

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:

```
.\sentrilite.exe
```

Open the dashboard.html to check live telemetry:

[illegible]

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.

Sentrilite Alert Report

Generated at.

Combined Alerts Distribution



Risk Color Legend

- Critical / High risk – immediate triage
- Medium risk – monitor & investigate
- Informational / low risk

Alert Breakdown

High Risk: 558
Medium Risk: 684
Low Risk: 637
Total: 1879
Total alerts (all nodes): 1879
Responding nodes: 3

Tags Summary (top 10):

network: 1238
privilege-escalation: 487
network-policy-change: 454
kernel: 58
firewall: 53
file: 24
permissions: 24
scanner: 19
internal: 10
error: 10

Top Processes / Commands

bash (1373)
/usr/sbin/iptables (258)
/usr/sbin/ip6tables (192)
/usr/bin/sudo (19)
package-vuln: trivy not installed or not in PATH (10)

Top Source IPs

No IPs with count > 5.

Node Risk Overview

ec2 us-east-2.compute.amazonaws.com
ec2 us-east-2.compute.amazonaws.com
ec2 us-east-2.compute.amazonaws.com

168	246	619
195	219	9
195	219	9

Main Dashboard (for all the servers)

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

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, wmiprvse.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

Sentrlite 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, Sentrlite 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
-  <https://sentrilite.com>