

1. Windows Log Analysis

Tools: Splunk Free, Windows Event Viewer

Objective: Detect unauthorized login attempts

Findings: 3 critical and 5 warnings

The screenshot shows the Splunk Free interface with the following details:

- Search Bar:** index=* "fail" OR "warn" OR "critical"
- Results Summary:** 9 events (before 11/7/25 6:37:32.000 AM) Sampling 1:10
- Time Range:** All time
- Event List:** Shows 9 events from various dates and times, categorized by type (Information, Warning) and source (Microsoft-Windows-Winlogon, ApplicationLgs.txt). One event is highlighted in yellow.
- Selected Fields:** host, source, sourcetype
- Interesting Fields:** date_hour, date_mday, date_minute, date_month, date_second, date_wday, date_year, date_zone, index, linecount

The screenshot shows the Splunk Enterprise interface with the following details:

- Search Bar:** index=* ("authentication" OR "failed") | eval category=if(match(_raw, "authentication"), "authentication", if(match(_raw, "failed"), "failed", "other")) | stats count by category
- Results Summary:** 6 events (before 11/7/25 7:09:15.000 AM) Sampling 1:1.000
- Time Range:** All time
- Event List:** Shows 6 events categorized by category (authentication, failed, other).
- Statistics View:** A table showing the count of events per category.

2 . Phishing Email Analysis

Tools : caniphish, virustotal

Findings : Detected some phishing email and verified using virustotal Tool.

The screenshot shows a Gmail inbox with several messages. The message highlighted is from 'Payoneer (payoneer[.]gps@alerting-services[.]com)' to 'john[.]doe@mybusiness[.]com'. The subject line is 'You have received a new payment to your Global Payment Service!'. The message body displays a payment summary: Amount \$9100.00 and Payment ID 40114047. It includes a note about account verification and a time-sensitive link to verify the account. A red box highlights the URL 'http://payouts.payoneer.com/Verify/Gateway.aspx?PD=9S1J4f39L9HDSM8Y'. A large red 'Verify' button is at the bottom. On the left sidebar, there are labels: Work (pink dot), Business (blue dot), Family (orange dot), and Friends (green dot). The 'Work' label is selected.

The screenshot shows the Virustotal analysis page for the file 72231b0c75efed1962da60523d0dd5d70524f1b5262694bcfd8d7c57b75bd1d1. The page indicates 'No security vendors flagged this file as malicious'. The file is a screenshot taken on November 7, 2025, at 11:33:14. It is a PNG file (163.80 KB) and was analyzed a moment ago. The interface includes tabs for DETECTION, DETAILS, and COMMUNITY. Below the main analysis, there is a call to action to 'Join our Community' and a section for 'Security vendors' analysis' showing results for various engines like Acronis, ALYac, Arcabit, AVG, and Baidu, all of which found the file undetected.

3. Vulnerability Scanning

Objective : Performing vulnerability scan on windows operating system.

localhost:8020/webclient#/uem/patch-mgmt/systems/computer/311/summary

Vulnerability Manager Plus Home Threats Patches Network Devices Systems Deployment ... Jump to SDP Update ...

Stop Scanning

U-3PJCC64
Service Pack: Windows 11 Version 24H2 (x... | Language: English | IP Address: 192.168.0.102 | Remote Office: Local Office

Windows 11 Enterprise Edition (x64)
Operating System

pujitha.gangolu@unisys.com
Logged On Users

Oct 26, 2025 07:...
Last Boot Time

Unisys
Domain Name

Summary Software & Components Vulnerabilities Patches Security Config Port Audit Actions

Security Overview

Vulnerability Status	:	Resource Health Status Unknown
Scan Status	:	Scanning In-Progress Scan Now
Last Successful Scan	:	--
No of patches to be installed	:	Unable to calculate health, as the scan is not yet performed
Reboot Status	:	Not Required
BitLocker Status	:	Enabled
Local Admins	:	0