Stop Malware — before it calls home.

Detect silent, periodic check-ins signalling a compromised device. The threats your antivirus never sees.

24/7	≤1hr	6	10
PASSIVE MONITORING	ALERT RESPONSE	DETECTION LAYERS	LIVE DASHBOARDS

THE PROBLEM

Your Antivirus Won't Catch This

Modern malware rarely announces itself. Instead, it installs silently, then reaches out to its operator via short, regular, encrypted messages — **beacons**. Once a live command channel is confirmed, attackers push further: lateral movement, data exfiltration, ransomware deployment.

Traditional defences inspect files and signatures. Beacons don't look like malware. They look like background traffic — which is exactly the point.

Ransomware Pre-staging

Operators verify access and map the network before encrypting — beacons are the first sign something is wrong.

Persistent Access Trojans

RATs check in every few minutes. Signature scanners see a normal process. Beacon analysis sees the pattern.

Stealthy Data Exfiltration

Small, consistent payloads sent at fixed intervals are invisible to volume-based anomaly detection.

Supply-chain Implants

Trusted software can be compromised. Even legitimate-looking traffic must be profiled for periodic behaviour.

THE SOLUTION

Behavioural Network Monitoring

Beacon Butty sits between your LAN and the internet, tracking and scoring every connection — without any packets being blocked or delayed. Zero impact on your network performance.

Rather than matching against known-bad signatures, it measures *behaviour*: connection regularity, consistent payload sizes, unusual destination profiles. These statistical patterns survive encryption and obfuscation.

B

Beacon Scoring

RITA v5 scores every host on periodicity, jitter, packet size and duration.

I

Intrusion Detection

Suricata IDS scans live traffic against thousands of signatures, with smart noise filtering.

N

Network Intelligence

TLS/DNS anomalies, geo, ASN, Tor exit nodes and domain entropy.

A

Asset Inventory

Automatic LAN discovery via DHCP, ARP and Nmap with OS and open ports.

F

FP Control

A MAC-keyed registry suppresses known-benign devices and domains.

!

Instant Alerts

Slack notifications with enable/disable and suppression windows.

A Six-Layer Detection Pipeline

1 Passive Packet Capture `Zeek 8`

Zeek monitors all LAN traffic on the internal interface — passively, with zero impact on throughput. Every TCP/UDP connection is logged with full metadata: timestamps, bytes, state, duration and TLS handshake details.

2 Beacon Scoring Engine `RITA v5`

Hourly, RITA imports Zeek connection data and runs statistical analysis per source/destination pair, scoring each on four axes: periodicity, jitter, byte-size consistency, and connection duration. Strobes and threat-intel hits are surfaced separately.

3 Signature-Based IDS Overlay `Suricata IDS`

Suricata runs concurrently with thousands of community and Emerging Threats signatures against live traffic. STREAM and QUIC noise is filtered automatically. Alerts are correlated back to the asset inventory via MAC and IP.

4 High-Performance Storage `ClickHouse · log2ram`

A columnar time-series database on NVMe SSD stores beacon scores, connection records, IDS alerts and host metrics. Sub-millisecond queries across weeks of data; live logs land on a RAM-backed tier to extend SSD lifespan.

5 Web Dashboard `Flask · Chart.js · HTTPS`

A Flask web application served over HTTPS provides real-time visibility across every detection layer. Ten purpose-built pages cover beacons, IDS, assets, intel, health, backup and hardware telemetry.

6 Alerting & Daily Digest `Slack · AWS Lambda · email`

A daily 07:00 digest summarises top beaconing hosts. Real-time alerts route through AWS Lambda to Slack, with per-type enable/disable and per-alert suppression windows. Test-fire any alert from the dashboard.

Detection Coverage

Periodic C2 Beacons
Statistical jitter and periodicity scoring catches malware check-ins regardless of obfuscation.

Persistent Strobes
Long-lived single-destination connections — the operational tell of an active C2 channel.

Tor Exit Node Contacts
Connections to known Tor infrastructure flagged immediately — a reliable indicator of compromise.

Threat Intel Hits
Destinations checked against curated threat-intelligence feeds — known bad IPs and domains.

Exploit Attempts
Suricata rules cover active exploit signatures: CVE payloads, shellcode, protocol abuse.

High-Entropy DNS
Random-looking subdomains — a common DGA and DNS-tunnelling tell — scored on SLD entropy.

Excessive DNS Volume
Hosts generating unusually high DNS query volumes — a common indicator of C2 location attempts.

New & Rogue Devices
A new MAC on the LAN triggers an immediate notification the moment it appears.

Alert Criteria

REAL-TIME

- High-score beacon (1.0)
- Persistent strobe traffic
- Threat-intel destination match
- Tor exit node contact
- Suricata P1 LAN rule
- Repeated Suricata P1 hits
- Service down (Zeek / CH / Suricata)
- Disk > 90% full
- New device on LAN

DAILY DIGEST

- Top beacon scorers
- Suricata P2 / P3 summary
- New devices (24h)
- High-DNS-volume hosts
- TLS / DNS anomaly digest
- Suppressed-by-FP recap
- Health & capacity headline

A SELF-MONITORING APPLIANCE

Continuous Health Monitoring
Every dependent service checked on a timer. Failures auto-page Slack with diagnostics.

Hardware Telemetry
CPU temp, fan speeds, memory, disk and uptime tracked over time. Tiered cooling.

Backup & Recovery
Three-tier backup including full system clone to USB SSD. Documented restore.

Encrypted Remote Access
Optional Tailscale enrolment for secure remote support — no inbound exposure.