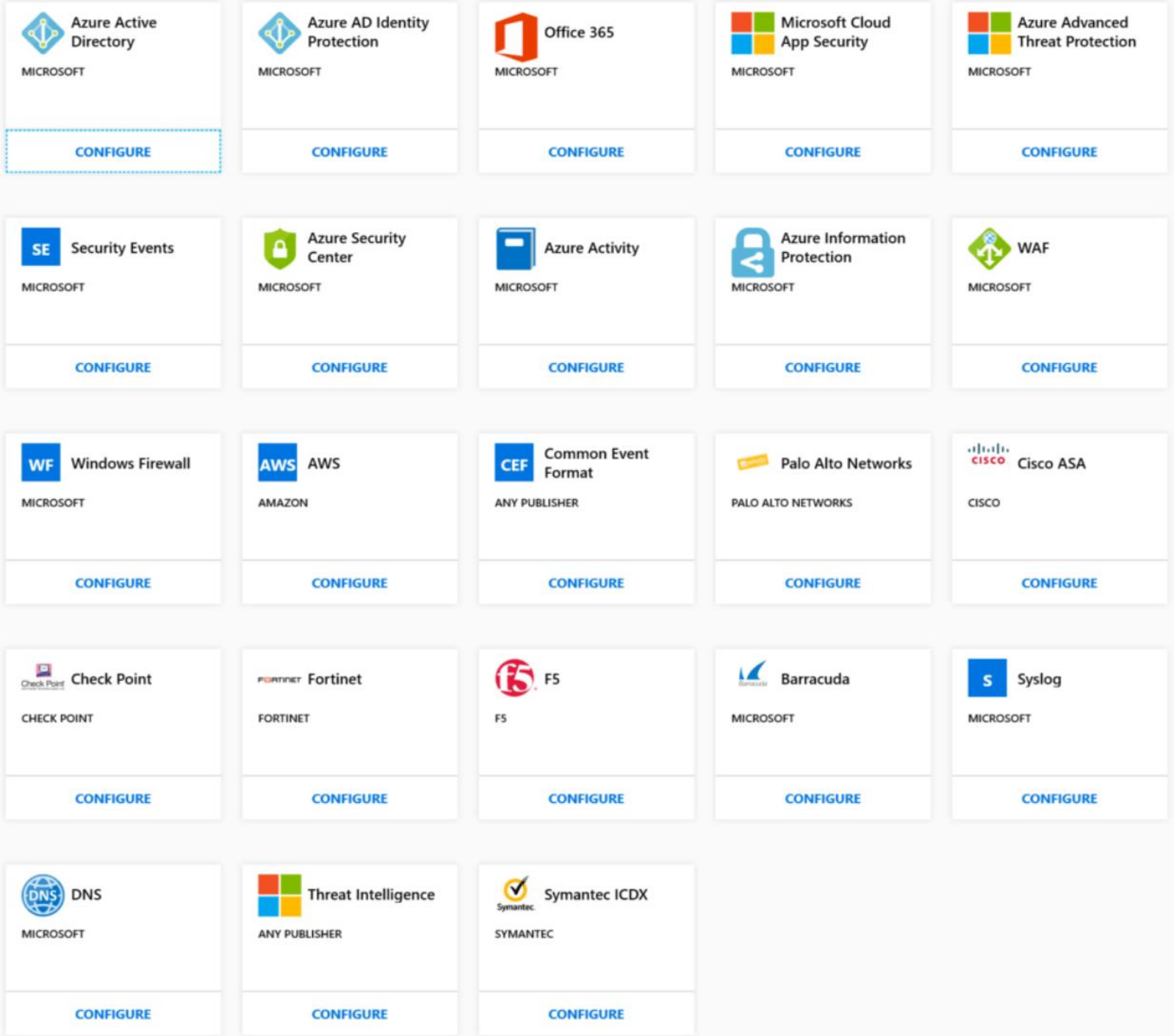
Võimalik tuvastada varasemalt märkamata jäänud ohud.

Miljonid signaalid filtreeritakse, luuakse vastastikused seosed ja prioritiseeritakse.

Integratsioon – olemasolevad tööriistad ja andmeallikad

Microsoft enda lahendused valmis kasutuseks

Connectors – liidestamaks paljud teised osapooled.



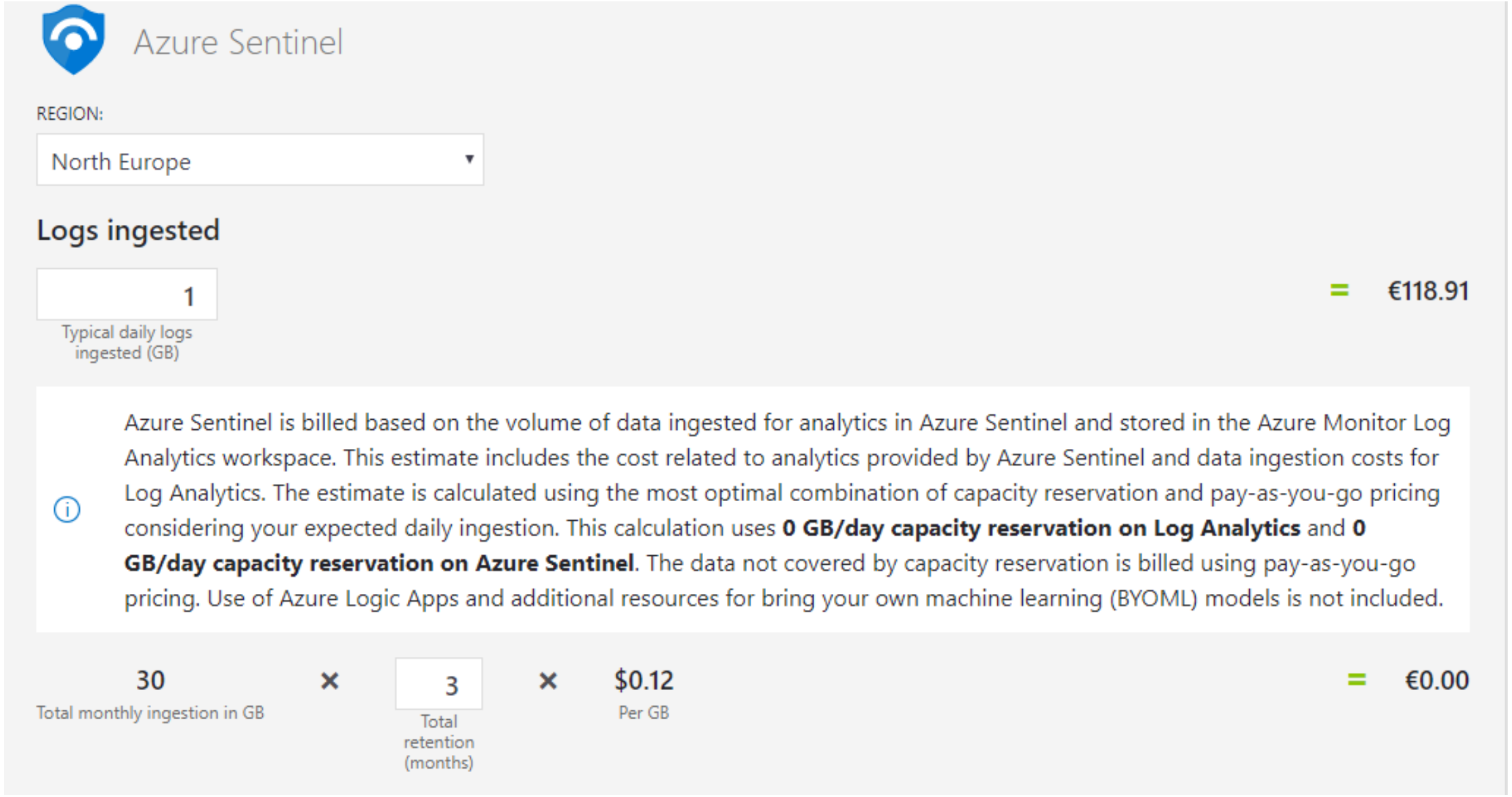
Hinnastus

Tasud mahu eest, mida Log Analytics´isse ja Azure Sentinel söödad.

Logide hoidmine, kuni 3 kuud – tasuta.

Azure Sentinel Data Source	Free Units Included
Azure Activity Logs	Unlimited
Office 365 Audit Logs	Unlimited
Microsoft Threat Protection Logs	Unlimited

Hinnastus


Azure Sentinel
REGION:
North Europe
Logs ingested
1
Typical daily logs ingested (GB)
= €118.91
Azure Sentinel is billed based on the volume of data ingested for analytics in Azure Sentinel and stored in the Azure Monitor Log Analytics workspace. This estimate includes the cost related to analytics provided by Azure Sentinel and data ingestion costs for Log Analytics. The estimate is calculated using the most optimal combination of capacity reservation and pay-as-you-go pricing considering your expected daily ingestion. This calculation uses 0 GB/day capacity reservation on Log Analytics and 0 GB/day capacity reservation on Azure Sentinel. The data not covered by capacity reservation is billed using pay-as-you-go pricing. Use of Azure Logic Apps and additional resources for bring your own machine learning (BYOML) models is not included.
30
Total monthly ingestion in GB
×
3
Total retention (months)
×
$0.12
Per GB
= €0.00

Tänud kuulamast!

Mis? Kus? Kuidas?

KIIRKOHTINGUTEST

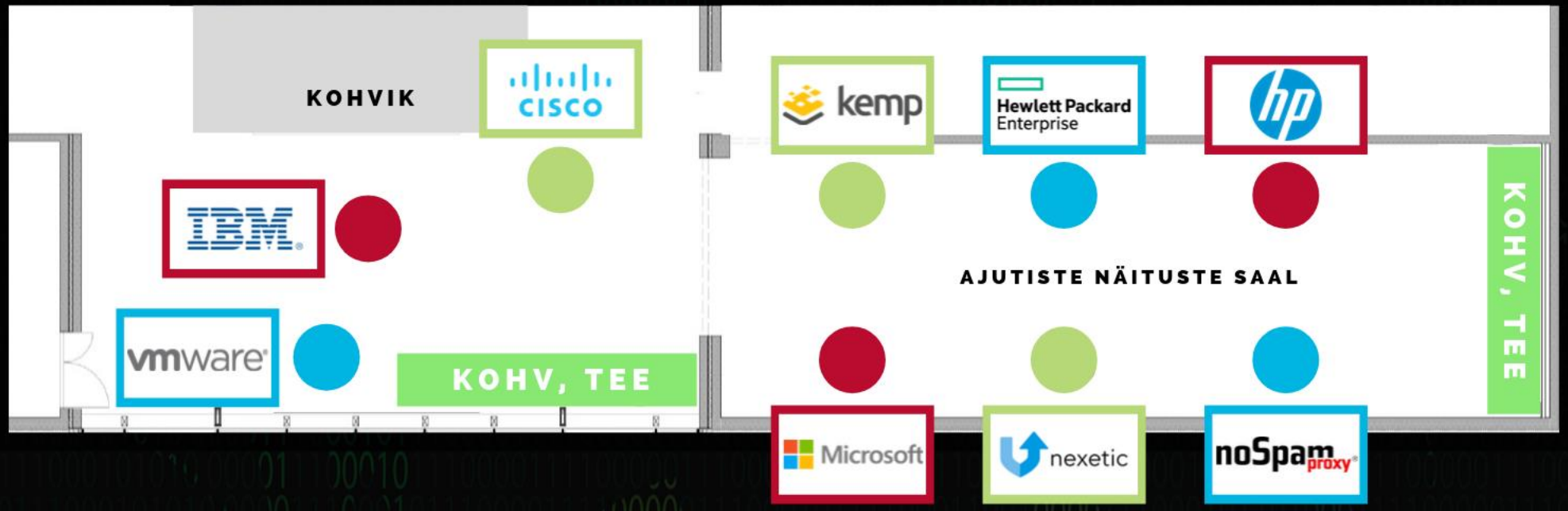
ALSO Akadeemia

		1	2	3	4	5	6	7	8	9
		11:06:00	11:12:00	11:18:00	11:24:00	11:30:00	11:36:00	11:42:00	11:48:00	11:54:00
1	NoSpamProxy									
2	Nexetic									
3	Microsoft									
4	HP									
5	HP Enterprise									
6	KEMP									
7	IBM									
8	VMware									
9	Cisco									

SECURITY DAY

Kiirkohtingud & expo ala

ALSO Akadeemia



SECURITY DAY