PRODUCT DATASHEET · 2026

# CodeRed NDR Sensor

SENSOR SOFTWARE v1.3.0

Passive Network Detection & Response Sensor

CodeRed NDR inspects a copy of your network traffic. It pulls that copy from a SPAN port or hardware TAP, reconstructs every session in real time, and turns raw packets into high-fidelity detections: command-and-control beacons, lateral movement, credential attacks, ransomware and exfiltration, all before they reach your crown jewels.

Twenty behavioral engines and a signature IDS cover roughly 75 MITRE ATT&CK techniques out of the box, while a per-host machine-learning baseline catches the deviations no rule was written for. Every alert lands in the SIEM you already run.

⬡ Behavioral ML + Signature IDS · ~75 ATT&CK Techniques

### Built for passive deployment

The sensor sits out of band on a SPAN or TAP and never bridges traffic, so a sensor fault can slow detection without taking the network down.

### Built for the SOC floor

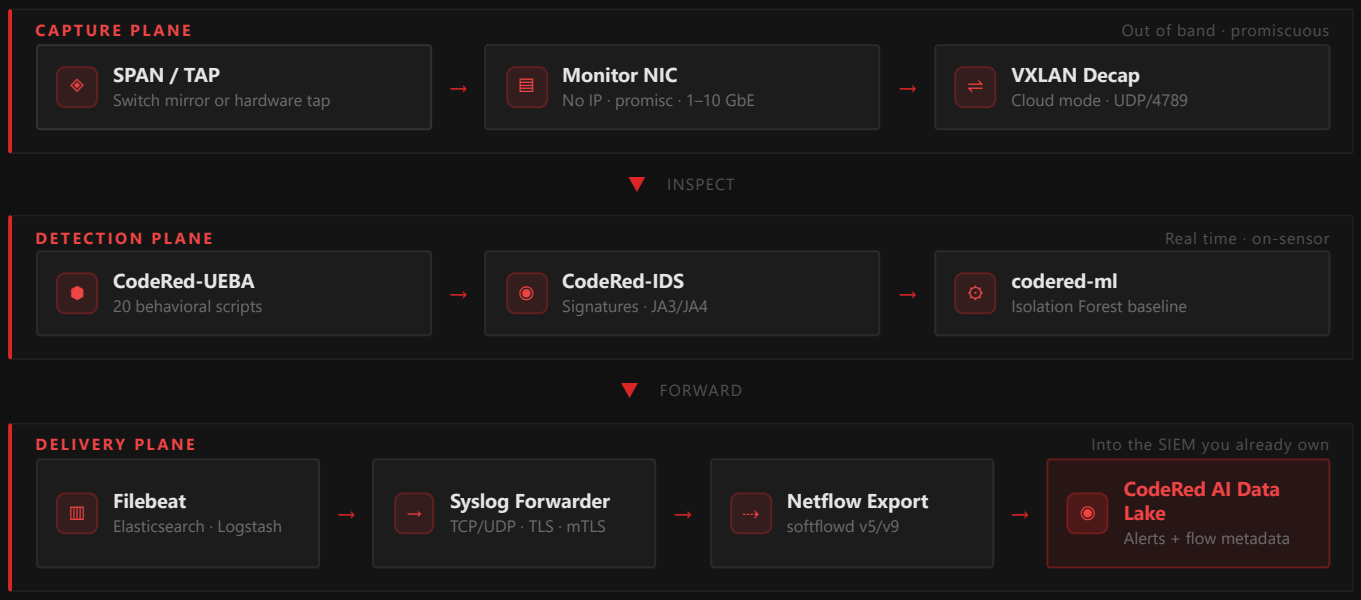
Alerts ship as CEF/JSON over Syslog, Beats or Elasticsearch, with Netflow feeding the SIEM's NDR module in parallel. No new console to learn.

PLATFORM OVERVIEW

# Full-Fidelity Traffic Analysis, Zero Inline Risk

A single OVA deploys in minutes. The sensor needs two network interfaces: one for management and one for the mirrored traffic feed. From that copy of the wire it runs protocol analysis, signature matching, TLS fingerprinting and machine-learning baselining at the same time, then forwards the results to your SIEM.

## System Architecture




## Why This Matters

Endpoint tooling is blind to unmanaged devices, IoT, OT controllers and the attacker's own infrastructure. The network sees all of them: every device that sends a packet is in scope, agent or not.

Rule and signature detections fire the moment traffic arrives. The ML engine adds a per-host baseline once it has 50 hours of that host's history.

### Core Components

| | |
|---|---|
| **CodeRed-UEBA** | Protocol parser running all 20 behavioral detection scripts |
| **CodeRed-IDS** | Signature IDS with JA3/JA4 TLS fingerprinting |
| **codered-ml** | Per-host anomaly detection via Isolation Forest |
| **Filebeat / Forwarder** | Ships alerts and logs to the SIEM |

## Deployment Model

### VIRTUAL APPLIANCE

Ships as an OVA for VMware ESXi/vSphere and Proxmox. A guided wizard configures the management IP, monitor interface and SIEM destination in about five minutes, then starts every service for you.

### CLOUD & ON-PREM

On-prem mode reads raw SPAN/TAP traffic. Cloud mode decapsulates the VXLAN wrapper used by AWS, Azure, Alibaba Cloud and GCP traffic mirroring. A single toggle switches between them.

### FULLY PASSIVE

The monitor NIC carries no IP address and never transmits. The only inbound path is SSH on the management interface, which is locked to admin ranges and fail2ban-protected.

DETECTION COVERAGE

# ~75 ATT&CK Techniques. Twenty Behavioral Engines.

CodeRed-UEBA reconstructs each protocol and reasons about behavior; CodeRed-IDS matches known-bad signatures and fingerprints. Together they map to roughly 75 MITRE ATT&CK techniques. Rule-based detections fire immediately, with no warm-up or training window.

| ~75 | 20 | JA3 / JA4 / HASSH | Immediate |
|---|---|---|---|
| ATT&CK techniques | Behavioral engines | Encrypted-traffic fingerprinting | No warm-up required |

## Command & Control and Covert Channels

| ENGINE | WHAT IT DETECTS |
|---|---|
| beaconing | Low-jitter C2 callbacks tracked per src–dst pair, including east-west internal beaconing T1071 · T1573 |
| ja3-fingerprint | JA3/JA3S TLS fingerprints for Cobalt Strike (15 profiles), Metasploit, Sliver, Brute Ratel, Havoc, AsyncRAT and more T1573.002 |
| http-c2 | Domain fronting, 20+ malleable C2 URI patterns, fast-flux DNS, DoH bypass and LOLBin user-agents T1090.004 · T1568.003 |
| dns-anomaly | DGA scoring by Shannon entropy and DNS tunnelling via long labels / high query rates T1568.002 · T1071.004 |
| icmp-tunnel | Oversized payloads, high ICMP rate and large ICMP data volume (icmptunnel, ptunnel, Hans) T1095 · T1572 |
| protocol-anomaly | Protocol/port mismatch, Tor exit connections, IPv6-in-IPv4 tunnelling, SNMP enumeration T1571 · T1572 |

## Lateral Movement

| ENGINE | WHAT IT DETECTS |
|---|---|
| lateral-smb | Admin-share access (C$, ADMIN$), remote service install via named pipes, Pass-the-Hash auth spikes T1021.002 · T1550.002 |
| lateral-rdp | RDP brute force, credential spray across targets and workstation-to-workstation hops T1021.001 · T1110 |
| lateral-wmi | WMI/DCE-RPC, DCOM binding, WinRM/PowerShell remoting and PsExec/PAExec named pipes T1047 · T1021.006 |
| hassh-ssh | SSH client HASSH fingerprints (Paramiko, Impacket, AsyncSSH), brute force and non-standard ports T1021.004 · T1110 |

*Detection thresholds and whitelists (jump servers, domain controllers, business hours) are tunable per environment without editing the detection scripts themselves.*

# Credentials, Exfiltration & Commodity Threats

## Credential Attacks

| ENGINE | WHAT IT DETECTS |
|---|---|
| kerberos-attacks | Kerberoasting (RC4 TGS-REQ bursts), AS-REP roasting, Golden/Silver ticket lifetimes and principal enumeration T1558.001–004 |
| credential-access | LLMNR/NBT-NS poisoning (Responder), NTLM relay, LDAP AD recon, high-value LDAP filters and SAMR/LSARPC enumeration T1557.001 · T1087.002 |

## Exfiltration & Impact

| ENGINE | WHAT IT DETECTS |
|---|---|
| ransomware | SMB mass-write bursts, 20 ransomware extensions, shadow-copy deletion via WMI, double-extortion exfil and executable staging T1486 · T1490 |
| insider-threat | Internal data staging (1 GB+), mass share access, FTP upload exfil, bulk email and off-hours external transfers T1074 · T1048.003 |
| long-connections | TCP sessions beyond 24 hours and asymmetric transfers (10:1 out:in over 100 MB) T1041 · T1048 |

## Commodity Threats & Reconnaissance

| ENGINE | WHAT IT DETECTS |
|---|---|
| cryptomining | Stratum protocol on 9 mining ports, 30+ known pool domains, miner user-agents (XMRig, ccminer, sgminer) T1496 |
| scan-detect | Port scans (20+ ports to one host) and network sweeps (15+ hosts on one port) inside 5 minutes T1046 |
| cert-anomaly | Self-signed certs to external hosts, sub-7-day validity, expired certs in use and IP-address Common Names T1587.003 |

*Two layers of detection*

Signature and behavioral rules need no history; they alert the instant matching traffic appears. The machine-learning engine on the next page adds a second layer that catches the slow, novel and low-and-slow activity a fixed threshold misses.

MACHINE LEARNING & SPECIALISED COVERAGE

# A Baseline Per Host, Not Per Network

## ML Behavioral Engine

Isolation Forest · no GPU, no labels

The engine learns what normal looks like for each internal host and alerts when that host drifts from its own history. A network-wide average would hide that outlier; a per-host baseline surfaces it.

- Reads conn, dns and http logs every 60 seconds
- Aggregates 9 features per host per hour into SQLite
- Trains per host after 50 hours on a 7-day window
- Scores each new hour and ships anomalies to the SIEM

### Features Tracked

conn_count · bytes_out · bytes_in · unique_dsts · ext_dsts · dns_queries · unique_fqdns · http_reqs · avg_duration · bytes_ratio

**BOUNDED BY DESIGN**

Capped at 25% CPU and 512 MB RAM at Nice 10 (typically 150–200 MB), so the model never starves CodeRed-UEBA or CodeRed-IDS.

### ML Alert Types

| | |
|---|---|
| **ML_DataExfiltration** | Bytes-out spike to external hosts (>5× baseline) |
| **ML_DNS_Anomaly** | DNS query or unique-domain volume spike |
| **ML_Reconnaissance** | External destination spread (>4× baseline) |
| **ML_ConnectionSpike** | Unusual total connection volume (>5×) |
| **ML_BehavioralAnomaly** | Multi-feature deviation from host baseline |

## OT / ICS Monitoring

| | |
|---|---|
| **Modbus TCP · 502** | Unauthorised coil/register writes |
| **DNP3 · 20000** | Direct Operate, Cold/Warm Restart |
| **EtherNet/IP · 44818** | PLC access from unexpected sources |
| **IEC 60870-5-104 · 2404** | Substation automation anomalies |
| **OPC-UA · 4840 / BACnet · 47808** | Industrial & building automation |

*Plus IT-to-OT lateral movement and OT reconnaissance detection.*

## Cloud Threat Detection

| DETECTION | WHAT IT CATCHES |
|---|---|
| **IMDS credential theft** | Any internal host reaching 169.254.169.254 (SSRF or container escape) T1552.005 |
| **AWS key exposure** | IAM key prefixes (AKIA, ASIA, AROA) seen in HTTP headers T1552.005 |
| **Cloud storage C2** | S3, Azure Blob, GCP Storage, Dropbox, Mega, Discord CDN used for staging/exfil T1102 · T1567.002 |
| **Tunnelling SaaS & large uploads** | ngrok / serveo / pagekite pivots and 50 MB+ outbound transfers T1572 · T1537 |

INTEGRATION & DELIVERY

# Alerts and Flow, Into Your SIEM

## → SIEM Forwarding

Four output types, one wizard

Filebeat ships to Elasticsearch and Logstash; a built-in syslog forwarder handles everything that speaks RFC5424. The wizard tests connectivity before it saves.

| | |
|---|---|
| **Elasticsearch** | HTTP/HTTPS JSON · 9200 / 9243 |
| **Logstash** | Beats protocol TCP · 5044 |
| **Syslog TCP** | RFC5424, optional TLS (RFC5425) + mTLS · 514 / 6514 |
| **Syslog UDP** | RFC5424 · 514 |

Validated with Wazuh, Pre Security, QRadar, ArcSight, Graylog, Splunk and any rsyslog / syslog-ng front end.

### Encrypted Transport (TLS)

| | |
|---|---|
| **System CA** | Verify against the OS trust store |
| **Custom CA** | Pin a private/self-signed PEM (recommended) |
| **mTLS** | Client-cert auth, layered on any verify mode |
| **Skip verify** | Bring-up only; loud MITM warning each connect |

## ⇢ Netflow & Monitoring

Flow metadata + operator visibility

A built-in softflowd exporter feeds your SIEM's NDR module with flow metadata for traffic baselining and network mapping. It runs alongside the syslog forwarder, and both stay active.

| | |
|---|---|
| **Netflow versions** | v5 (fixed) or v9 (template-based) |
| **Transport** | UDP to collector · default 2055 |
| **Runs with syslog** | Independent services, no conflict |

### Operator Visibility

- Live sensor status: services, disk, CPU, drop rate
- Packet-capture monitor for top talkers and protocol mix
- Guided diagnostics for SPAN, SIEM, NTP and freshness
- One-command redacted support bundle

### Alert Conditions

SPAN traffic lost · SIEM unreachable · Packet drop spike · Service down

**MANAGED FROM ONE MENU**

One SSH CLI menu drives every setting: SIEM destination, TLS, deployment mode, monitor interfaces and Netflow. You never hand-edit a config file.

TECHNICAL SPECIFICATIONS

# Sensor Specifications

## Virtual Appliance

| | |
|---|---|
| **Delivery** | OVA for VMware ESXi/vSphere and Proxmox |
| **CPU** | 4 vCPU minimum · 8 vCPU recommended |
| **RAM** | 8 GB minimum · 16 GB recommended |
| **Disk** | 100 GB minimum · 500 GB for busy links |
| **NICs** | 2 (mgmt + monitor) · 3+ for multi-zone |
| **Deployment mode** | On-prem (raw SPAN/TAP) or cloud (VXLAN) |

## Detection Engines

| | |
|---|---|
| **Behavioral** | CodeRed-UEBA, 20 detection scripts |
| **Signature** | CodeRed-IDS with JA3/JA4 fingerprinting |
| **Machine learning** | codered-ml, per-host Isolation Forest |
| **ATT&CK coverage** | ~75 techniques |
| **OT protocols** | Modbus, DNP3, EtherNet/IP, IEC-104, OPC-UA, BACnet |
| **Warm-up** | Rules immediate · ML after 50 h per host |

## Forwarding & Export

| | |
|---|---|
| **SIEM outputs** | Elasticsearch, Logstash, Syslog TCP/UDP |
| **Encryption** | TLS (RFC5425) with optional mutual TLS |
| **Netflow** | softflowd v5 / v9 over UDP |

## Network & Firewall

| | |
|---|---|
| **Outbound 9200 / 9243** | Elasticsearch (HTTP / HTTPS) |
| **Outbound 5044** | Logstash (Beats, optional TLS) |
| **Outbound 514 / 6514** | Syslog plaintext / TLS |
| **Outbound 2055** | Netflow to SIEM NDR module (UDP) |
| **Outbound 53 / 123** | DNS resolution / NTP sync |
| **Outbound 443** | IDS rule & threat-intel updates |
| **Inbound 22** | SSH management, restricted to admin ranges |

## Security Hardening

| | |
|---|---|
| **SSH** | Root login disabled, modern ciphers only, 15-min idle cut-off |
| **Brute-force defence** | fail2ban: 4 fails in 5 min = 30-min ban |
| **Password policy** | Min 12 chars; upper + digit + symbol; PAM-verified |
| **File permissions** | Config 640, credentials 600, NSM data 750 |
| **Applied by** | Installer applies it, no manual steps |

SIZING

vCPU, memory and disk retention scale with monitored bandwidth and log-retention window. For links at or above 1 Gbps a hardware TAP is recommended over SPAN. Our team sizes the sensor against your traffic profile as part of onboarding.

# See the Traffic Endpoints Can't.

Mirror a port to the sensor and watch the first detections land in your SIEM the same day.

## Get In Touch


**Email**
business@coderedcyber.ai

**Website**
https://coderedcyber.ai

**Provintell Technologies Sdn. Bhd.**
Powered by CodeRed Cyber


## See It Running

A live proof of value on your own network. We deploy the sensor against a SPAN of your choosing and review the detections it surfaces with your team.

**BOOK A TECHNICAL WALKTHROUGH**
https://coderedcyber.ai

## Deploys Alongside

The NDR Sensor is one component of the CodeRed platform. Its alerts and flow enrich the same SIEM fed by the rest of the estate.

### CodeRed AI Log Manager

Universal log acquisition and SIEM forwarding, with AI-generated connectors for any source. Covered in its own datasheet.

### CodeRed Server Agent

Endpoint telemetry across Linux, macOS and Windows. Covered in its own datasheet.

## Why Teams Choose It

- ✓ Every device on the wire is in scope
- ✓ ~75 ATT&CK techniques out of the box
- ✓ Behavioral ML on top of signatures
- ✓ Runs fully passive, with no inline risk
- ✓ Feeds the SIEM you already own