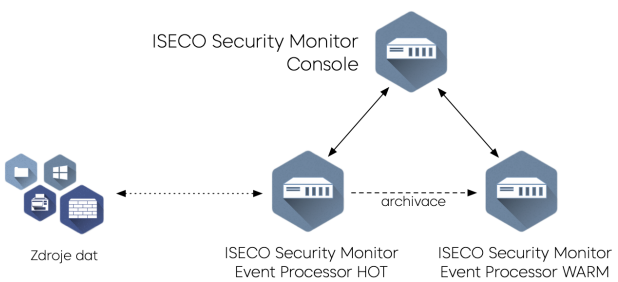
ISECO

www.iseco.cz

Víceúrovňová architektura uložiště pro ISECO Security Monitor

Gold Partner

Nasazení je vždy kombinací 1x konzole, Event Processor HOT a Event Processor WARM, kde pro každých 40 000 EPS příchozích dat je nezbytný jeden další HOT event processor.



Víceúrovňová architektura uložiště pro systémy typu Log Management a SIEM obecně umožňuje optimalizovat požadavky na rychlost hledání v systému a zároveň minimalizovat náklady na uložiště.

Řešení ISECO Security Monitor na platformě IBM QRadar rozšiřuje možnosti IBM QRadar a podporuje možnost nasazení s víceúrovňovou architekturou uložišť ve dvou základních úrovních:

- HOT – pro aktuální data s požadavkem nejrychlejšího hledání
- WARM – pro online dostupná v systému, nicméně starší než definovaná doba

Tabulka níže shrnuje možnosti nasazení ISECO Security Monitor na základě architektury řešení, kde nasazení s víceúrovňovou architekturou uložišť je možná pouze pro distribuovanou architekturu. Dále platí omezení, kdy pro nasazení pro větší než 5000 EPS je nezbytné využít ISECO Security Monitor appliances garantující bezproblémové zpracování příchozích dat.

Architektura	Virtualizace	ISECO Appliance
All-in-one	N/A	N/A
Distribuovaná, do 5000 EPS	ANO	ANO
Distribuovaná, nad 5000 EPS	N/A	ANO

HOT

ISM Appliance Plus HOT

- 2U
- 2x Intel Xeon Silver 4310 – 2,1GHz 18MB cache 12core, HT, 120W, LGA4189 4,1P/2P,6TB, 2666MHz
- 8x 32GB 3200MHz DDR4
- 12x SSD 7,68TB SATA3 6Gbps 2,5" 97/26k IOPS 550/520 MB/s v RAID 6, HW řadič s cache
- 2x SSD 480GB, 97/60k IOPS 560/530 MB/s v RAID 1, HW řadič s cache
- 4x 1 GbE
- 2x 10 GbE SFP+

WARM

ISM Appliance Plus WARM – 220 TB

- 2U
- 2x Intel Xeon Silver 4310 – 2,1GHz 18MB cache 12core, HT, 120W, LGA4189 4,1P/2P, 6TB, 2666MHz
- 8x 32GB 3200MHz DDR4
- 12x 22TB 7200rpm, SAS3 v RAID 6, HW řadiče cache
- 2x SSD 480GB, 97/60k IOPS 560/530 MB/s v RAID 1, HW řadič s cache
- 4x 1 GbE
- 2x 10 GbE SFP+

E-mail
info@iseco.cz

Tel.
+420 234 760 570

Adresa
ISECO.CZ s.r.o., Bartůňkova 2349/3a, Chodov 149 00 Praha 4