

# Sentrilite EDR/XDR for Windows — Threat-Detection-as-Code, Observability, Runtime-Security, Live Telemetry, Misconfig Scanner with AI/LLM insights.

## Installation Steps

In the Zip File, open Sentrilite.exe OR In a Powershell Terminal run:

Start Sentrilite Service: \sentrilite-service.bat start

Check Service Status: \sentrilite-service.bat status

Stop Sentrilite Service: \sentrilite-service.bat stop

## Live System Telemetry

Open the dashboard.html to check live telemetry:

The screenshot displays the Sentrilite Live System Events Dashboard. On the left, there are two managers: 'EDR Manager' and 'XDR Manager'. The EDR Manager shows metrics for High Risk (1944), Medium (7012), and Low (403) events. The XDR Manager also has similar sections. The main dashboard area is titled 'Sentrilite Live System Events Dashboard' and features a table of live events. The table includes columns for ID, Time, Process, User, Command, and Description. The events listed are primarily PowerShell-related, showing various command executions, process creations, and network connections. The interface includes buttons for 'Download PDF Report', 'Resume', 'Alerts On', 'Alert History', and a 'Connected' status indicator.

ID	Time	Process	User	Command	Description
[2025-12-15 12:48:13]	PID=25028	UID=0	USER=DESKTOP-L25PAOQ\gaura	COMM=C:\Program Files\Google\Chrome\Application\chrome.exe	IP=198.54.122.136 TYPE=NETWORK_CONNECT [windows, network]
[2025-12-15 12:48:12]	PID=25028	UID=0	USER=DESKTOP-L25PAOQ\gaura	COMM= CMD=C:\Program Files\Google\Chrome\Application\chrome.exe	IP=3.151.131.117 TYPE=NETWORK_CLOSE [windows, network]
[2025-12-15 12:48:12]	PID=25028	UID=0	USER=DESKTOP-L25PAOQ\gaura	COMM= CMD=C:\Program Files\Google\Chrome\Application\chrome.exe	IP=3.151.131.117 TYPE=NETWORK_CLOSE [windows, network]
[2025-12-15 12:48:13]	PID=33773	UID=0	USER=DESKTOP-L25PAOQ\gaura	COMM=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	CMD=powershell ARG=-NoProfile -Command \$events = Get-WinEvent -LogName 'Microsoft-Windows-Sysmon/Operational' -MaxEvents 256 -ErrorAction SilentlyContinue   Select-Object -Property RecordId, Id, TimeCreated, Message   Sort-Object RecordId \$events   ConvertTo-Json -Compress " IP=localhost TYPE=PROCESS_CREATE [windows, process, obfuscated-script, suspicious-powershell]
[2025-12-15 12:48:08]	PID=20592	UID=0	USER=DESKTOP-L25PAOQ\gaura	COMM=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	ARG=powershell -Command " IP=localhost TYPE=SYMMON_PROCESS_CREATE [windows, sysmon, process, windowsPowerShell], Script-execution"
[2025-12-15 12:48:08]	PID=20592	UID=0	USER=DESKTOP-L25PAOQ\gaura	COMM=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	CMD=powershell ARG=-NoProfile -Command \$events = Get-WinEvent -LogName 'Microsoft-Windows-Sysmon/Operational' -MaxEvents 256 -ErrorAction SilentlyContinue   Select-Object -Property RecordId, Id, TimeCreated, Message   Sort-Object RecordId \$events   ConvertTo-Json -Compress " IP=localhost TYPE=PROCESS_TERMINATE [windows, process, powershell, script-execution]
[2025-12-15 12:48:11]	PID=27420	UID=0	USER=DESKTOP-L25PAOQ\gaura	COMM=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	CMD=powershell ARG=-NoProfile -NonInteractive -Command Get-Process   Where-Object { \$_.Path -like '*temp*' -or \$_.Path -like '*appdata\local\tmp*' -or \$_.ProcessName -like '*suspicious*' }   Select-Object -Property ProcessName, Id, Path   ConvertTo-Json   IP=localhost TYPE=PROCESS_CREATE [windows, process, non-browser-network, IobIn-Network, suspicious-process]
[2025-12-15 12:48:10]	PID=43428	UID=0	USER=DESKTOP-L25PAOQ\gaura	COMM=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	CMD=powershell ARG=-NoProfile -Command \$events = Get-WinEvent -LogName 'Microsoft-Windows-Sysmon/Operational' -MaxEvents 256 -ErrorAction SilentlyContinue   Select-Object -Property RecordId, Id, TimeCreated, Message   Sort-Object RecordId \$events   ConvertTo-Json -Compress " IP=localhost TYPE=PROCESS_CREATE [windows, process, obfuscated-script, suspicious-powershell]
[2025-12-15 12:48:11]	PID=43428	UID=0	USER= COMM= IP=localhost	TYPE=PROCESS_TERMINATE [windows, process]	
[2025-12-15 12:48:19]	PID=27420	UID=0	USER= COMM=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	CMD=powershell ARG=-NoProfile -NonInteractive -Command Get-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run' -ErrorAction SilentlyContinue   Get-Member -MemberType Properties   Where-Object { \$_.Name -notlike '\$*' }   Select-Object -Property Name"   IP=localhost TYPE=PROCESS_TERMINATE [windows, process, powershell, script-execution]	
[2025-12-15 12:48:19]	PID=44752	UID=0	USER=DESKTOP-L25PAOQ\gaura	COMM=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	CMD=powershell ARG=-NoProfile -NonInteractive -Command Get-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run' -ErrorAction SilentlyContinue   Get-Member -MemberType Properties   Where-Object { \$_.Name -notlike '\$*' }   Select-Object -Property Name"   IP=localhost TYPE=PROCESS_CREATE [windows, process, obfuscated-script, suspicious-powershell]

# Configuration

- license.key — place in the current directory (baked in image or mounted as Secret).
- sys.conf — network config, placed in the current directory (baked in image or mounted as ConfigMap).
- Rule files - (custom\_rules.json, sensitive\_files.json, windows\_security\_rules.json) reside in the working dir; rules can be managed via the dashboard.

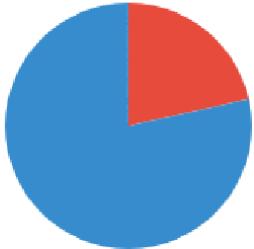
# Alert Report

From the Dashboard, click Download PDF Report to generate the Alert Summary report.

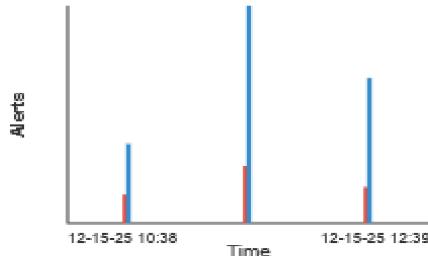
## Sentrilite Alert Report

Machine: localhost  
Generated at: 12/15/2025, 12:39:52 PM

Alerts Risk Distribution



Event Timeline (12-15-25 to 12-15-25)



### Risk Color Legend

- Critical / High risk
- Medium risk

### Alert Breakdown

High Risk: 1814  
Medium Risk: 6615  
Low Risk: 0  
Other: 63  
Total: 8492

### Tags Summary (top 10):

windows: 8492  
process: 8429  
powershell: 6614  
script-execution: 6614  
sysmon: 4673  
obfuscated-script: 1677  
suspicious-powershell: 1677  
non-browser-network: 93  
lolbin-network: 93  
suspicious-network: 93

### Top Processes / Commands

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe (6610)  
powershell (1464)  
"C:\Program Files\Google\Chrome\Application\chrome.exe" (54)  
C:\Windows\System32\RuntimeBroker.exe (52)

### Top Source IPs

No IPs with count > 5.

# Main Dashboard (for all the servers)

The screenshot shows the Sentrilite Main Dashboard. At the top, there's a header bar with the title "Sentrilite: Hybrid-Cloud Observability & Security". Below the header are buttons for "Download PDF Report", "Download Combined Alerts (JSON)", "Choose File node\_list.txt", "Upload Node List", "Download Dashboard", "Select All", and "Clear All Alerts". On the left, there's a sidebar with sections for "Create Rule", "View Rules", "Delete Rules", and "Network Rule". The main area is a table with columns: Select, Server IP, Status, Alerts, Groups, Dashboard, and AI Insights. The table lists seven servers:

Select	Server IP	Status	Alerts	Groups	Dashboard	AI Insights
■	ec2-3-17-135-143.us-east-2.compute.amazonaws.com	Online	Critical	private	Open	<a href="#">View</a>   <a href="#">Edit</a>
■	ec2-3-86-227-160.compute-1.amazonaws.com	Online	Critical	aws	Open	<a href="#">View</a>   <a href="#">Edit</a>
■	ec2-54-157-205-225.compute-1.amazonaws.com	Online	None	aws	Open	<a href="#">View</a>   <a href="#">Edit</a>
■	myapp-eastus-001.cloudapp.azure.com	Unreachable	Unknown	azure	Open	<a href="#">View</a>   <a href="#">Edit</a>
■	myapp-eastus-002.cloudapp.azure.com	Unreachable	Unknown	azure	Open	<a href="#">View</a>   <a href="#">Edit</a>
■	gke-node-01.us-central1.example.internal	Unreachable	Unknown	gcp	Open	<a href="#">View</a>   <a href="#">Edit</a>
■	gke-node-02.us-central1.example.internal	Unreachable	Unknown	gcp	Open	<a href="#">View</a>   <a href="#">Edit</a>

## Sentrilite EDR/XDR for Windows

Sentrilite EDR/XDR for Windows is a lightweight Detection-as-Code (DAC), real-time endpoint security and observability platform. It streams structured system events to a live dashboard where JSON rules drive risk scoring, tagging, alerting, and reporting.

It provides a low-overhead endpoint security layer for Windows servers and workstations without requiring heavyweight EDR agents. If Sysmon is present, Sentrilite can automatically enrich coverage by ingesting Sysmon logs; if not, it falls back to its own native collectors.

## What Sentrilite Collects on Windows

### Process Activity Monitoring

Sentrilite captures all process creation and termination and normalizes them into a unified event model:

- Full executable path (cmd / comm)
- Parent PID / child PID
- User / SID context (e.g., NT AUTHORITY\SYSTEM, local users)
- Timestamps
- Tags (e.g., windows, process, powershell, lolbin-network)

You can write rules for:

- Suspicious binaries (e.g., powershell.exe, wscript.exe, certutil.exe)

- LOLBins and lateral-movement tools (psexec.exe, wmic.exe, wmioprse.exe)
- Obfuscated or encoded script execution (e.g., -EncodedCommand, FromBase64String())
- Unexpected parent-child chains (e.g., winword.exe → powershell.exe)

## File Access Monitoring (Rule-Driven)

The Windows agent detects sensitive file usage via process arguments and custom file rules, using `custom_rules.json` and `sensitive_files.json`:

- High-risk alerts for reads/writes to sensitive paths (credentials, config, keys, etc.)
- Tag events with categories such as:
- exfiltration
- credential-access
- custom tags like “gaurav” for your own watch files

## Network Activity Monitoring

Sentrilite monitors outbound connections via Windows networking APIs (`GetExtendedTcpTable`), producing events that include:

- Local address / port
- Remote address / port
- Protocol (TCP)
- Owning process (image path)
- User context
- Basic connection state (LISTEN, ESTABLISHED, etc.)
- Rules can differentiate between:
- Browser baseline traffic vs. non-browser processes making external connections
- System services vs. unexpected user processes
- Access to special IPs (e.g., cloud metadata 169.254.169.254)

## Optional Sysmon-Aware Enrichment

If Sysmon and the Microsoft-Windows-Sysmon/Operational log are available, Sentrilite starts a Sysmon reader loop that:

- Polls Sysmon events via `Get-WinEvent`
- Maps them into the same Event structure as native events
- Adds a sysmon tag plus category tags:
- process (Event ID 1)
- network (ID 3)
- driver (ID 6)
- module-load (ID 7)
- file (ID 11)
- registry (IDs 12, 13, 14)

- wmi (IDs 19, 20, 21)
- dns, network (ID 22)
- Keeps Arg1 concise and structured (short summaries rather than raw multi-line blobs)

## Key point:

Sentrilite works without Sysmon, but if Sysmon is installed, you automatically get richer coverage with the same rule engine, same WebSocket pipeline, and same alert model.

## Detection-as-Code (DAC)

Detection logic is fully programmable using JSON:

Rule files:

- custom\_rules.json
- windows\_security\_rules.json (Details in WINDOWS\_SECURITY\_RULES\_DESCRIPTION.md)
- sensitive\_files.json

## Hot reload:

Rule files are reloaded on change — no rebuilds, no restarts.

Match on any event field, including:

- cmd, comm
  - arg1 (first argument / summarized payload)
  - user
  - ip
  - msg\_type\_str (e.g., PROCESS\_CREATE, SYSMON\_DNS\_QUERY)
  - tags
  - aliases like file, iid mapped into shared fields
- Rules can:
- Assign risk levels: 1 = high, 2 = medium, 3 = low
  - Add custom tags for later correlation / dashboards
  - Trigger alerts automatically when conditions match  
(e.g., high-risk PowerShell with encoded commands, LSASS access, non-browser outbound network, WMI-based lateral movement)

This gives Windows administrators full programmability over detection logic without touching code.

---

## Licensing

The project is currently using a trial license.key .

---

## Third-Party Integrations (PagerDuty & Alertmanager)

- PagerDuty
  - Alertmanager (Prometheus ecosystem)
  - SIEM forwarding (JSON events)
- 

## Alerts

When a rule marks an event as high-risk, Sentrilite:

- Creates a structured alert (JSON)
- Pushes it in real time to the dashboard
- Saves it to alerts.json
- Marks the node as “high risk” (risk-level = 1)
- Can forward to external systems (PagerDuty, AlertManager)

Alerts include:

- Process info
  - User identity
  - Risk reasoning via tags
  - File paths or network destinations
  - Human-readable summaries
- 

## Support

For licensing, troubleshooting, or feature requests:

-  [info@sentrilite.com](mailto:info@sentrilite.com)
-  <https://sentrilite.com>