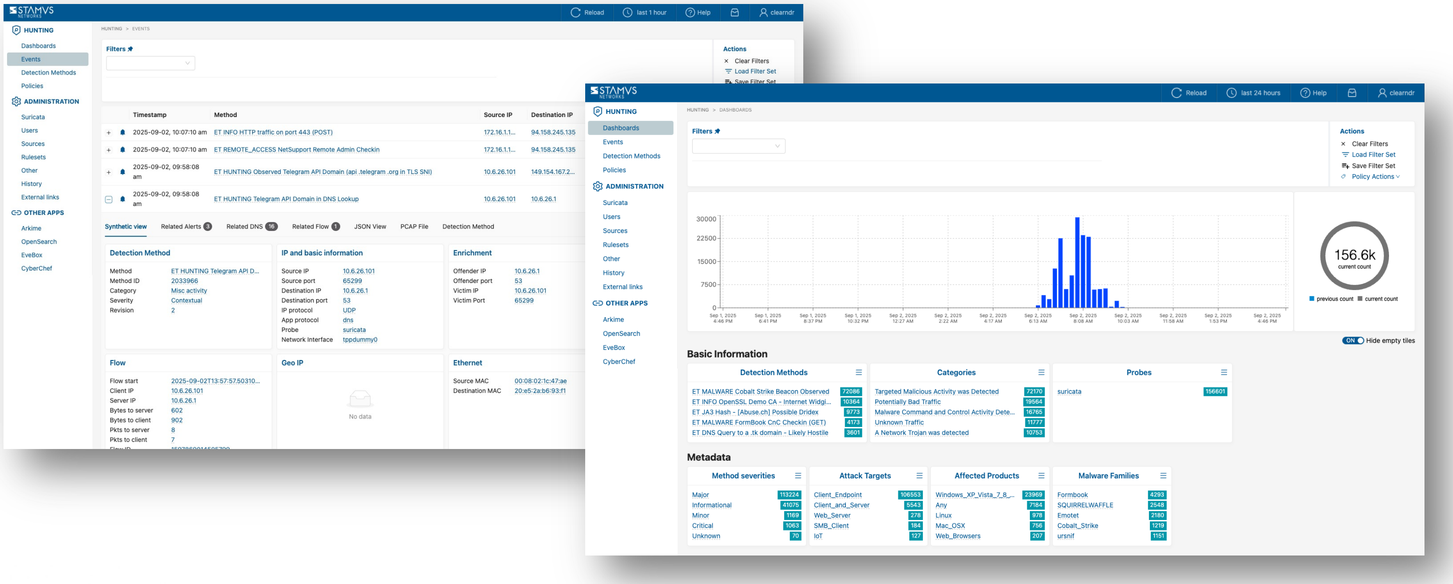
Datasheet

Clear NDR® Community
by Stamus Networks

Clear NDR Community is a free, open-source, and turn-key Suricata network detection and response (NDR) implementation – with built-in threat hunting and native AI interfaces – created and maintained by Stamus Networks.



	Timestamp	Method	Source IP	Destination IP
+	2025-09-02, 10:07:10 am	ET INFO HTTP traffic on port 443 (POST)	172.16.1.1...	94.158.245.135
+	2025-09-02, 10:07:10 am	ET REMOTE_ACCESS NetSupport Remote Admin Checkin	172.16.1.1...	94.158.245.135
+	2025-09-02, 09:58:08 am	ET HUNTING Observed Telegram API Domain (api .telegram .org in TLS SNI)	10.6.26.101	149.154.167.2...
−	2025-09-02, 09:58:08 am	ET HUNTING Telegram API Domain in DNS Lookup	10.6.26.101	10.6.26.1

Detection Method

Method	ET HUNTING Telegram API D...
Method ID	2033966
Category	Misc activity
Severity	Contextual
Revision	2

IP and basic information

Source IP	10.6.26.101
Source port	65299
Destination IP	10.6.26.1
Destination port	53
IP protocol	UDP
App protocol	dns
Probe	suricata
Network Interface	tppdummy0

Enrichment

Offender IP	10.6.26.1
Offender port	53
Victim IP	10.6.26.101
Victim Port	65299

Flow

Flow start	2025-09-02T13:57:57.50310...
Client IP	10.6.26.101
Server IP	10.6.26.1
Bytes to server	602
Bytes to client	902
Pkts to server	8
Pkts to client	7

Geo IP

No data

Ethernet

Source MAC	00:08:02:1c:47:ae
Destination MAC	20:e5:2a:b6:93:f1

Basic Information

Detection Methods	
ET MALWARE Cobalt Strike Beacon Observed	72086
ET INFO OpenSSL Demo CA - Internet Widgi...	10364
ET JA3 Hash - [Abuse.ch] Possible Dridex	9773
ET MALWARE FormBook CnC Checkin (GET)	4173
ET DNS Query to a .tk domain - Likely Hostile	3601

Categories	
Targeted Malicious Activity was Detected	72170
Potentially Bad Traffic	19564
Malware Command and Control Activity Dete...	16765
Unknown Traffic	11777
A Network Trojan was detected	10753

Probes	
suricata	156601

Metadata

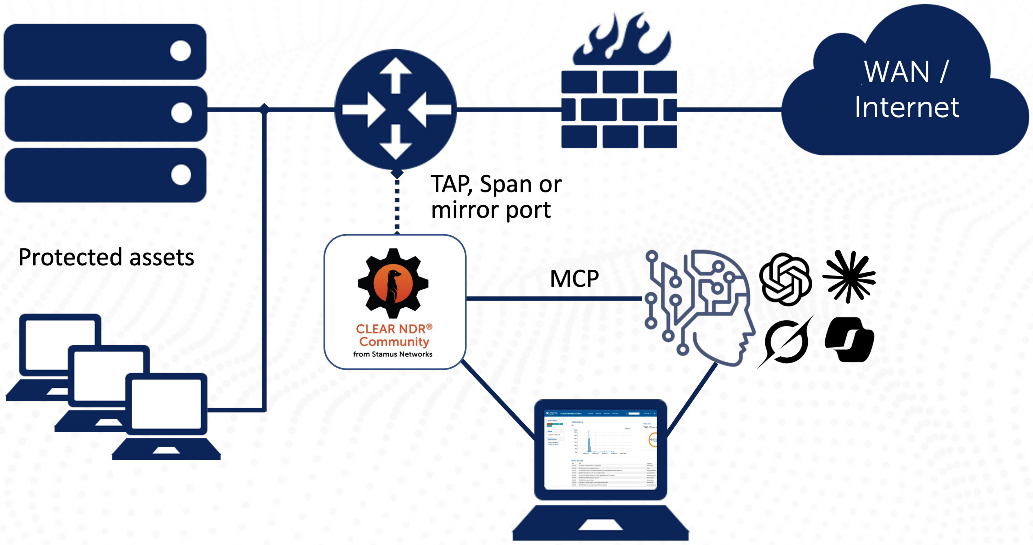
Method severities	
Major	113224
Informational	41075
Minor	1169
Critical	1063
Unknown	70

Attack Targets	
Client_Endpoint	106553
Client_and_Server	5543
Web_Server	278
SMB_Client	184
IoT	127

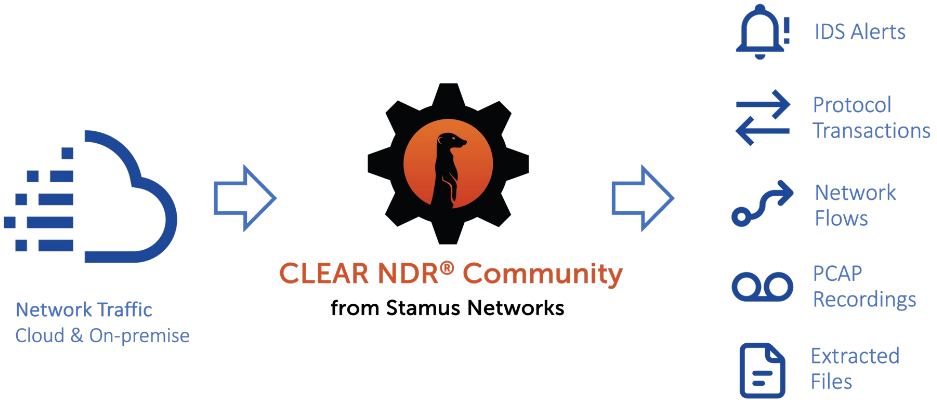
Affected Products	
Windows_XP_Vista_7_8_...	23969
Any	7184
Linux	978
Mac_OSX	756
Web_Browsers	207

Malware Families	
Formbook	4293
SQUIRRELWAFFLE	2548
Emotet	2180
Cobalt_Strike	1219
ursnif	1151

Released under GPLv3 license, the live distribution is available as either a live and installable Debian-based ISO or via Docker container on any Linux operating system.



Clear NDR Community is a showcase for the powerful Suricata IDS/IPS/NSM engine and the network protocol logs and security alerts it produces. All data in Clear NDR Community is generated by Suricata



WHAT IS INCLUDED IN CLEAR NDR COMMUNITY

The following is a list of the key open-source components incorporated in Clear NDR Community:

- Suricata: Suricata 8.0
- Fluentd: Open source data collector
- OpenSearch: Open source, enterprise-grade search and observability suite
- Evebox: Suricata alert and event management tool
- Arkime: Network analysis & packet capture
- Scirius: This Suricata hunting and ruleset management interface - developed by Stamus Networks - manages multiple Suricata rulesets and threat intelligence sources
- Model Context Protocol (MCP) – standard interface to third party AI systems

NOTE: All of the above component are pulled and instantiated using a single Go binary called *StamusCtl*. Instructions for which can be found on the the documentation site

SCIRIUS – CLEAR NDR USER INTERFACE

The Clear NDR - Community user interface (also known as Scirius) is the Stamus Networks open-source application that brings all these components together. It provides the web interface for the entire system, giving you the ability to:

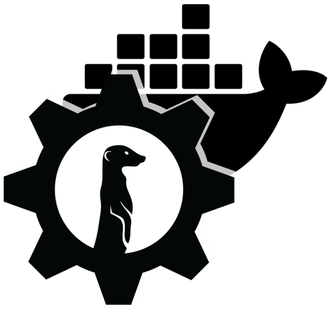
- Manage multiple Suricata rulesets and threat intelligence sources
- Upload and manage custom Suricata rules and IoC data files
- Hunt for threats using predefined filters and enhanced contextual views
- Apply thresholding and suppression to limit verbosity of noisy alerts
- View Suricata performance statistics and information about Suricata rule activity
- Apply EveBox, Cyberchef and over 50 OpenSearch dashboards to the Suricata NSM and alert data

Note: Scirius is bundled with the other elements into a single system. It is not possible to manage multiple Clear NDR instances with Scirius.

THREE INSTALLATION OPTIONS

Clear NDR Community is available either as a portable Docker Compose package or as turnkey installation images (ISO files).

Docker Containerized Package



Use the Docker containerized package to install Clear NDR Community in any LINUX environment and ensure you are including the very latest containers, including Evebox and Suricata.

Complete Image with Desktop

Use the image with Desktop when you want a turnkey installation that includes the Debian x64 12 (Bookworm) Linux desktop environment. Can be deployed on bare metal hardware or VM.

Complete Image without Desktop

Use the image without Desktop when you want a turnkey Clear NDR Community installation in a headless environment (based on Debian 12 Bookworm). Can be deployed on bare metal hardware or VM.

PLATFORM REQUIREMENTS

The following are the minimum requirements for installing Clear NDR Community:

- 2 CPU cores (x86)
- 8-10 GB of free RAM
- 50GB (10 GB for Docker package) of free disk space (high-performance SSD is recommended)
- 2 network interfaces

Because both Suricata and OpenSearch are multithreaded, performance will improve with additional cores. Likewise, by allocating additional memory, Clear NDR Community will more easily support additional traffic loads. Finally, more disk space is required to support higher traffic rates and longer data retention.

WHO IS CLEAR NDR COMMUNITY DESIGNED FOR?

For many small-to-medium sized organizations, Clear NDR Community can be a suitable production-grade NDR.

And because all the data available in Clear NDR Community is generated by the Suricata engine, Clear NDR Community is widely used by network security practitioners, educators, and hobbyists to explore what is possible with Suricata IDS/IPS/NSM and the network protocol monitoring logs and alerts it produces.

For enterprise scale applications, please review our commercial solution, Clear NDR Enterprise, described below.

REPORT ISSUES AND GET SUPPORT

To access README documentation, the issues tracker, and the Clear NDR Community wiki, please visit the Clear NDR GitHub page here: https://github.com/StamusNetworks/SELKS

To ask questions or ask for help, join the Stamus Networks Discord server here: https://discord.com/invite/e6GQKGS5HN

WHAT ABOUT ENTERPRISE SCALE DEPLOYMENTS?

While Clear NDR Community is an excellent platform to explore the power of Suricata for intrusion detection and threat hunting, it was never designed to be deployed in an enterprise setting. For enterprise applications, please review our commercial solution, Clear NDR Enterprise edition.

To learn more about the differences between Clear NDR Community and our enterprise solutions, refer to the white paper, Understanding Clear NDR Community and Stamus Commercial Platforms.

Download it here: https://www.stamus-networks.com/selks#enterprise

	Basic capabilities offered by Clear NDR® - *Community*	**Additional** capabilities in Clear NDR® - *Enterprise*
Primary Use Cases	• Single site IDS/IPS replacement • Single site open source NDR • Suricata education and threat research	• Multi-site hybrid enterprise attack surface (cloud, branch office, data center, etc) • Enabler of the AI-powered Autonomous SOC • Enterprise network detection and response • Regulatory or directive compliance
Best Fit Organizations	• Small organizations • Students • Threat researchers	• Medium-to-extra large Enterprises with a dedicated security operations team • Highly-targeted entities, including critical infrastructure • Managed security service providers (MSSP or MDR)
Detection mechanisms	• Signatures • IoC matching	• AI and Machine learning • Statistical algorithms • Other heuristics
Event types	• IDS Alerts • Network protocol transactions • Flow records	• Suspicious events – such as C2 beacons, host outliers, SMB insights • Sightings – host and user anomalies • Declarations of Compromise™ (DoC) – ultra high-confidence threat events • Declarations of Policy Violations™ (DoPV) – high-confidence events triggered by organization-specific policy violations • Rich source of structured network metadata - ideal for use in AI models for the autonomous SOC
Evidentiary artifacts	• Network protocol transactions • Flow records • Conditional PCAP • File extraction	• Incident timeline • Cyber kill chain mapping • Optional conditional logging • File extraction
Event workflow and triage	• Manual	• Users are presented high-fidelity threat incidents (DoC) and policy violation (DoPV) events, and incident investigation is aided by an attack timeline, detailed evidence collection and review, and reporting • Experienced users may tag events as "Informational" or "Relevant" and are automatically classified by the system for easy prioritization by less experienced users
Response Automations	• Not included • Can be built using API calls into the event data.	• Triggered based on high-fidelity detection events – DoC and DoPV • Simple notifications such as email or messaging • Sophisticated responses, including policy changes, quarantine actions, or playbook initiations in third party systems such as XDR, EDR, SOAR, IR, or Firewall systems
Other Integrations	• Third party threat intelligence and rulesets • API-based query and control • User interface contextual deep linking into other systems • Model context protocol (MCP) with basic endpoints	• Pre-built integrations into various third-party systems to support the response automations described above • These include XDR, EDR, SOAR, IR, Firewall, DDI, and more • Straightforward integrations into other systems via API, Webhook, custom deep-linking, and email • Model context protocol (MCP) endpoints provide access to advanced network intelligence for DoC, DoPV, Host Insights, and more
Host attributes	• May be collected via periodic queries into database and correlated using third party analytics	• Hosts are auto-classified into device types (roles), such as domain controllers, printers, proxy servers, etc • Host Insights – collects and maintains 60+ attributes for every host seen on the network (up to millions) • Attack surface inventory - identifies all hosts seen communicating on the network
Organizational context	• Usernames are extracted and presented	• Associates host names, usernames, and organization-specific network names for rapid assessment and identification during triage and incident response
Support	• Support is through the open-source user community • Issues and feature requests reported via GitHub	• Enterprise-class onboarding, training, and technical support • Dedicated customer success manager • Quarterly business reviews • Issues and feature requests logged and tracked though ticketing system

ABOUT STAMUS NETWORKS

Stamus Networks believes that cyber defense is bigger than any single person, platform, company, or technology. That's why we leverage the power of community to deliver the next generation of open and transparent network defense. Trusted by security teams at the world's most targeted organizations, our flagship offering – Clear NDR® – empowers cyber defenders to uncover and stop serious threats and unauthorized network activity before they harm their organizations. Clear NDR helps defenders see more clearly and act more confidently through detection they can trust with results they can explain.

STAMUS® NETWORKS

5 Avenue Ingres
75016 Paris
France

450 E 96th St. Suite 500
Indianapolis, IN 46240
United States

contact@stamus-networks.com
www.stamus-networks.com