Spinoso Vincenzo
Donvito Giacinto

Sviluppo di un framework flessibile per asset management dinamico e policy management

Perché sviluppare un framework?

- Mappa della farm
- Inventario dinamico hosts e risorse di rete
- Redazione allegato tecnico DVR
- Scansione openvas su ***hostlist***
- View personalizzate (sia nel formato, sia nei contenuti) delle informazioni raccolte

Mappa della farm

- Problema: **dove sono le macchine?**
- Macchine etichettate, ma può capitare che l'etichetta non sia presente

- Soluzione
  - dagli switch ricaviamo MAC, IP, port via SNMP
  - incrociamo con un JSON file scritto manualmente che mappa le porte dello switch sui rack in farm
  - ricaviamo la **posizione (rack) di ogni host**

Inventario dinamico hosts e risorse di rete

- Problema: **quali sono gli hosts e gli switch presenti in rete? Come sono caratterizzati gli host?**

- Soluzione
  - Incrociamo i dati provenienti da varie sorgenti (NMap, Foreman, Puppet, Gitlab, Zabbix, OpenStack, VMWare, monitoring di esperimento…)
  - **Raccogliamo dati** su vendor, hypervisor, S/N, servizi esposti (porte), monitoring, CPU, dischi, OS… **per ogni host**

Redazione allegato tecnico DVR

- Problema: **come calcoliamo il valore del rischio per ogni host?**

- Soluzione
  - Associamo staticamente un profilo a ogni host
  - Associamo valori di riservatezza, integrità, disponibilità a ciascun profilo
  - Calcoliamo il rischio intrinseco per ciascun host
  - **Produciamo un docx da allegare al DVR** (*in progress*)

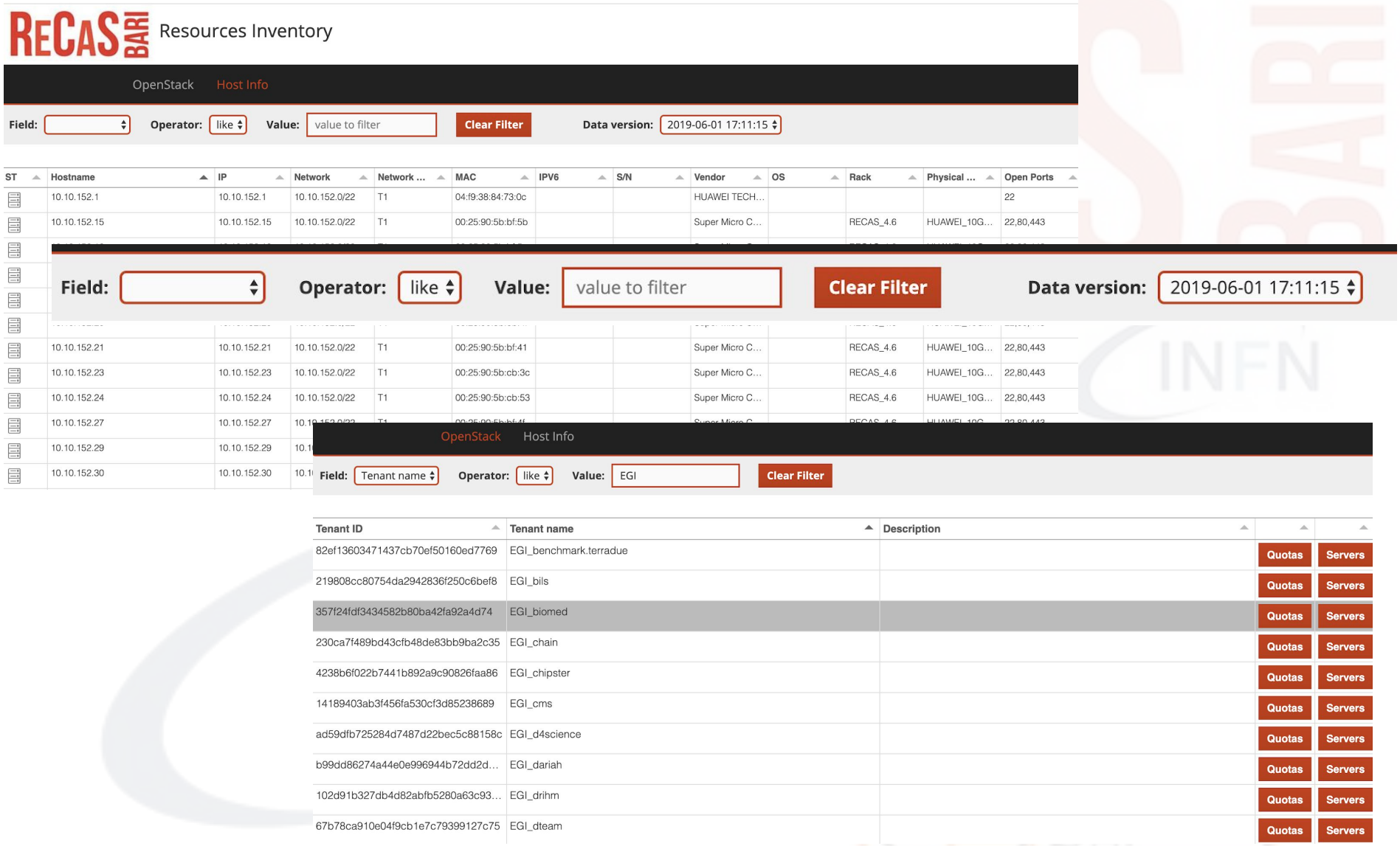
Scansione OpenVAS su hostlist

- Problema: **come eseguire la scansione di tutto il centro in un tempo ragionevole?**

- Soluzione
  - Invece di impostare le reti come target del task OpenVAS, usiamo la host list **precedentemente generata**
  - **Tempo di scansione per sezione + RECAS: circa 48h (was: forever)**

```
"90.147.168.208": {
  "foreman_os": "Scientific Linux 6.7",
  "hostname": "storm.recas.ba.infn.it",
  "vendor": "Super Micro Computer, Inc.",
  "network": "90.147.168.0/23",
  "virtual": 0,
  "serialnumber": "",
  "ts": 1559624899.989397,
  "alive": 1,
  "mac": "00:25:90:94:f2:a5",
  "Y": 1,
  "ipscan": [
    {
      "tproto": "tcp",
      "state": "open",
      "protocol": "ssh",
      "port": "22"
    }
  ],
  "location": "RECAS",
  "ipv6": [
    "fe80::225:90ff:fe94:f2a5",
    "2001:760:4227::24"
  ],
  "portname": [
    "HUAWEI_10GE8/0/14"
  ],
  "X": 1,
  "networkdescription": "RECAS farm",
  "port": [
    "HUAWEI_464"
  ]
}
```

```
  "90.147.169.47": {
    "hostname":
"wn-infn-3-8-35.recas.ba.infn.it",
    "vendor": "Super Micro Computer, Inc.",
    "network": "90.147.168.0/23",
    "puppet_os": "CentOS 7.5.1804",
    "virtual": 0,
    "serialnumber": "S15559024816367",
    "zabbix_available": "available",
    "ts": 1559624899.989397,
    "alive": 1,
    "processorcount": 64,
    "mac": "0c:c4:7a:1e:04:66",
    "Y": 8,
    "ipscan": [
      {
        "tproto": "tcp",
        "state": "open",
        "protocol": "ssh",
        "port": "22"
      }
    ],
    "zabbix_error": "",
    "location": "RECAS",
    "X": 3,
    "portname": [
      "HUAWEI_10GE3/0/30"
    ],
    "zabbix_status": "monitored",
    "networkdescription": "RECAS farm",
    "zabbix_hostid": "10999",
    "port": [
      "HUAWEI_240"
    ]
  },
```



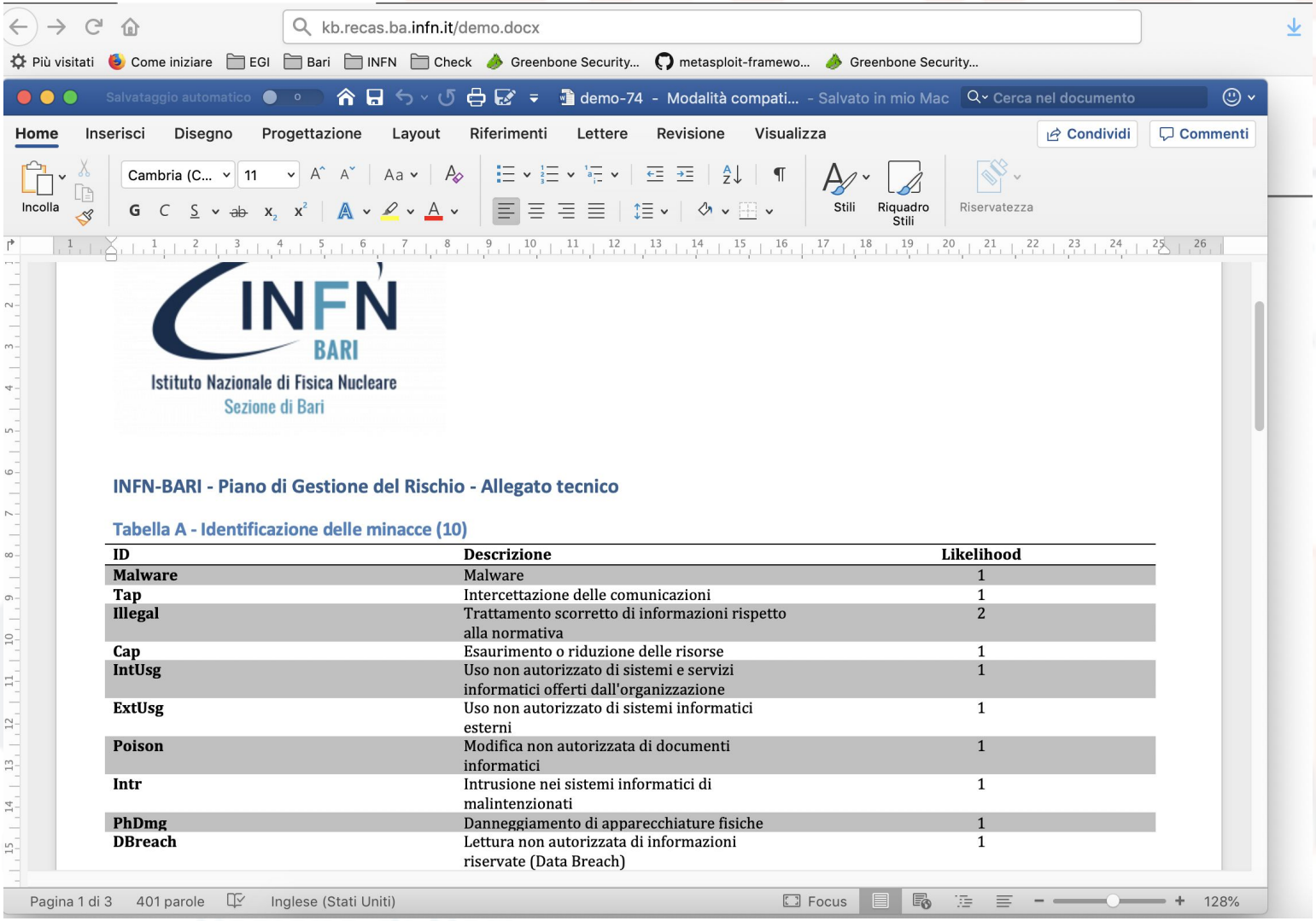
Demo frontends sviluppati da Michele Perniola michele.perniola@ba.infn.it
usando http://tabulator.info/ and https://jquery.com/

KEBAB - Hostinfo

vmwa

Status	Hostname	IP	Network	MAC	IPv6	S/N	Vendor	Operating System	Rack	Physicalport	Open ports
	testjst.recas.ba.infn.it	90.147.169.43	90.147.168.0/23 (RECAS farm)	00:50:56:8c:c1:79	fe80::250:56ff:fe8c:c179		VMware, Inc.	Ubuntu 18.04 LTS	?	HUAWEI_10GE8/0/29	22,80
	recas-bari-administration.recas.ba.infn.it	172.20.0.194	172.20.0.0/16 (RECAS private farm services)	00:50:56:8c:df:aa			VMware, Inc.	Ubuntu 16.04.6 LTS	RECAS_1.1	HUAWEI_10GE8/0/23	22,80,3306
	bacula.recas.ba.infn.it	90.147.168.151	90.147.168.0/23 (RECAS farm)	00:50:56:8c:1e:83	fe80::250:56ff:fe8c:1e83		VMware, Inc.	Ubuntu 14.04 LTS	RECAS_4.4	HUAWEI_10GE7/0/12	22
	ldapb.ba.infn.it	192.135.10.176	192.135.10.0/24 (INFN-BARI)	00:50:56:8c:87:3c			VMware, Inc.		RECAS_1.1	HUAWEI_10GE8/0/23 HP_D4	
	foreman.priv.recas.ba.infn.it	172.20.0.3	172.20.0.0/16 (RECAS private farm services)	00:50:56:8c:d5:07			VMware, Inc.		?	HUAWEI_10GE9/0/6	22,80,443,8443
	jennifer.ba.infn.it	192.135.20.222	192.135.20.0/24 (INFN-BARI)	00:50:56:8c:66:b4			VMware, Inc.		?	HUAWEI_10GE9/0/6 HP_D4	
	plouton-api.recas.ba.infn.it	172.20.0.216	172.20.0.0/16 (RECAS private farm services)	00:50:56:8c:84:ff			VMware, Inc.	Debian 9.7	RECAS_1.4	HUAWEI_10GE10/0/39	22
	vw-vrli.recas.ba.infn.it	172.20.0.218	172.20.0.0/16 (RECAS private farm services)	00:50:56:8c:1b:e5			VMware, Inc.	None	?	HUAWEI_10GE9/0/6	22,80,443
	ce-04.recas.ba.infn.it	90.147.169.70	90.147.168.0/23 (RECAS farm)	00:50:56:8c:8b:f0	2001:760:4227::14 fe80::250:56ff:fe8c:8bf0	VMware-42 0c 7e 39 3d 22 90 73-bd 3a ba fa 82 01 82 84	VMware, Inc.	CentOs 7.3	RECAS_1.1	HUAWEI_10GE8/0/23	22,3306,8443
	medphys.ba.infn.it	192.135.10.221	192.135.10.0/24 (INFN-BARI)	00:50:56:8c:f3:a9			VMware, Inc.		?	HUAWEI_10GE9/0/6 HP_D4	80,443

Generazione del DVR



Generazione del DVR

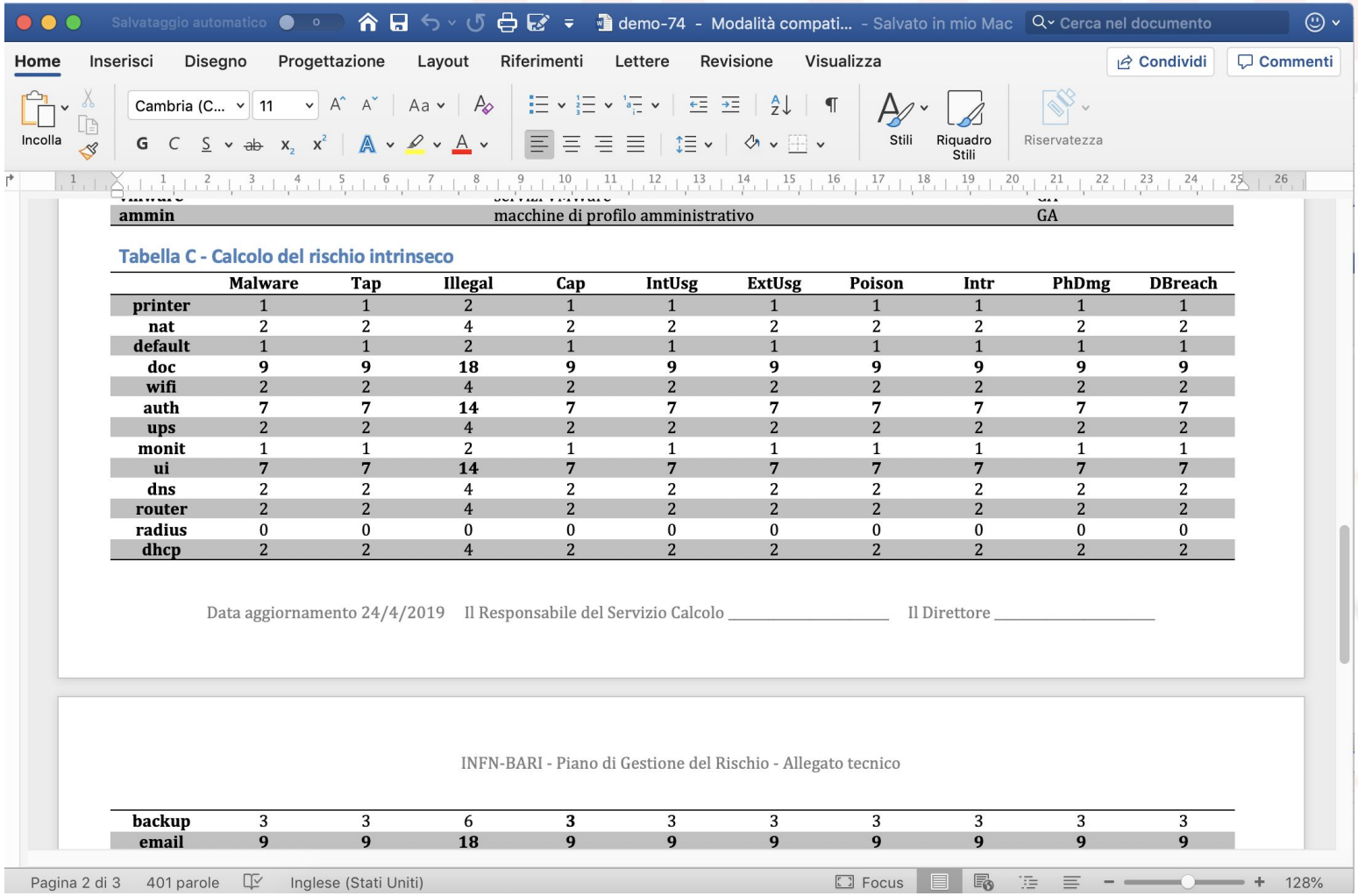
Tabella B - Classificazione degli hosts - Profili (17)

ID	Descrizione	GA/TS
printer	stampante in rete	GA
nat	server NAT	GA
default	profilo tecnico-scientifico generico	TS
doc	documentale	GA
wifi	server WiFi	GA
auth	server di autenticazione	GA
ups	host di accesso agli ups	GA
monit	server di monitoring	GA
ui	user interface	GA
dns	server DNS	GA
router	router per accesso WAN	GA
radius	server RADIUS	GA
dhcp	server DHCP	GA
backup	server di backup	GA
email	server di posta	GA
vmware	servizi VMWare	GA
ammin	macchine di profilo amministrativo	GA

Generazione del DVR

risk(profile,threat) := threat(likelihood(threat)) * f(R(profile),I(profile),D(profile))

(f = max oppure sum …)



ammin	macchine di profilo amministrativo	GA

Tabella C - Calcolo del rischio intrinseco

	Malware	Tap	Illegal	Cap	IntUsg	ExtUsg	Poison	Intr	PhDmg	DBreach
printer	1	1	2	1	1	1	1	1	1	1
nat	2	2	4	2	2	2	2	2	2	2
default	1	1	2	1	1	1	1	1	1	1
doc	9	9	18	9	9	9	9	9	9	9
wifi	2	2	4	2	2	2	2	2	2	2
auth	7	7	14	7	7	7	7	7	7	7
ups	2	2	4	2	2	2	2	2	2	2
monit	1	1	2	1	1	1	1	1	1	1
ui	7	7	14	7	7	7	7	7	7	7
dns	2	2	4	2	2	2	2	2	2	2
router	2	2	4	2	2	2	2	2	2	2
radius	0	0	0	0	0	0	0	0	0	0
dhcp	2	2	4	2	2	2	2	2	2	2

Data aggiornamento 24/4/2019 Il Responsabile del Servizio Calcolo _____ Il Direttore _____

INFN-BARI - Piano di Gestione del Rischio - Allegato tecnico

backup	3	3	6	**3**	3	3	3	3	3	3
email	**9**	**9**	**18**	**9**	**9**	**9**	**9**	**9**	**9**	**9**

BACKEND

"NO-SQL"

REST-API

FRONTEND

ZABBIX

openstack™

vmware

PostgreSQL usato come NoSQL (tipo di dato JSONB), rende disponibile anche lo **storico dei dati raccolti**

- Mail periodica
- Generazione docx
- Sensore Zabbix
- Frontend web

Collezione di script Bash/Python interdipendenti, eseguite da uno scheduler python multithread

/list
/get?name=<object>
/history?name=<object>
/get?name=<object>&version=<ver>

In progress o *in programma*

- Integrare associazione host (portatile/desktop/VM) a utente
  - Esiste DB delle richieste che associa MAC a utente
- Completare generazione allegato DVR integrando la scansione OpenVAS
  - Report CSV già generato automaticamente a CLI
  - Review dei profili
- API autenticata
- *Frontend su ELK*
- *Form per l'inserimento di dati "statici"*
- *Valutare alternativa a PostgreSQL (big data?)*

Conclusioni: Perché sviluppare un framework?

- Difficile (finora) trovare un software che abbia **tutte le caratteristiche** richieste
- Anche a patto di trovare più software, al fine di realizzare un **inventario dinamico e automatico** dovrebbero poi **interagire** tra loro
- API ormai ampiamente disponibili su molti software, **semplice e safe estrarre informazioni**
- Focus sulla generazione di documenti e azioni utili all'applicazione delle **misure AgID**
- **Sostenibile**? Per ora sì, **è semplice** aggiungere nuovi script per generare nuovi dati (JSON)
- Applicabile ad altri contesti? Sì, ma necessario modificare gli script (**parametrizzazione**) e adattarli al nuovo **contesto** (switch, servizi più o meno presenti...)
- **Alternative?...**