Labyrinth Deception

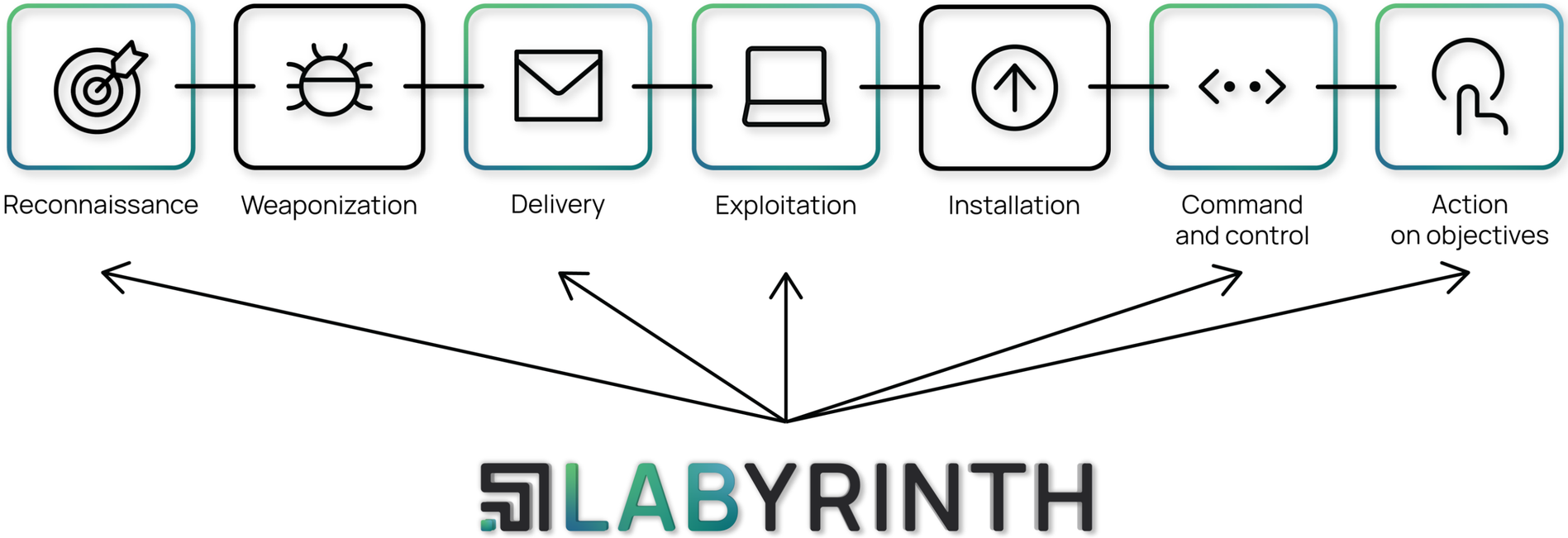
Drugačiji pristup za praćenje mreže?

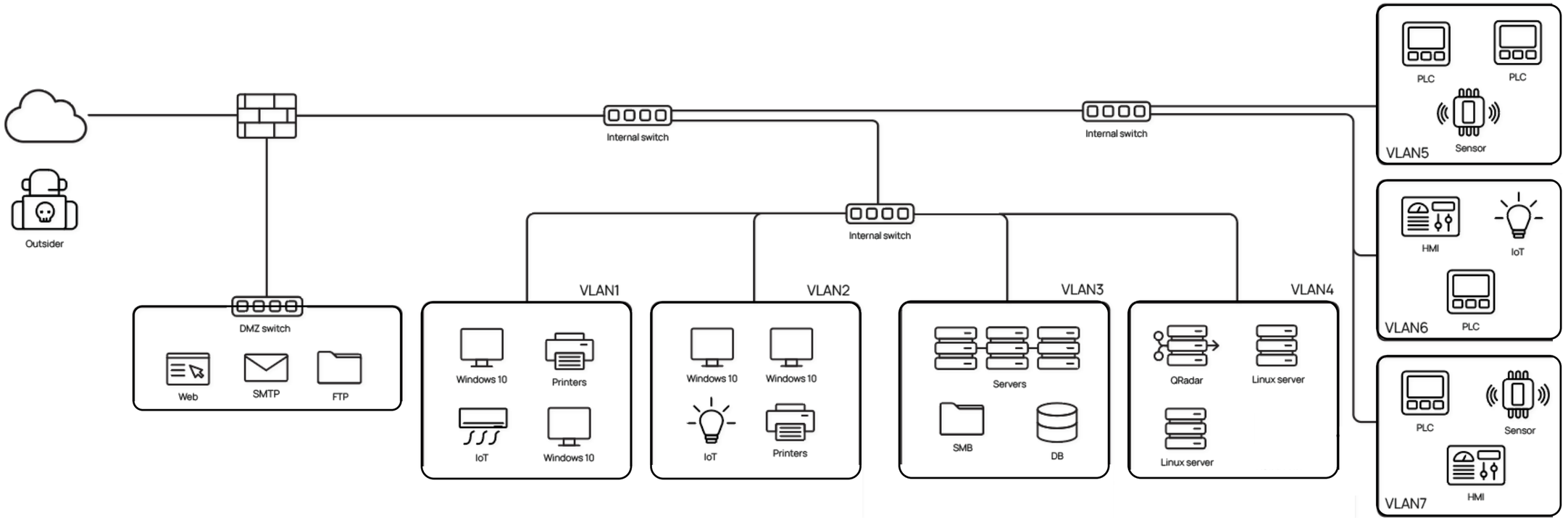
Tko je Labyrinth?

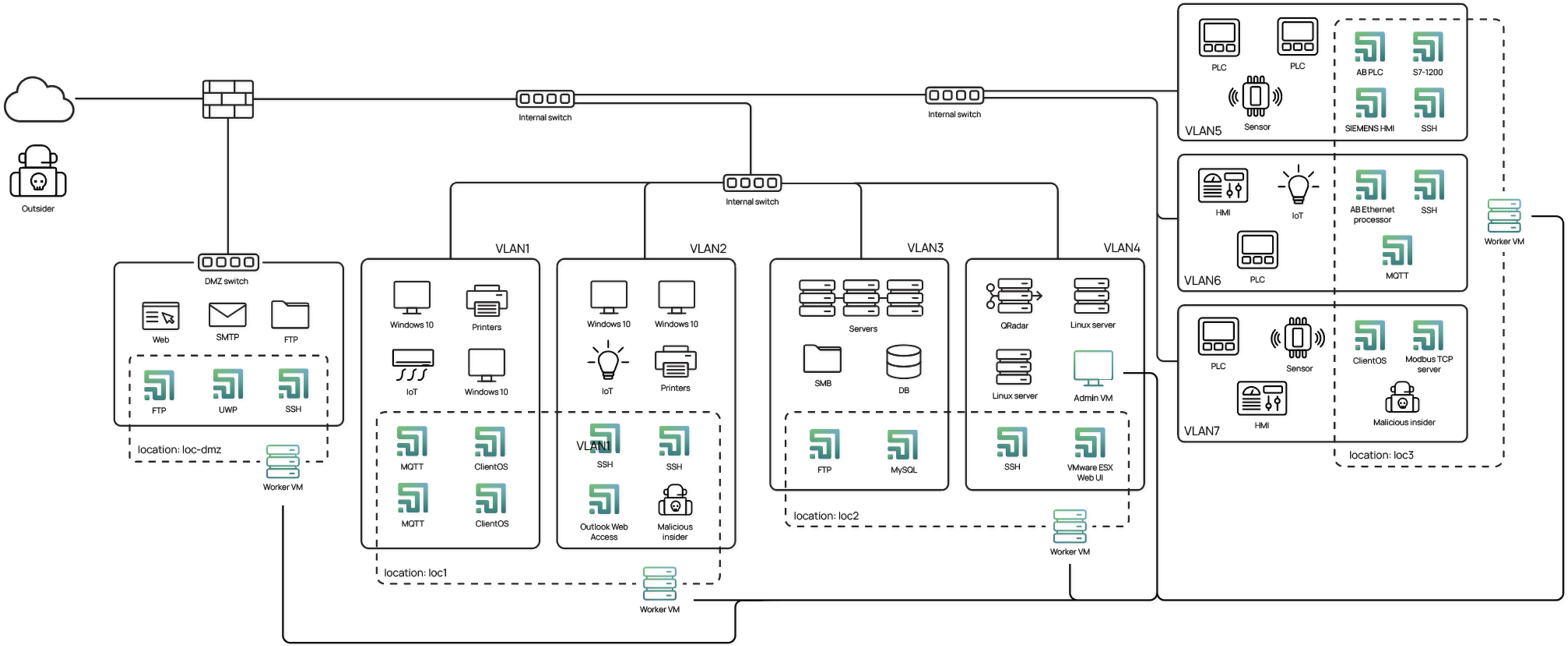
- **Osnovan u 2019.**
- HQ u Zabrze, Poljska
- Web stranica: www.labyrinth.tech
- LinkedIn profil: link
- YouTube kanal: link

Kibernetički „kill-chain“

Labyrinth je najučinkovitiji u **ranom otkrivanju napada**



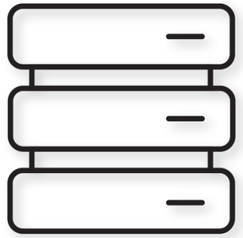

Outsider
Internal switch
Internal switch
Internal switch
DMZ switch
Web
SMTP
FTP
VLAN1
Windows 10
Printers
IoT
Windows 10
VLAN2
Windows 10
Windows 10
IoT
Printers
VLAN3
Servers
SMB
DB
VLAN4
QRadar
Linux server
Linux server
VLAN5
PLC
PLC
Sensor
VLAN6
HMI
IoT
PLC
VLAN7
PLC
Sensor
HMI


Outsider
Internal switch
Internal switch
Internal switch
DMZ switch
Web
SMTP
FTP
FTP
UWP
SSH
location: loc-dmz
Worker VM
VLAN1
Windows 10
Printers
IoT
Windows 10
MQTT
ClientOS
MQTT
ClientOS
location: loc1
Worker VM
VLAN2
Windows 10
Windows 10
IoT
Printers
VLAN1
SSH
SSH
Outlook Web Access
Malicious insider
VLAN3
Servers
SMB
DB
FTP
MySQL
VLAN4
QRadar
Linux server
Linux server
Admin VM
SSH
VMware ESX Web UI
location: loc2
Worker VM
PLC
PLC
AB PLC
S7-1200
Sensor
SIEMENS HMI
SSH
VLAN5
HMI
IoT
AB Ethernet processor
SSH
PLC
MQTT
VLAN6
PLC
Sensor
ClientOS
Modbus TCP server
HMI
Malicious insider
VLAN7
location: loc3
Worker VM

Arhitektura platforme

Admin VM (Management Console)

All information collected at the Points is forwarded to the Management Console for incident analysis and response.



Worker VM

The Worker VM is the host that hosts all the Points in Labyrinth. It can operate in multiple VLANs simultaneously.

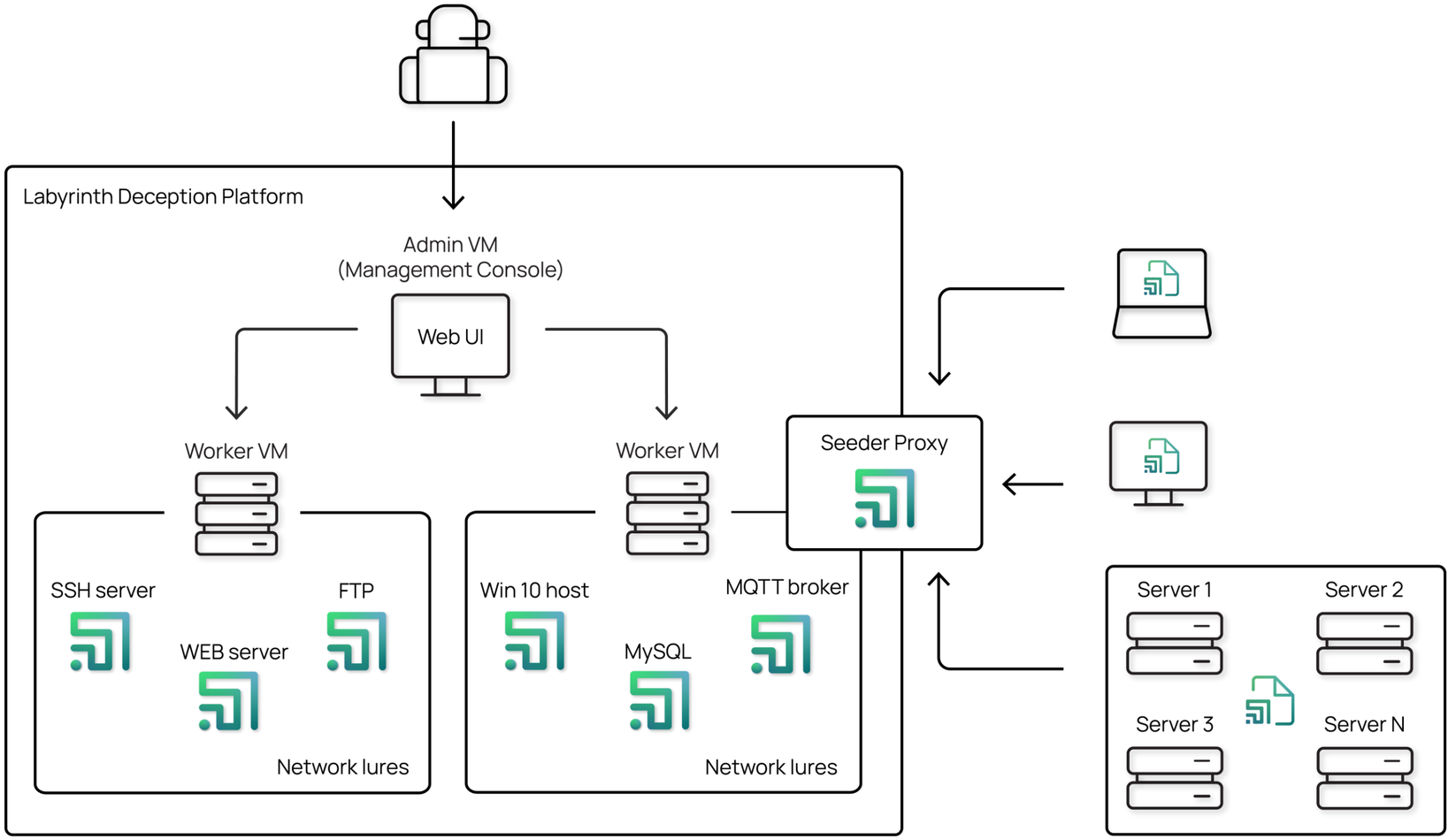
Point

Points simulate applications and services in a real-world IT environment and interact with attackers, keeping them inside the Labyrinth.

Host with Seeder Agent

Agents are deployed on real hosts and distribute attractive artifacts to them. The artifacts used by attackers direct them to Points.

Arhitektura rješenja



Seeder Agent usmjeri napadača u zamku (Point)

Zamka (Point) komunicira s napadačem i šalje alarme na konzolu

Konzola alarmira ekipu za odazivanje i šalje metapodatke za analizu

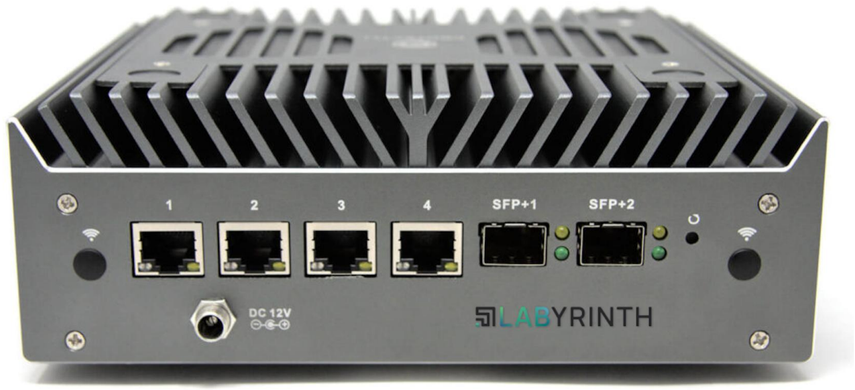
Ekipa za odazivanje potvrdi podatke i zaustavlja napad

Podržane platforme

Microsoft Hyper-V

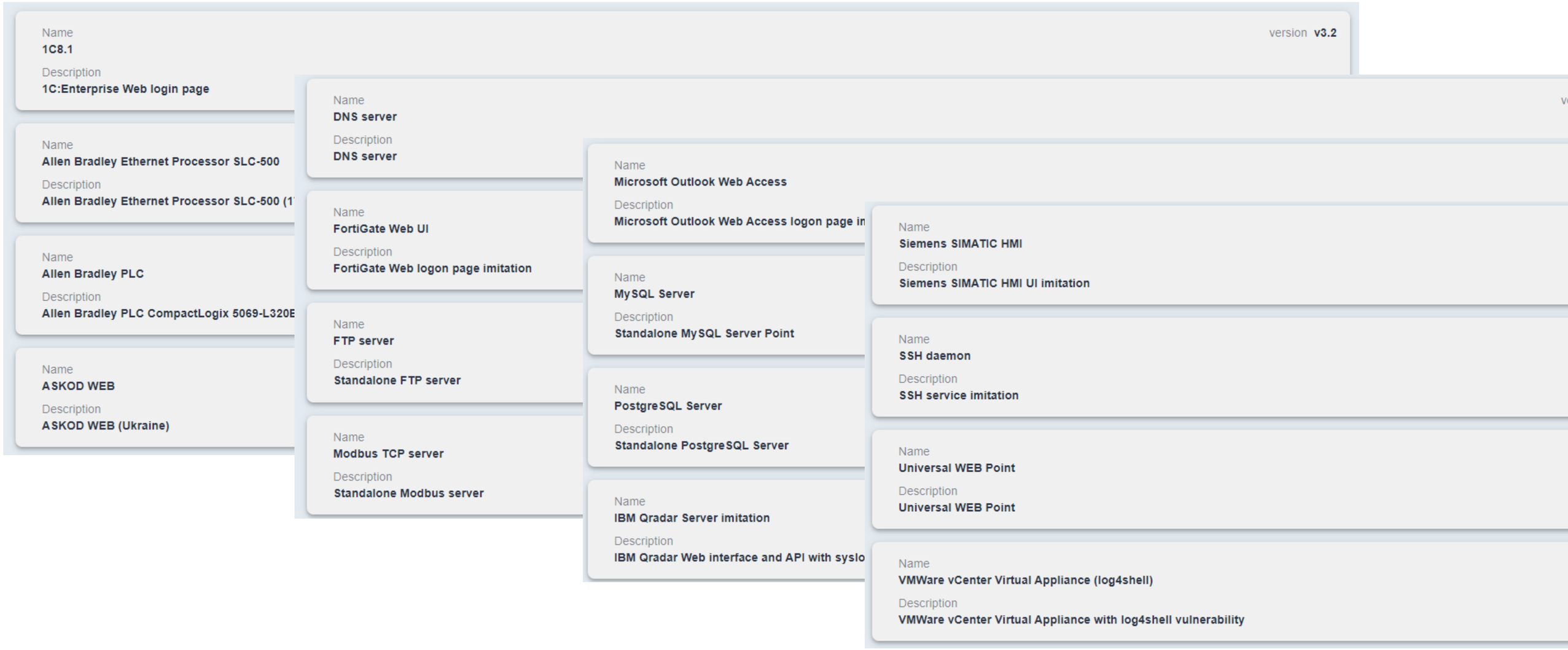
Azure

vmware®

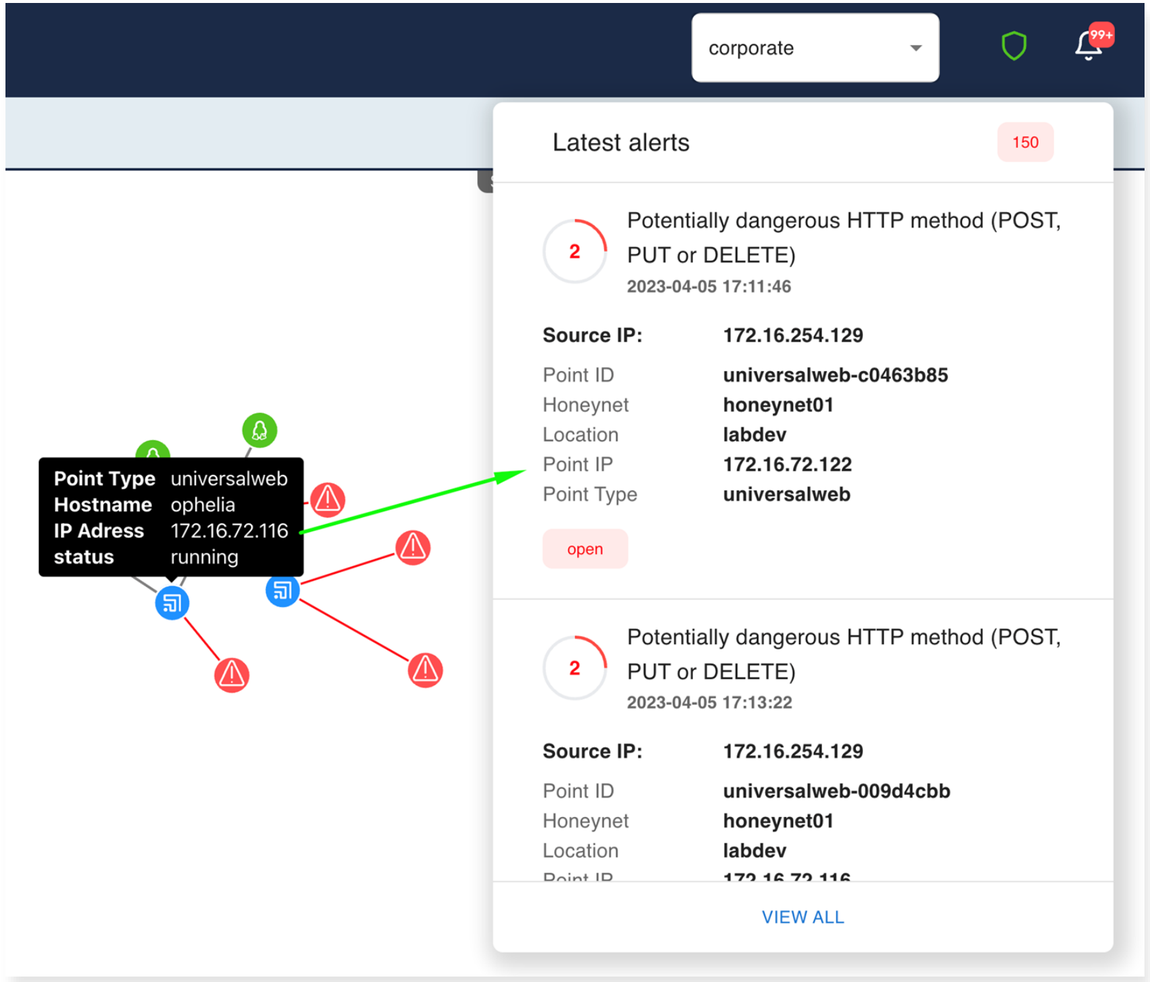


PROXMOX
Proxmox Virtual Environment

Deception Point Type Bases

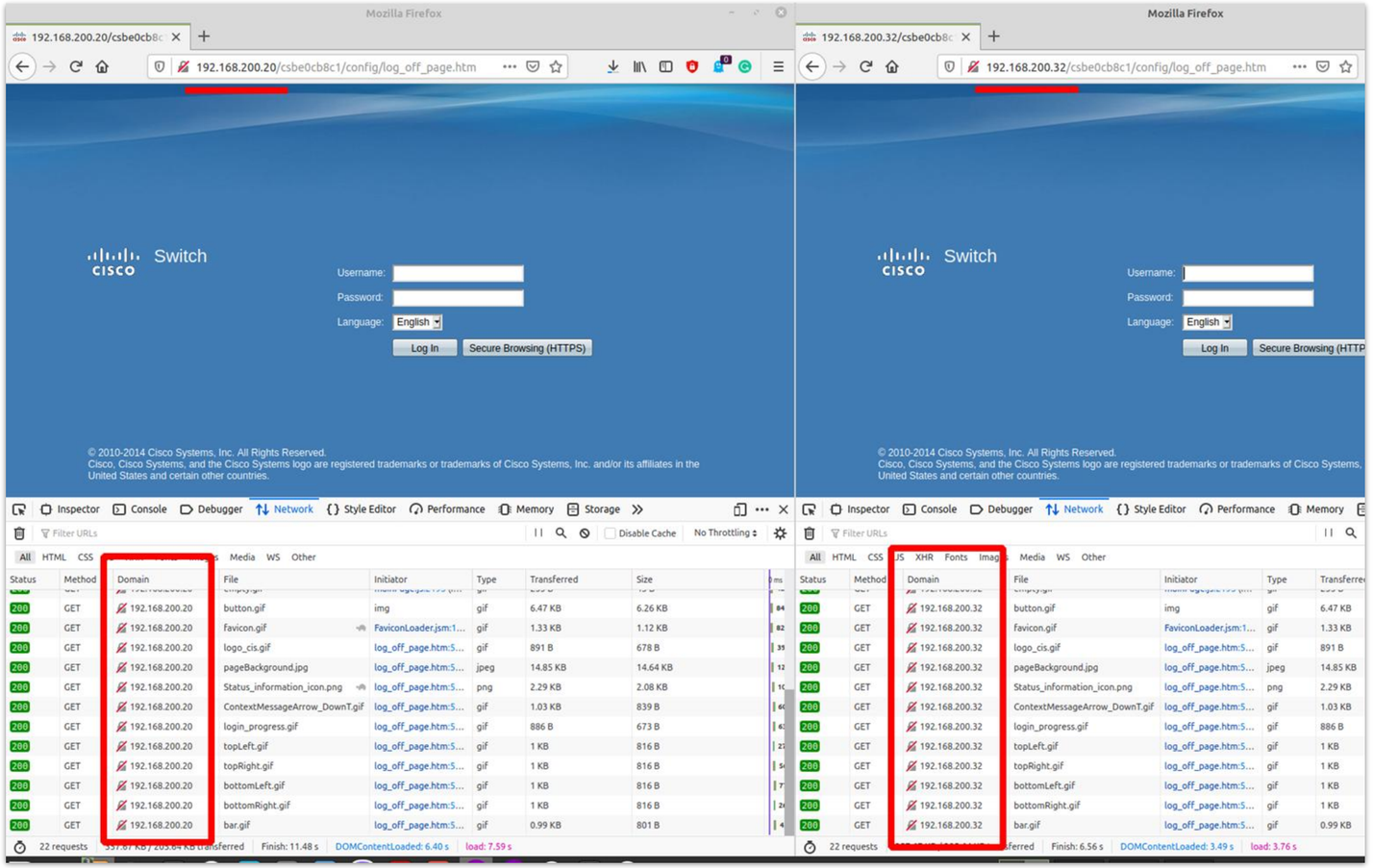


Universal Web Point



Universal Web Point

- „Kloniranje“ web aplikacije
- Dodan ranjivosti iz OWASP TOP10
- Radi kao proxy



Primjer alarma

	Severity	Status	Timestamp	Point ID	Attacker IP	Alert Reason
☐	H	open	2024-05-16 11:08:58	sshd-3eae0458	10.10.10.1	sshd successful login detected

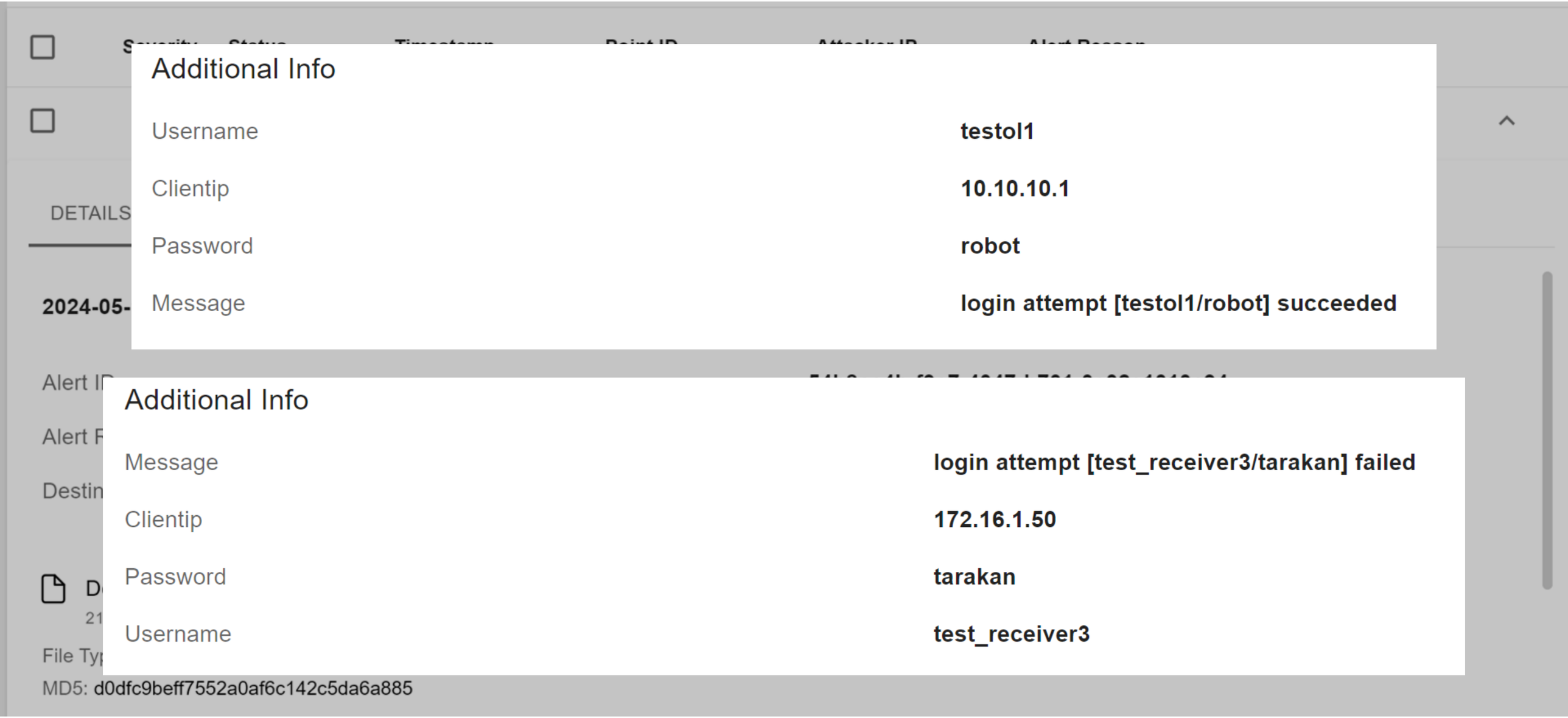
DETAILS EVENTS ACTIVITY(0)

2024-05-16 11:08:58

Alert ID	**54b8ce4b-f9e7-4047-b731-3e02e1010c94**
Alert Reason	**sshd successful login detected**
Destination IP	**10.10.10.71**

Download PCAP
21.31 KB

File Type: pcap
MD5: d0dfc9beff7552a0af6c142c5da6a885

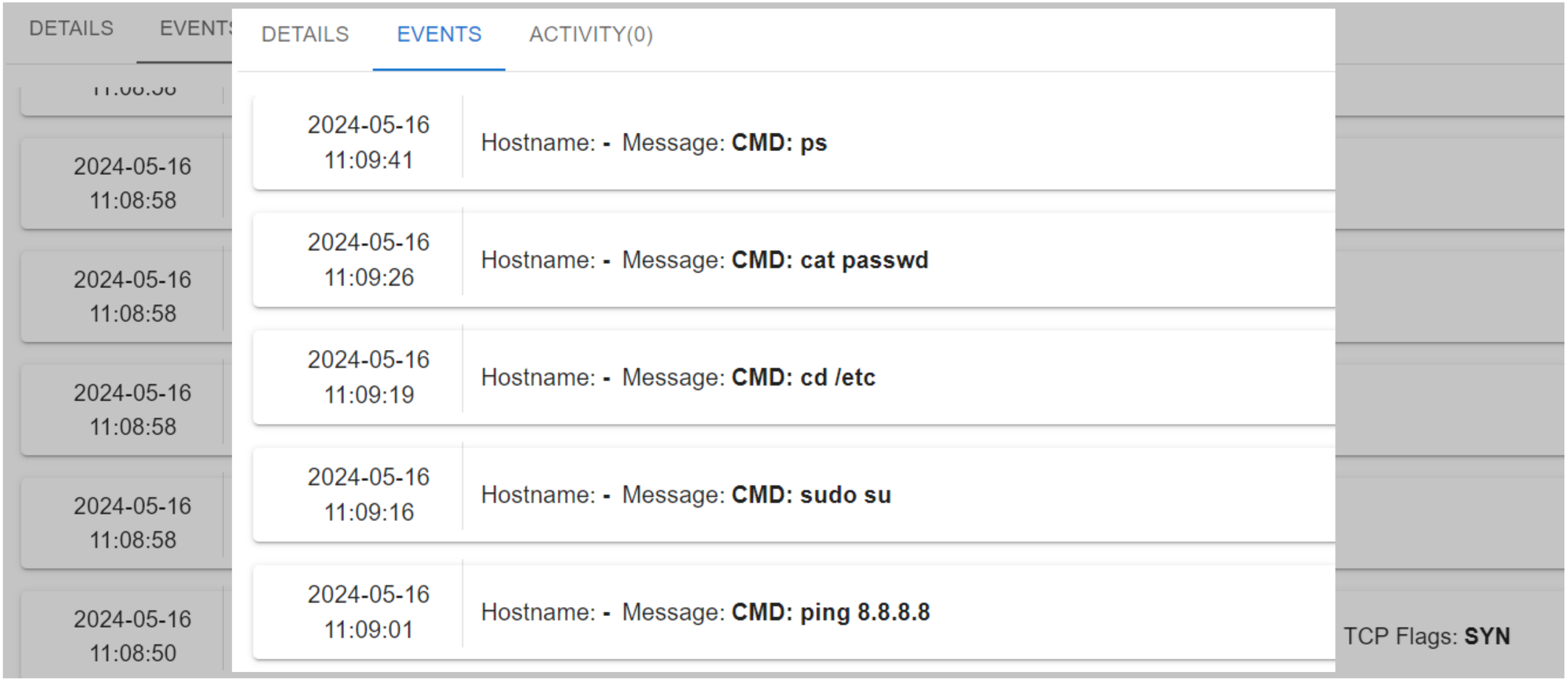

Additional Info
Username
testol1
Clientip
10.10.10.1
Password
robot
Message
login attempt [testol1/robot] succeeded
DETAILS
2024-05-
Alert ID
Alert R
Destin
Additional Info
Message
login attempt [test_receiver3/tarakan] failed
Clientip
172.16.1.50
Password
tarakan
Username
test_receiver3
File Typ
MD5: d0dfc9beff7552a0af6c142c5da6a885

Detajli alarma

DETAILS EVENTS ACTIVITY(0)

11:08:56	
2024-05-16 11:08:58	Hostname: **-** Username: **testol1** Message: **login attempt [testol1/robot] succeeded**
2024-05-16 11:08:58	Hostname: **-** Message: **SSH client hassh fingerprint: 55b7fab6f5d2b485a6773eee233e4a52**
2024-05-16 11:08:58	Hostname: **-** Message: **New connection: 10.10.10.1:12033 (10.10.10.71:22) [session: 8495d6e5e930]**
2024-05-16 11:08:58	Hostname: **-** Message: **Remote SSH version: SSH-2.0-OpenSSH_7.8 FreeBSD-20180909**
2024-05-16 11:08:50	Transport: **tcp** Source IP: **10.10.10.1** Source Port: **12033** Destination IP: **10.10.10.71** Destination Port: **22** TCP Flags: **SYN**

Detajli alarma



Integracije

TheHive

CROWDSTRIKE

splunk>

Radar®

FORTINET®

State	Name	Edit
	CrowdStrike	
	Cuckoo Sandbox	
	Fortigate	
	Microsoft Teams Notifications	
	IBM-Qradar	
	Slack Notification	
	SMTP Notification	
	Splunk	
	SIEM Integration (Syslog forwarder)	
	TheHive	