medcom

Sikkerhed i SDNv4

3. oktober 2024

Agenda

- Kontraktkrav
- Driftssikkerhed
- Cybersikkerhed - SIEM / SOC
- Sårbarhedsskanning af SDN-services (udstillede og egne services)
- GDPR og NIS2
- Opsamling og spørgsmål

Kontraktkrav

- Omfattende mindstekrav i udbud og kontrakt herunder:
  - ISO27001 og CIS kontroller
  - Sårbarhedsskanning og penetrationstest
  - Håndtere advarsler fra CFCS og DCIS Sund
  - Logning og backup
  - Beredskab og rapportering af sikkerhedshændelser
  - Risikovurdering
- IDS/IPS
- SIEM / SOC

Driftsovervågning SDNv3

Device Manager | Devices Found [21]

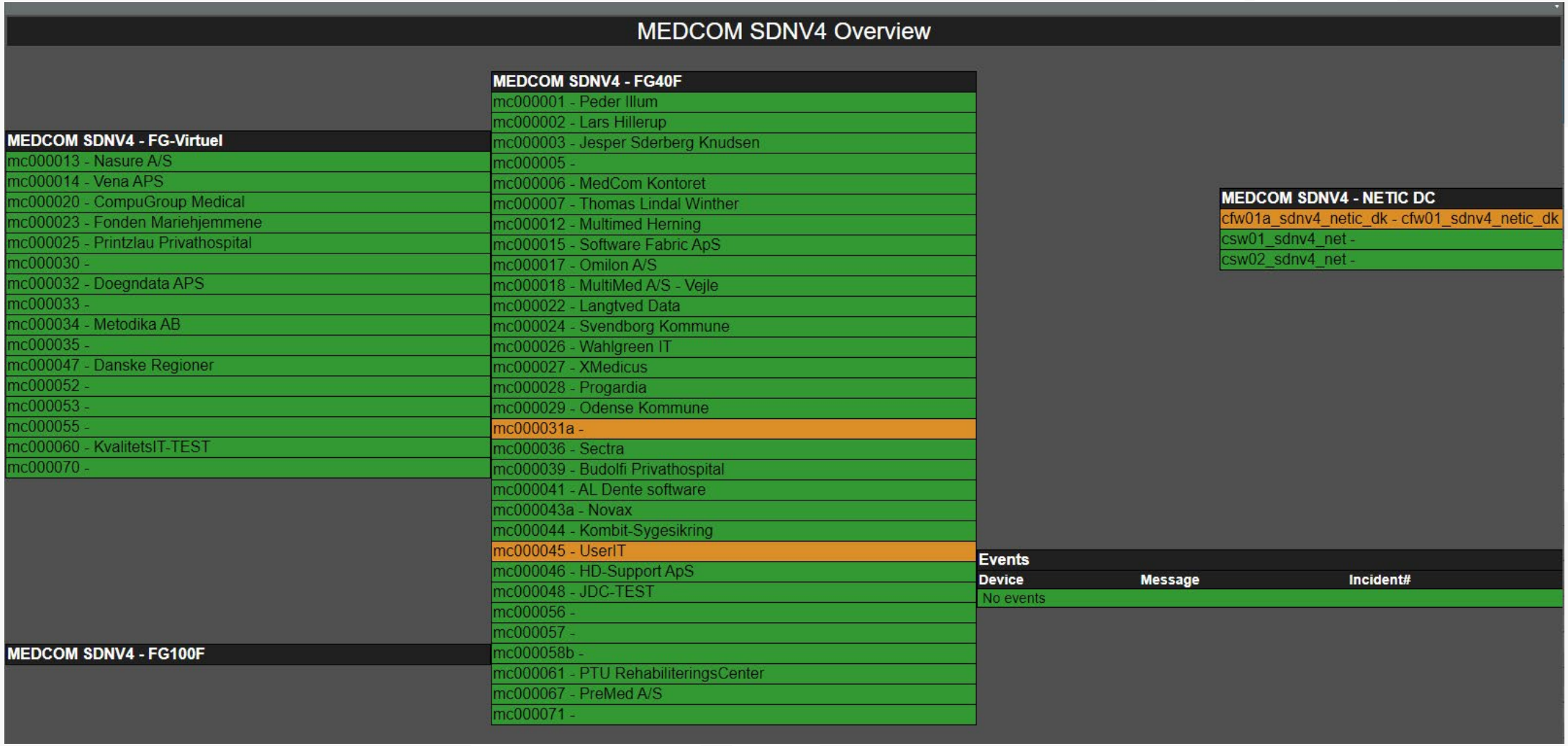
	Device Name	IP Address	Device Category	Device Class | Sub-class	DID	Organization	Current State
	sdn3						>=Healthy
1.	SDN3-SW-1.medcom	195.80.253.40	Network.Modules	Cisco Systems | C68xx Virtual Switch	22337	Medcom	Healthy
2.	SDN3-SP-2-Hvidovre.medcom	172.31.253.106	Network.Switches	Cisco Systems | Catalyst 36xx Stackable Ethernet	22336	Medcom	Healthy
3.	SDN3-SP-1-Ringsted.medcom	172.31.253.98	Network.Switches	Cisco Systems | Catalyst 36xx Stackable Ethernet	21473	Medcom	Healthy
4.	SDN3-RN-2.medcom	172.31.254.46	Network.Router	Cisco Systems | Cat9300FixedSwitchStack	16645	Medcom	Healthy
5.	SDN3-RN-1.medcom	172.31.254.42	Network.Router	Cisco Systems | Cat9300FixedSwitchStack	16642	Medcom	Healthy
6.	SDN3-RMGOD.medcom	195.80.240.209	Network.Router	Cisco Systems | Cat9300FixedSwitchStack	148979	Medcom	Healthy
7.	SDN3-RMAAR.medcom	195.80.240.201	Network.Router	Cisco Systems | Cat9300FixedSwitchStack	76199	Medcom	Healthy
8.	SDN3-RGH-2.medcom	172.31.253.10	Network.Router	Cisco Systems | Cat9300FixedSwitchStack	66706	Medcom	Healthy
9.	SDN3-RGH-1.medcom	172.31.253.14	Network.Router	Cisco Systems | Cat9300FixedSwitchStack	66701	Medcom	Healthy
10.	SDN3-RegSJ-Sla.medcom	172.31.253.170	Network.Router	Cisco Systems | Cat9300FixedSwitchStack	16650	Medcom	Healthy
11.	SDN3-RegSJ-Rin.medcom	172.31.253.174	Network.Router	Cisco Systems | Cat9300FixedSwitchStack	16653	Medcom	Healthy
12.	SDN3-Regnod_AAS	172.31.254.234	Network.Router	Cisco Systems | Cat9300FixedSwitchStack	82924	Medcom	Healthy
13.	SDN3-Regnod-IThuset	172.31.254.238	Network.Router	Cisco Systems | Cat9300FixedSwitchStack	16652	Medcom	Healthy
14.	SDN3-REG-SYD-2.medcom	172.31.254.78	Network.Router	Cisco Systems | Cat9300FixedSwitchStack	16655	Medcom	Healthy
15.	SDN3-REG-SYD-1.medcom	172.31.254.82	Network.Router	Cisco Systems | Cat9300FixedSwitchStack	80017	Medcom	Healthy
16.	SDN3-KMD-2.medcom	195.80.240.233	Network.Router	Cisco Systems | Cat9300FixedSwitchStack	16640	Medcom	Healthy
17.	SDN3-KMD-1.medcom	195.80.240.241	Network.Router	Cisco Systems | Cat9300FixedSwitchStack	73057	Medcom	Healthy
18.	SDN3-IBM-LMS-2.medcom	172.31.254.118	Network.Switches	Cisco Systems | Catalyst 36xx Stackable Ethernet	16654	Medcom	Healthy
19.	SDN3-IBM-LMS-1.medcom	172.31.254.117	Network.Switches	Cisco Systems | Catalyst 36xx Stackable Ethernet	16656	Medcom	Healthy
20.	SDN3-HUB-2.medcom	195.80.253.45	Network.Router	Cisco Systems | ASR 1001-X	22353	Medcom	Healthy
21.	SDN3-HUB-1.medcom	195.80.253.44	Network.Router	Cisco Systems | ASR 1001-X	22352	Medcom	Healthy

Driftsovervågning SDNv4

Device Manager | Devices Found [49]

	Device Name	IP Address	Device Category	Device Class | Sub-class	DID	Organization	Current State
	sdnv4,mc						>=Healthy
26.	mc000029	100.100.64.30	Network.Firewall	Fortinet | FortiGate-40F	207654	Medcom	Healthy
27.	mc000028	100.100.64.29	Network.Firewall	Fortinet | FortiGate-40F	210126	Medcom	Healthy
28.	mc000027	100.100.64.28	Network.Firewall	Fortinet | FortiGate-40F	210127	Medcom	Healthy
29.	mc000026	100.100.64.27	Network.Firewall	Fortinet | FortiGate-40F	207582	Medcom	Healthy
30.	mc000025	100.100.64.26	Network.Firewall	Fortinet | FortiGate VM	210125	Medcom	Healthy
31.	mc000024	100.100.64.25	Network.Firewall	Fortinet | FortiGate-40F	208698	Medcom	Healthy
32.	mc000023	100.100.64.24	Network.Firewall	Fortinet | FortiGate VM	207365	Medcom	Healthy
33.	mc000022	100.100.64.23	Network.Firewall	Fortinet | FortiGate-40F	208469	Medcom	Healthy
34.	mc000020	100.100.64.21	Network.Firewall	Fortinet | FortiGate VM	210124	Medcom	Healthy
35.	mc000018	100.100.64.19	Network.Firewall	Fortinet | FortiGate-40F	208491	Medcom	Healthy
36.	mc000017	100.100.64.18	Network.Firewall	Fortinet | FortiGate-40F	211037	Medcom	Healthy
37.	mc000015	100.100.64.16	Network.Firewall	Fortinet | FortiGate-40F	206783	Medcom	Healthy
38.	mc000014	100.100.64.15	Network.Firewall	Fortinet | FortiGate VM	206688	Medcom	Healthy
39.	mc000013	100.100.64.14	Network.Firewall	Fortinet | FortiGate VM	206684	Medcom	Healthy
40.	mc000012	100.100.64.13	Network.Firewall	Fortinet | FortiGate-40F	204627	Medcom	Healthy
41.	mc000007	100.100.64.8	Network.Firewall	Fortinet | FortiGate-40F	204631	Medcom	Healthy
42.	mc000006	100.100.64.7	Network.Firewall	Fortinet | FortiGate-40F	192280	Medcom	Healthy
43.	mc000005	100.100.64.6	Network.Firewall	Fortinet | FortiGate-40F	204628	Medcom	Healthy
44.	mc000003	100.100.64.4	Network.Firewall	Fortinet | FortiGate-40F	192283	Medcom	Healthy
45.	mc000002	100.100.64.3	Network.Firewall	Fortinet | FortiGate-40F	192282	Medcom	Healthy
46.	mc000001	100.100.64.2	Network.Firewall	Fortinet | FortiGate-40F	192281	Medcom	Healthy
47.	csw02_sdnv4_net	100.100.3.3	Network.Switches	Fortinet | FortiSwitch 1048E	191453	Medcom	Healthy
48.	csw01_sdnv4_net	100.100.3.4	Network.Switches	Fortinet | FortiSwitch 1048E	191452	Medcom	Healthy

Driftsovervågning - dashboard



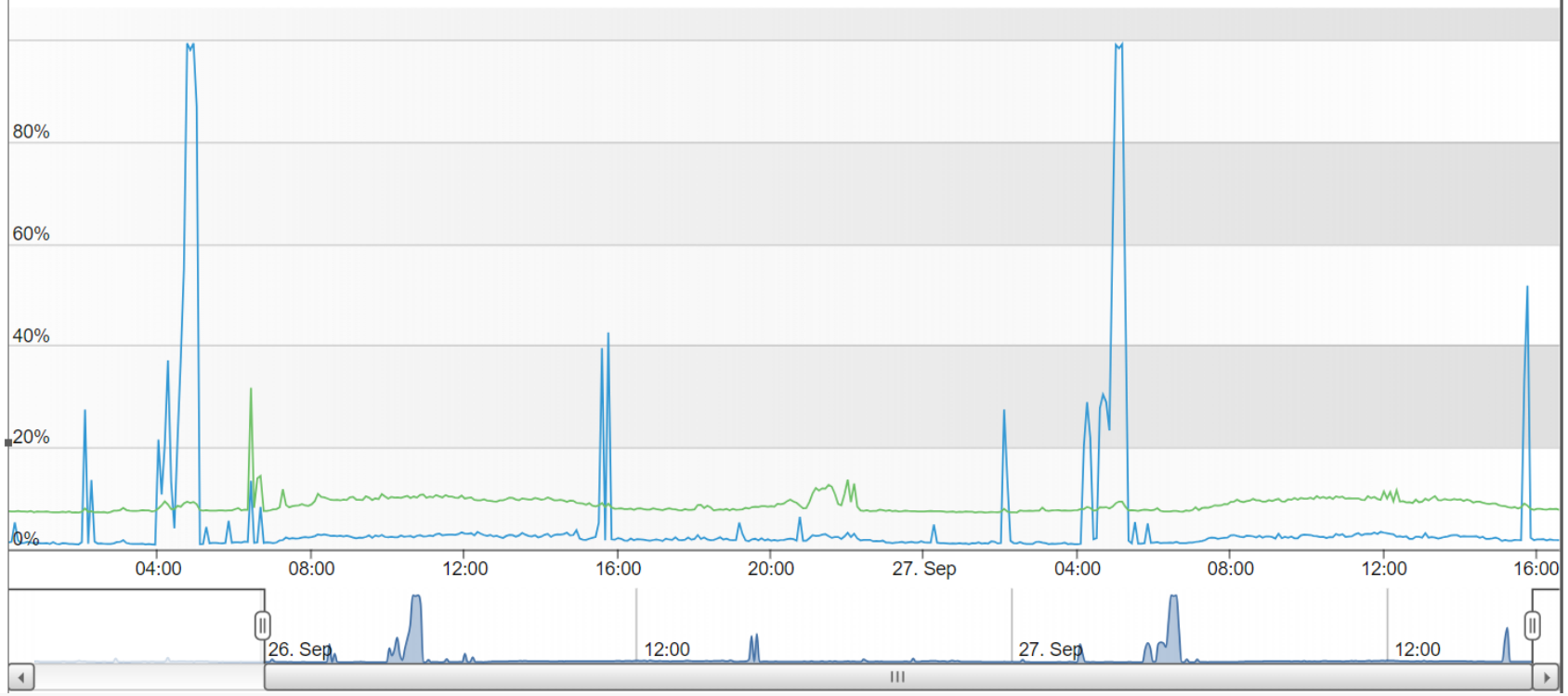
Driftsovervågning - detaljer

Device Name	SDN3-SP-1-Ringsted.medcom	Managed Type	Physical Device
IP Address / ID	172.31.253.98 | 21473	Category	Network.Switches
Class	Cisco Systems	Sub-Class	Catalyst 36xx Stackable Ethernet
Organization	Medcom	Uptime	1067 days, 16:39:59
Collection Mode	Active	Collection Time	2024-09-27 16:35:00
Description	Cisco IOS Software [Gibraltar], Catalyst L3 Switch Software (CAT3K_CAA-	Group / Collector	MEDCOM | ov-em7-medcom-dcol1
Device Hostname			

- Overview
- Network Interfaces
  - > Link mod TDC HX918333/C0151212 <
    - Utilization (%)
    - Bandwidth Usage
    - Bandwidth Usage (Stacked)
    - Errors and Discards
    - Errors and Discards (%)
    - Packets
    - Packets (%)
- Cisco: Physical Memory
- Cisco: CPU
- Cisco: BGP Peer Stats
- .BGP Activity & State
- Cisco: BGP Route Counts
- NetDesign: Cisco Temperature Sensor Performance

Options | Report | **Network Utilization Report \| > Link Mod TDC HX918333/C0151212 < \| a0:e0:af:93:26:9c** | Reset | Guide

Zoom 6H 12H 1D Max — From: 09/26/2024 00:05 To: 09/27/2024 16:35



Driftsovervågning - alarmopsætning

Device Name	mc000001	Managed Type	Physical Device
IP Address / ID	100.100.64.2 | 192281	Category	Network.Firewall
Class	Fortinet	Sub-Class	FortiGate-40F
Organization	Medcom	Uptime	63 days, 20:11:34
Collection Mode	Active	Collection Time	2024-09-27 16:30:00
Description	Peder Illum	Group / Collector	MEDCOM | ov-em7-medcom-dcol1
Device Hostname			

Device Thresholds — Actions | Reset | Guide

Dynamic App Thresholds | NetDesign: FortiGate (CPU/MEM/DISK)

CPU	80 %	[Default: 80]	
Memory	80 %	[Default: 80]	
Raw Data Retention	15 days	[Default: 15]	
Hourly Rollup Retention	90 days	[Default: 90]	
Daily Rollup Retention	360 days	[Default: 360]	

Device Name	mc000001	Managed Type	Physical Device
IP Address / ID	100.100.64.2 | 192281	Category	Network.Firewall
Class	Fortinet	Sub-Class	FortiGate-40F
Organization	Medcom	Uptime	63 days, 20:11:34
Collection Mode	Active	Collection Time	2024-09-27 16:30:00
Description	Peder Illum	Group / Collector	MEDCOM | ov-em7-medcom-dcol1
Device Hostname			

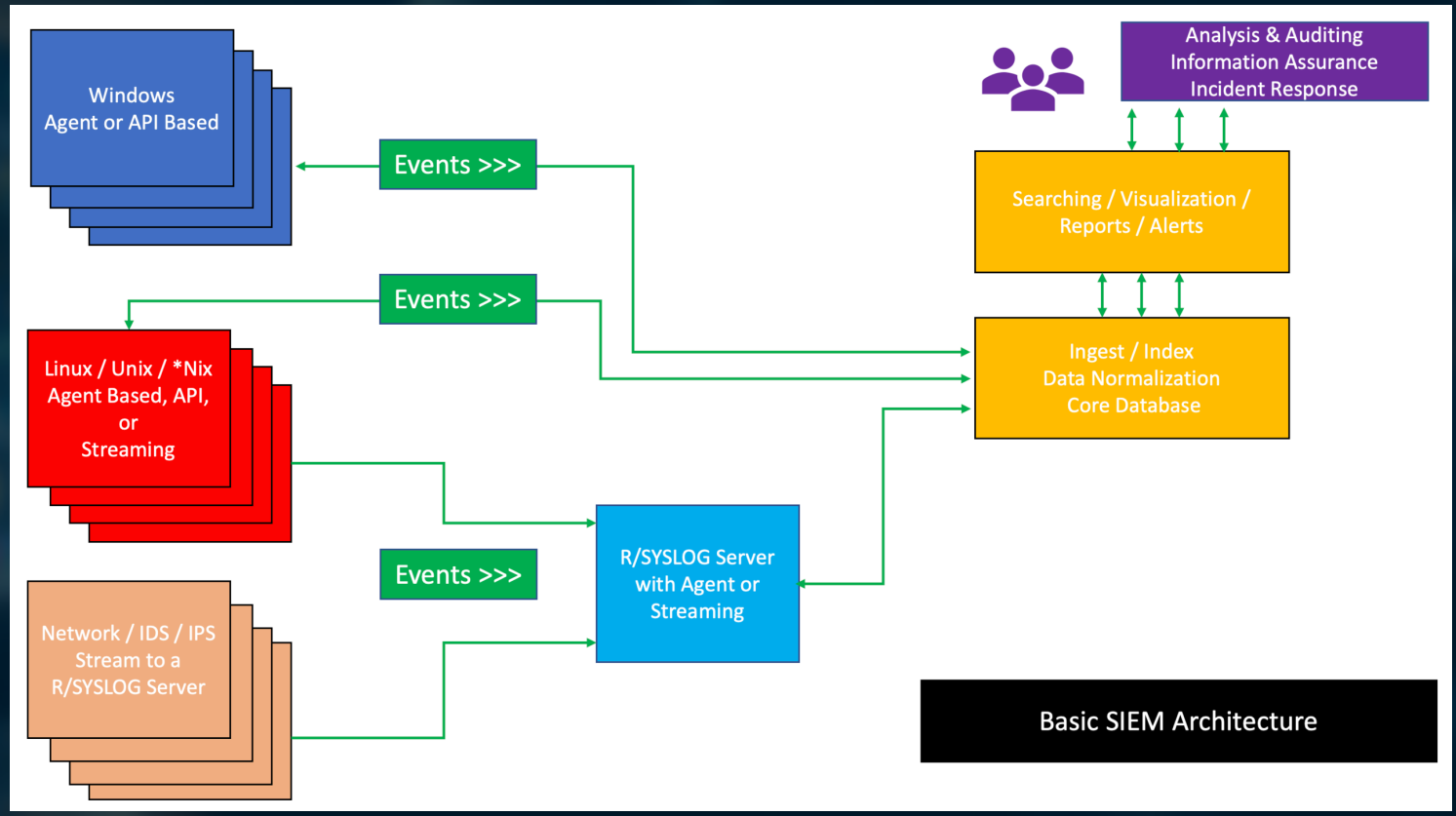
Device Thresholds — Actions | Reset | Guide

Operating System Thresholds

System Latency	200 ms	[Default: 200 ms]
System Availability	99 %	[Default: 99 %]

Security information and event management systems

- Primary purpose of a SIEM
  - Data aggregation & correlation
  - Alerting
  - Dashboads
  - Compliance
  - Retention
  - Forensics analysis
- SIEM solutions
  - Elasticsearch
  - Splunk
  - Qradar
  - Sentinel



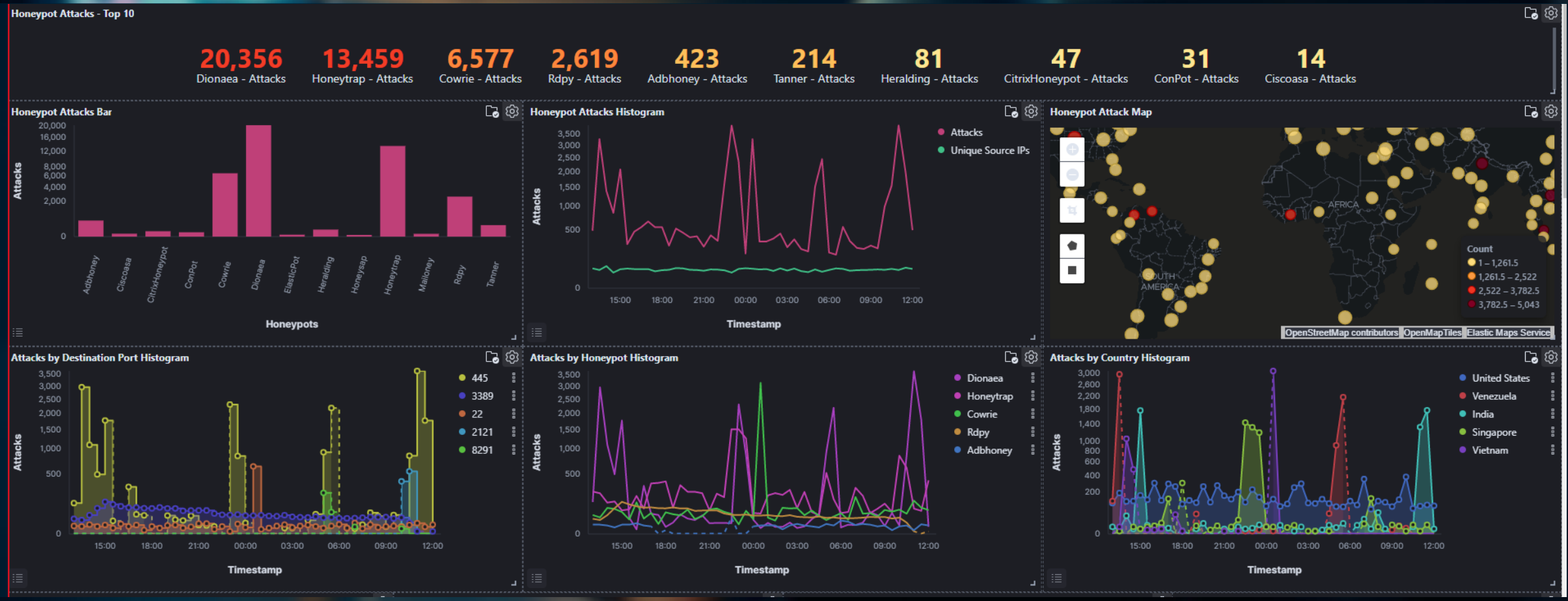
Parsing of log data

```
Jul 03 2014 14:33:09: %ASA-6-302014: Teardown TCP connection 806405 for
 inside:10.0.0.100/50554 to identity:172.18.124.136/51358 duration 0:00:00 bytes
 442 TCP Reset-I
```

```
An account was successfully logged on.

Subject:
        Security ID:            SYSTEM
        Account Name:           DESKTOP-TEST533$
        Account Domain:         NETDESIGN
        Logon ID:               0x3E7

Logon Information:
        Logon Type:             5
        Restricted Admin Mode:  -
        Virtual Account:                No
        Elevated Token:         Yes

Impersonation Level:            Impersonation

New Logon:
        Security ID:            SYSTEM
        Account Name:           SYSTEM
        Account Domain:         NT AUTHORITY
        Logon ID:               0x3E7
        Linked Logon ID:                0x0
        Network Account Name:   -
        Network Account Domain: -
        Logon GUID:             {00000000-0000-0000-0000-000000000000}

Process Information:
        Process ID:             0x470
        Process Name:           C:\Windows\System32\services.exe

Network Information:
```

geoip_ext.continent_code	EU
geoip_ext.country_code2	DK
geoip_ext.country_code3	DK
geoip_ext.country_name	Denmark
geoip_ext.ip	87.63.238.94
geoip_ext.latitude	55.688
geoip_ext.location	POINT (12.5589 55.6786)
geoip_ext.longitude	12.563
geoip_ext.postal_code	2450
geoip_ext.region_code	84
geoip_ext.region_name	Capital Region
geoip_ext.timezone	Europe/Copenhagen
geoip.as_org	MnogoByte LLC

SIEM dashboards



Vores logs

Datasets with hosts

Top 50 values of event.dataset	Top 300 values of host.name	Count of records
forti.manager	medsdncol01	2,141,007
microsoft.wineventlog.security	WIN-1CGDMF7UON0	1,381,276
linux.systemd	sdn-aft-worker01-drift	756,890
linux.systemd-networkd	sdn-aft-worker01-drift	65,502
linux.ntpd	sdn-aft-worker01-drift	45,861
forti.analyzer	faz_sdnv4_netic_dk	42,993
linux.kernel	sdn-aft-worker01-drift	25,189
linux.networkd-dispatcher	sdn-aft-worker01-drift	13,109
microsoft.wineventlog.system	WIN-1CGDMF7UON0	12,609
linux.systemd-udevd	sdn-aft-worker01-drift	9,992
linux.freshclam	sdn-aft-worker01-drift	4,815
linux.CRON	sdn-aft-worker01-drift	1,452
linux.rke2	sdn-aft-worker01-drift	1,412
linux.fwupdmgr	sdn-aft-worker01-drift	1,324
linux.apt.systemd.daily	sdn-aft-worker01-drift	676
linux.crond	sdn-aft-worker01-drift	375
microsoft.wineventlog.application	WIN-1CGDMF7UON0	277
linux.unattended-upgrade	sdn-aft-worker01-drift	216
linux.50-motd-news	sdn-aft-worker01-drift	168
linux.dbus-daemon	sdn-aft-worker01-drift	158
linux.snapd	sdn-aft-worker01-drift	133
linux.multipathd	sdn-aft-worker01-drift	102
linux.cloud-init	sdn-aft-worker01-drift	66
linux.sshd	sdn-aft-worker01-drift	33
linux.multipath	sdn-aft-worker01-drift	32
linux.VGAuthService	sdn-aft-worker01-drift	18

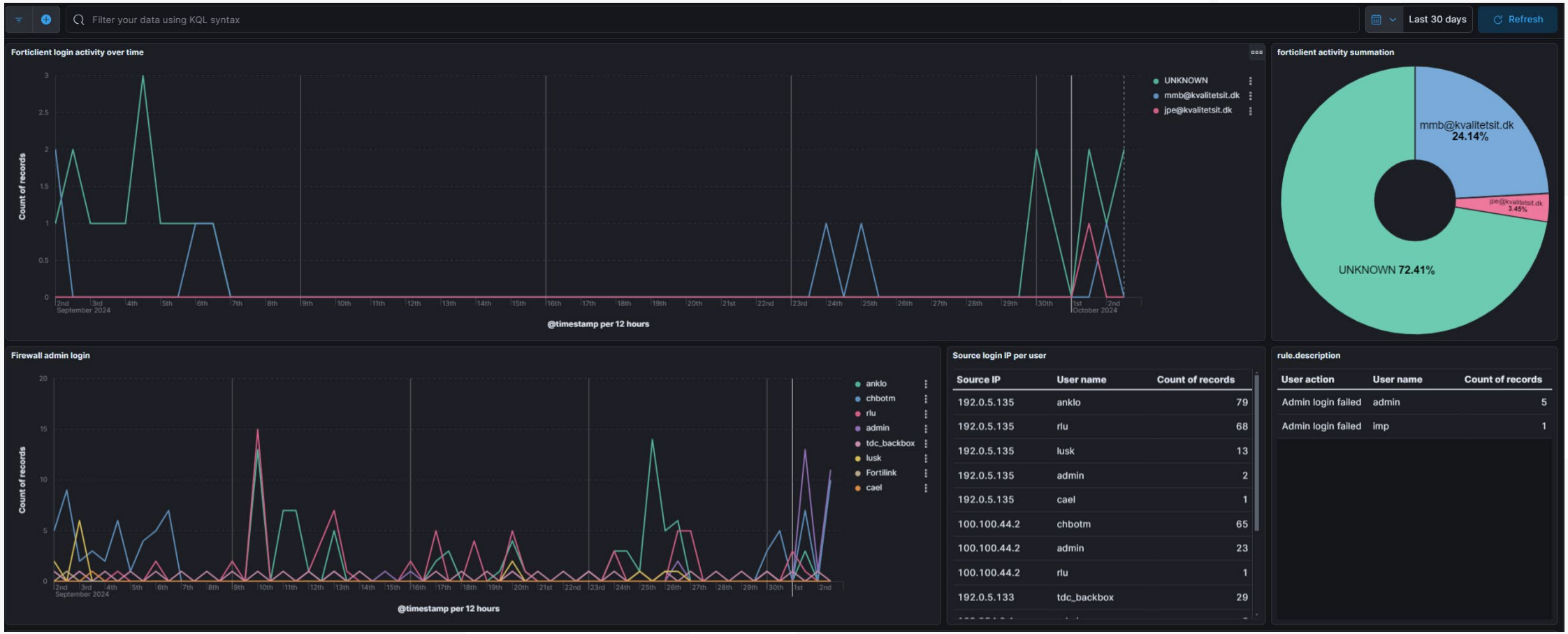
Datasets with observer names

Top 50 values of event.dataset	Top 300 values of observer.name	Count of records
fortinet.firewall	HAGroup_FG200F	381,987,325
fortinet.firewall	mc000018a	228,736,924
fortinet.firewall	mc000043a	23,325,805
fortinet.firewall	mc000039	9,082,321
fortinet.firewall	mc000045a	6,320,909
fortinet.firewall	mc000024	4,012,386
fortinet.firewall	mc000017	3,896,778
fortinet.firewall	mc000002	3,260,012
fortinet.firewall	mc000026	3,232,456
fortinet.firewall	mc000041	3,037,275
fortinet.firewall	mc000029	3,009,393
fortinet.firewall	mc000007	2,918,235
fortinet.firewall	mc000003	2,773,484
fortinet.firewall	mc000028	2,548,742
fortinet.firewall	mc000036	2,310,815
fortinet.firewall	mc000006	2,231,621
fortinet.firewall	mc000027	2,102,641
fortinet.firewall	mc000044	2,013,578
fortinet.firewall	mc000061	2,007,355
fortinet.firewall	mc000020	1,932,232
fortinet.firewall	mc000046	1,788,094
fortinet.firewall	mc000012	1,655,230
fortinet.firewall	mc000015	1,558,781
fortinet.firewall	mc000052	1,524,216
fortinet.firewall	mc000022	1,472,555
fortinet.firewall	mc000001	1,210,764

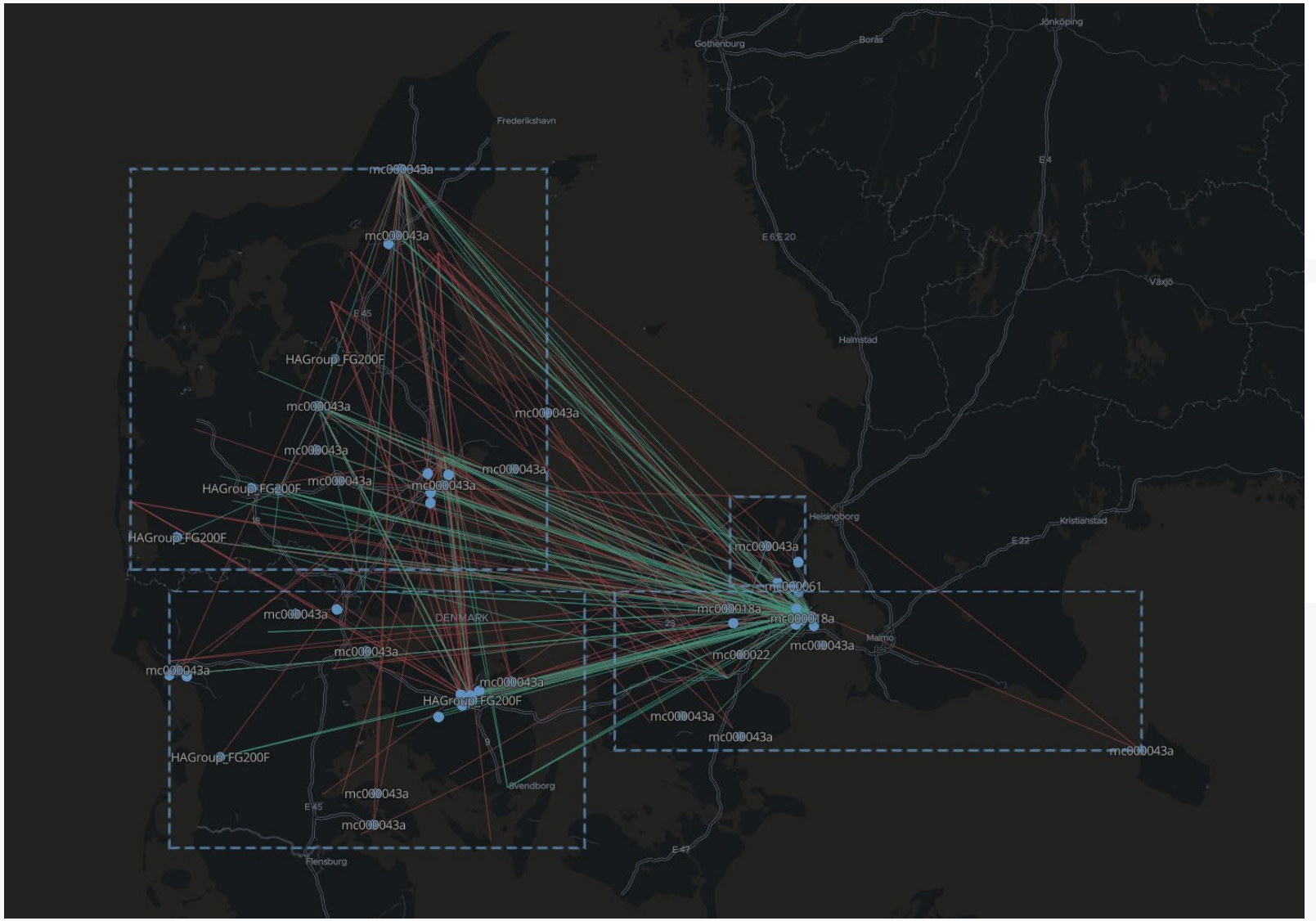
Alarmer

Actions	@timestamp	Assignees	user.name.text	event.action	Rule	Severity	Risk Score	host.name
	May 17, 2024 @ 16:32:02.431		WIN-1CGDMF7UON0$	created-process	ND: Executable from Windows Temp Folder	low	21	WIN-1CGDMF7UON0
	May 17, 2024 @ 16:32:02.433		WIN-1CGDMF7UON0$	created-process	ND: Executable from Windows Temp Folder	low	21	WIN-1CGDMF7UON0
	May 24, 2024 @ 13:44:13.852		admin	login	ND: FortiManager Successful Super User Login	medium	47	medsdncol01
	May 24, 2024 @ 15:48:36.955		admin	login	ND: FortiManager Successful Super User Login	medium	47	medsdncol01
	Jun 4, 2024 @ 09:55:14.321		—	—	ND: Fortinet Firewall Successful Super Admin Login	medium	47	—
	Jun 4, 2024 @ 10:00:14.154		—	—	ND: Fortinet Firewall Successful Super Admin Login	medium	47	—
	Jun 4, 2024 @ 10:35:16.524		—	—	ND: Fortinet Firewall Successful Super Admin Login	medium	47	—
	Jun 4, 2024 @ 10:45:16.918		—	—	ND: Fortinet Firewall Successful Super Admin Login	medium	47	—
	Jun 10, 2024 @ 17:05:55.535		admin	login	ND: FortiManager Successful Super User Login	medium	47	medsdncol01
	Jun 11, 2024 @ 13:06:06.794		admin	login	ND: FortiManager Successful Super User Login	medium	47	medsdncol01
	Jun 11, 2024 @ 15:46:07.834		admin	login	ND: FortiManager Successful Super User Login	medium	47	medsdncol01
	Jun 12, 2024 @ 11:08:38.379		admin	login	ND: FortiManager Successful Super User Login	medium	47	medsdncol01
	Jun 16, 2024 @ 06:07:39.330		admin	login	ND: FortiManager Successful Super User Login	medium	47	medsdncol01
	Jun 20, 2024 @ 07:01:48.904		—	—	ND: Fortinet Firewall Successful Super Admin Login	medium	47	—
	Jun 20, 2024 @ 07:06:48.669		—	—	ND: Fortinet Firewall Successful Super Admin Login	medium	47	—
	Jun 20, 2024 @ 07:06:48.671		—	—	ND: Fortinet Firewall Successful Super Admin Login	medium	47	—
	Jun 27, 2024 @ 16:33:24.994		admin	login	ND: FortiManager Successful Super User Login	medium	47	medsdncol01

Login aktivitet



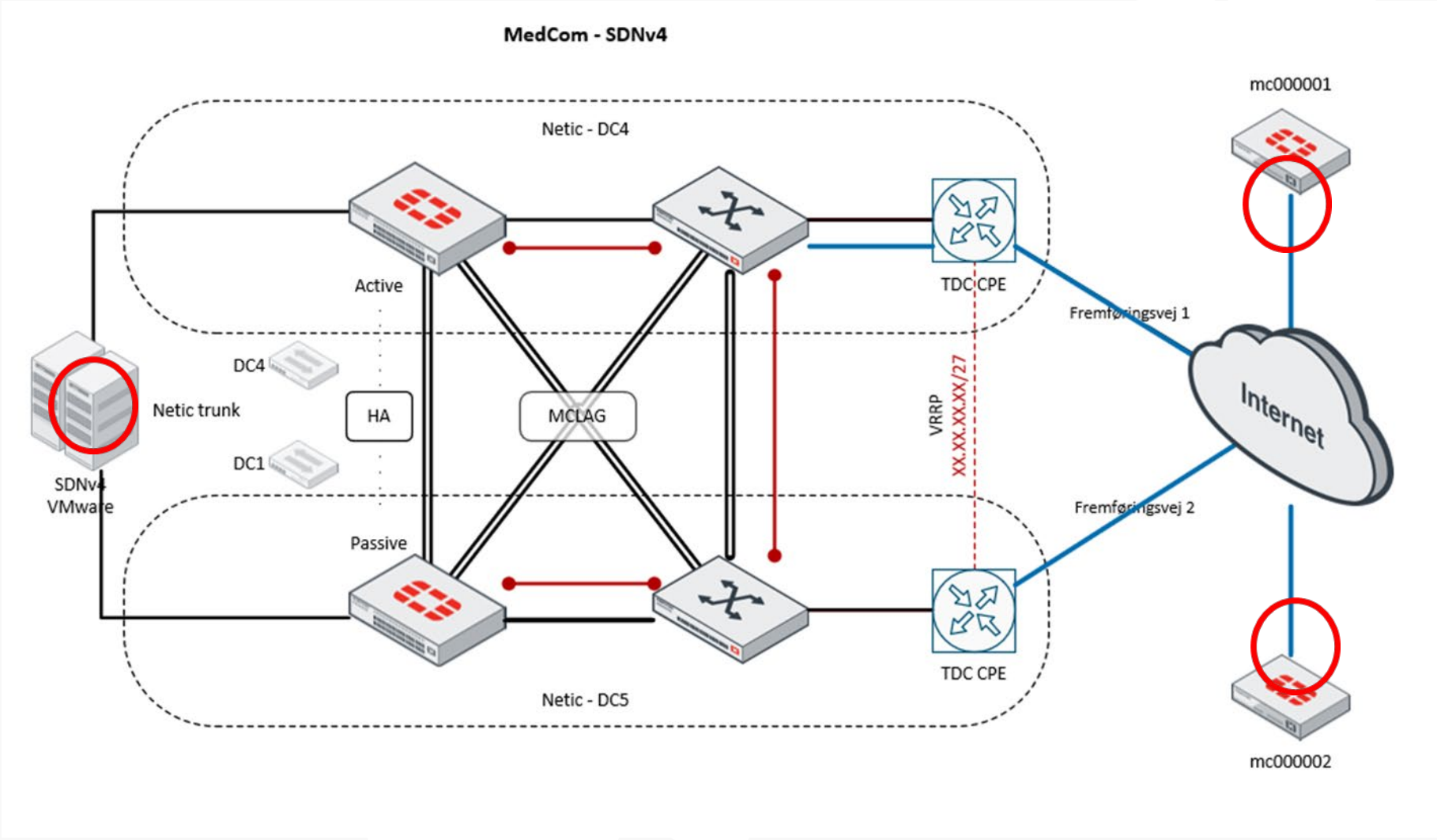
Trafikkort


Gothenburg
Borås
Jönköping
Frederikshavn
Växjö
Halmstad
Helsingborg
Kristianstad
Malmö
Flensburg
Svendborg
DENMARK
E 45
E 6, E 20
E 4
E 22
E 47
mc000043a
HAGroup FG200F
mc000061
mc000018a
mc000022

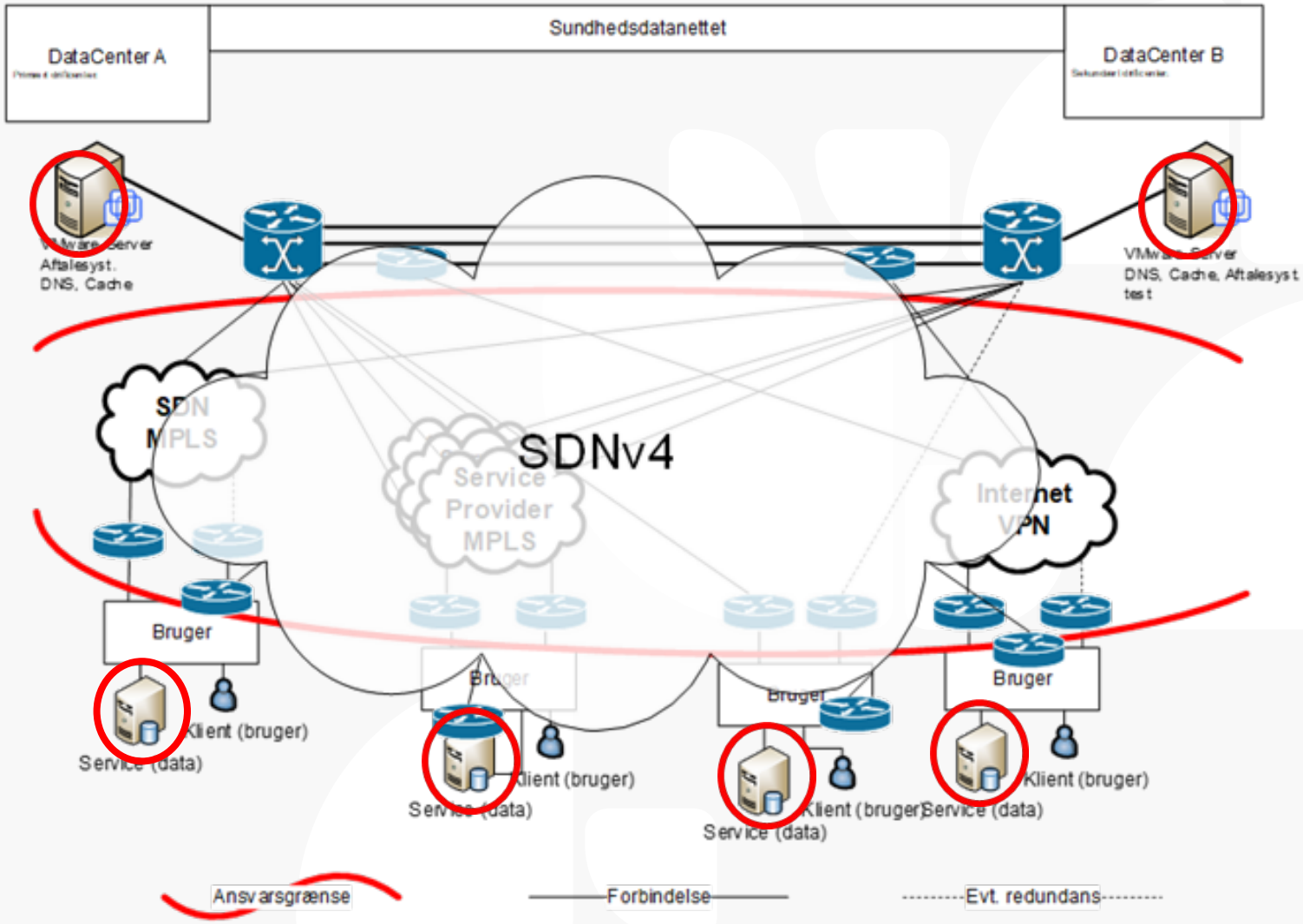
”Heat map”


ICELAND
CANADA
RUSSIA
FINLAND
NORWAY
SWEDEN
ALASKA
NUNAVUT
NUNATSIAVUT
NEWFOUNDLAND AND LABRADOR
ONTARIO
MANITOBA
ALBERTA
BRITISH COLUMBIA
NORTHWEST TERRITORIES
YUKON
MINNESOTA
OREGON
IDAHO
WYOMING
NEVADA
ARIZONA
ARKANSAS
MEXICO
CUBA
HAITI
GUATEMALA
NICARAGUA
PANAMA
COLOMBIA
VENEZUELA
GUYANA
ECUADOR
PERU
BRAZIL
BOLIVIA
CHILE
ARGENTINA
FALKLAND ISLANDS
Rio de Janeiro
MAURITANIA
SENEGAL
GUINEA
LIBERIA
NIGERIA
GHANA
BURKINA FASO
ETHIOPIA
SOMALIA
KENYA
TANZANIA
GABON
ANGOLA
ZAMBIA
ZIMBABWE
MADAGASCAR
SOUTH AFRICA
SAUDI ARABIA
YEMEN
CHINA
MONGOLIA
KYRGYZSTAN
JAPAN
SOUTH KOREA
TAIWAN
PHILIPPINES
CAMBODIA
BRUNEI
PAPUA NEW GUINEA
AUSTRALIA
Sydney
NEW ZEALAND
TASMANIA
KAMCHATKA KRAI
SAKHALIN OBLAST
BURYATIA
AMUR OBLAST
MAGADAN REGION
CHUKOTKA AUTONOMOUS OKRUG
SAKHA (YAKUTIA)
NENETS AUTONOMOUS DISTRICT
KHANTY-MANSIYSK AUTONOMOUS OKRUG – UGRA
YAMALO-NENETS AUTONOMOUS OKRUG

Skanning af SD-WAN



Sårbarhedsskanning af services



GDPR og NIS2

- GDPR og NIS2
- Egenkontrol gennem revisionserklæringer
- Barrierer for tillid – lovgivning
- Tillid er godt – er kontrol altid bedre?

Spørgsmål

Kontakt

Peder Illum

Konsulent – Systemforvaltningsteam

pi@medcom.dk

2926 3654