AURORA

Sigma detection on Windows. Configurable response per match.

Detect on the endpoint, forward only the matches. A lightweight Windows agent applies Sigma rules and IOCs to the local event stream: less data to move and store, and a response you configure.

REAL-TIME DETECTION ON WINDOWS

Detect locally. Respond on a match.

Sigma detections

Apply built-in rules or add your own behavioral detections.

IOC matching

Hashes, filenames, C2 addresses, named pipes and handles.

Extra detection modules

Cobalt Strike beaconing, LSASS dumping and process tampering. Enterprise edition.

Transparent logic

Understand why a rule matched. Tune detections and responses to your environment.

Less data to forward

Send detections as text or JSON to your backend instead of forwarding the full event stream.

On-premises operation

Keep event processing and results in your network. No Sysmon or additional kernel driver required.

nextron systems

We detect hackers.

500+ customers · 30+ countries · scanning tools recommended by security agencies

AURORA

Deploy on your terms.

Local configuration or central control through Management Center.

LOCAL DEPLOYMENT

Configuration files

Run interactively or as a Windows service. Configure rules, IOCs and outputs locally; schedule program and signature updates.

CENTRAL MANAGEMENT

MANAGEMENT CENTER

Deploy agents, target rules to asset groups, review updates and configure responses. Route results to Analysis Cockpit.

Review and respond

Review process trees, file age and dashboard notifications. Simulate responses before activation.

Tune the footprint

Set CPU and output limits. Choose configuration presets and filter false positives.

Monitor agent health

Use event statistics and diagnostics to investigate noisy sources, resource use and ETW tampering.

Choose your edition.

CAPABILITY	Lite	Enterprise
Public rules + custom content	Included	**Included**
Private Nextron Sigma + IOCs	-	**Included**
Additional detection modules	-	**Included**
Management Center integration	-	**Included**
Encrypted rules	-	**Included**
Rules with response actions	5	**Unlimited**

AURORA Lite is free for internal use. Enterprise licensing is required for paid services and use on third-party networks.

Put your detection rules to work.

info@nextron-systems.com
nextron-systems.com/aurora