

# Microsoft Azure Sentinel

Simo Veinstein



## Traditional SOC Challenges

Sophistication of threats

High volume of noisy alerts

IT deployment & maintenance

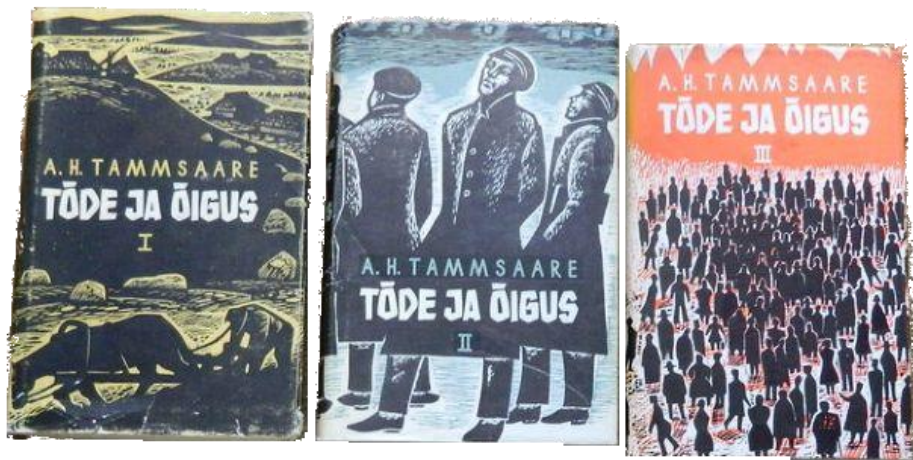
Rising infrastructure costs and upfront investment

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?

100% pilvepõhine SIEM

+

AI analüütikaks

+

SOAR – Security orchestration automation  
and response



Azure Log Analytics



Security Center



**On-premises**

**Azure**

**Other clouds**



Seadmed

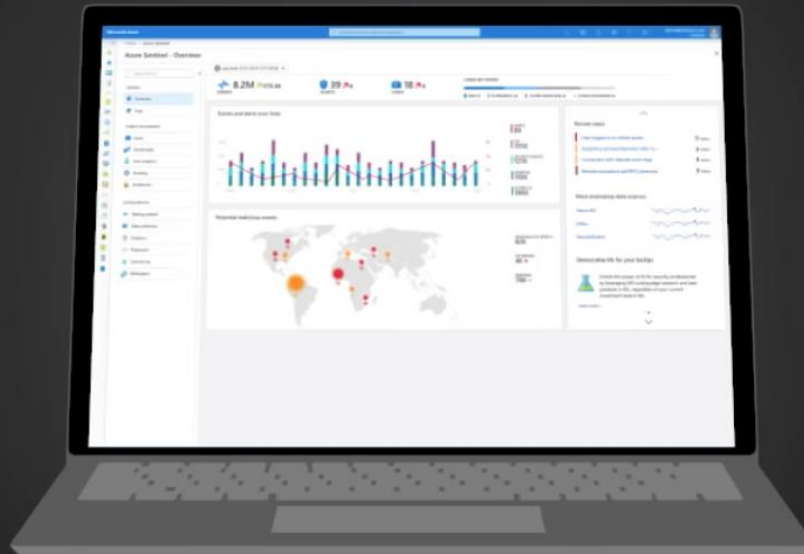
Kasutajad

Rakendused

Serverid

Võrgud

Erinevad pilved



# Tuvasta ohud ja analüüsi logisid kiirelt AI abil

Masinõppe mudelid, mis põhinevad Microsofti pikaajasel kogemusel.

Võimalik tuvastada varasemalt märkamata jäänud ohud.
























Miljonid signaalid filtreeritakse, luuakse vastastikused seosed ja prioritseeritakse.



# Integratsioon – olemasolevad tööriistad ja andmeallikad

Microsoft enda lahendused valmis kasutuseks

Connectors – liidestamiseks paljud teised osapooled.

|  |  |   |  |  |
|--|--|---|--|--|
|  <p>Azure Active Directory<br/>MICROSOFT</p> <p>CONFIGURE</p> |  <p>Azure AD Identity Protection<br/>MICROSOFT</p> <p>CONFIGURE</p> |  <p>Office 365<br/>MICROSOFT</p> <p>CONFIGURE</p>                |  <p>Microsoft Cloud App Security<br/>MICROSOFT</p> <p>CONFIGURE</p>   |  <p>Azure Advanced Threat Protection<br/>MICROSOFT</p> <p>CONFIGURE</p> |
|  <p>Security Events<br/>MICROSOFT</p> <p>CONFIGURE</p>      |  <p>Azure Security Center<br/>MICROSOFT</p> <p>CONFIGURE</p>      |  <p>Azure Activity<br/>MICROSOFT</p> <p>CONFIGURE</p>          |  <p>Azure Information Protection<br/>MICROSOFT</p> <p>CONFIGURE</p> |  <p>WAF<br/>MICROSOFT</p> <p>CONFIGURE</p>                            |
|  <p>Windows Firewall<br/>MICROSOFT</p> <p>CONFIGURE</p>     |  <p>AWS<br/>AMAZON</p> <p>CONFIGURE</p>                           |  <p>Common Event Format<br/>ANY PUBLISHER</p> <p>CONFIGURE</p> |  <p>Palo Alto Networks<br/>PALO ALTO NETWORKS</p> <p>CONFIGURE</p>  |  <p>Cisco ASA<br/>CISCO</p> <p>CONFIGURE</p>                          |
|  <p>Check Point<br/>CHECK POINT</p> <p>CONFIGURE</p>        |  <p>Fortinet<br/>FORTINET</p> <p>CONFIGURE</p>                    |  <p>F5<br/>F5</p> <p>CONFIGURE</p>                             |  <p>Barracuda<br/>MICROSOFT</p> <p>CONFIGURE</p>                    |  <p>Syslog<br/>MICROSOFT</p> <p>CONFIGURE</p>                         |
|  <p>DNS<br/>MICROSOFT</p> <p>CONFIGURE</p>                |  <p>Threat Intelligence<br/>ANY PUBLISHER</p> <p>CONFIGURE</p>  |  <p>Symantec ICDX<br/>SYMANTEC</p> <p>CONFIGURE</p>          |  |  |

# Azure Sentinel - Overview

Search (Ctrl+F)

- GENERAL
  - Overview
  - Logs
- THREAT MANAGEMENT
  - Incidents
  - Dashboards
  - User analytics
  - Hunting
  - Notebooks
- CONFIGURATION
  - Getting started
  - Data collection
  - Analytics
  - Playbooks
  - Community
  - Workspace

Last week (1/21/2018-1/27/2018)

**8.2M** ↑ 978.4K

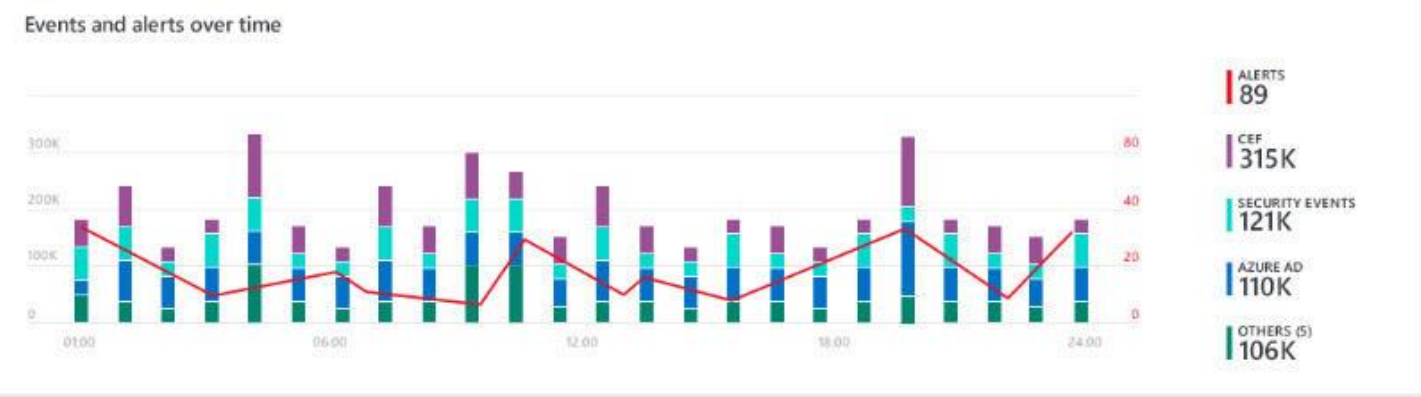
EVENTS

**39** ↑ 6

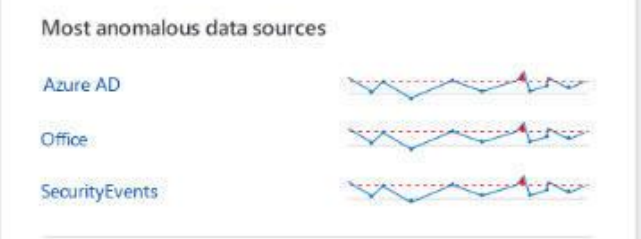
ALERTS

**18** ↑ 4

INCIDENTS



- ### Recent incidents
- User logged in to critical assets 9 Alerts
  - Suspicious process execution after co... 9 Alerts
  - Computers with cleaned event logs 8 Alerts
  - Remote procedure call (RPC) attempts 8 Alerts



### Democratize ML for your SecOps

Unlock the power of AI for security professionals by leveraging MS cutting edge research and best practices in ML, regardless of your current investment level in ML.

[Learn more >](#)

# 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

**Tänu** kuulamast!

# Mis? Kus? Kuidas?

## KIIRKOHTINGUTEST



|                 | 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   |          |          | Blue     |          |          | Green    |          | Red      |          |
| 2 Nexetic       | Green    |          |          |          | Red      |          |          |          | Blue     |
| 3 Microsoft     |          | Red      |          | Green    |          |          | Blue     |          |          |
| 4 HP            |          |          | Red      |          |          | Blue     |          | Green    |          |
| 5 HP Enterprise | Blue     |          |          |          | Green    |          |          |          | Red      |
| 6 KEMP          |          | Green    |          | Blue     |          |          | Red      |          |          |
| 7 IBM           |          |          | Green    |          |          | Red      |          | Green    |          |
| 8 VMware        | Red      |          |          |          | Green    |          |          |          | Green    |
| 9 Cisco         |          | Green    |          | Red      |          |          | Green    |          |          |

**SECURITY DAY**

# Kiirkohtingud & expo ala

**ALSO**  
Akadeemia



**SECURITY DAY**