# HYPERVIGIL

BY BLOCK ARMOUR

HYPERVIGIL – A 'SOC IN A BOX' TO HELP SMEs IMPROVE SECURITY POSTURE, EFFECTIVELY MANAGE INCIDENTS, AND COMPLY WITH REGULATIONS

# BACKGROUND:

SMEs are the backbone of an economy, and their limited cyber hygiene can result in cyberattacks on downstream OEMs, critical infrastructure/services, and end users

*A SOC can help an SME to improve its cybersecurity posture, efficiently detect and respond to cyberattacks, as well as adequately comply with regulatory requirements*

**SIEM**
Threat Detection, event correlation, and incident alerts

**SOAR**
Automate and streamline incident response processes

**Threat Intelligence**
Relevant CTI feeds to identify and assess threats

**Playbook/ Runbook**
Best-practice based incident investigation and response

However, enterprises and MSSPs struggle to deploy, manage, and maintain traditional SOCs due to the prohibitively high costs and multiple complexities involved.

**Content:** Generic design, architecture, and content which lacks organizational context

**Cost:** Huge investment required in SIEM licenses and technical personnelt

**Manual:** Lacks automated quick-response mechanisms and needs integrations

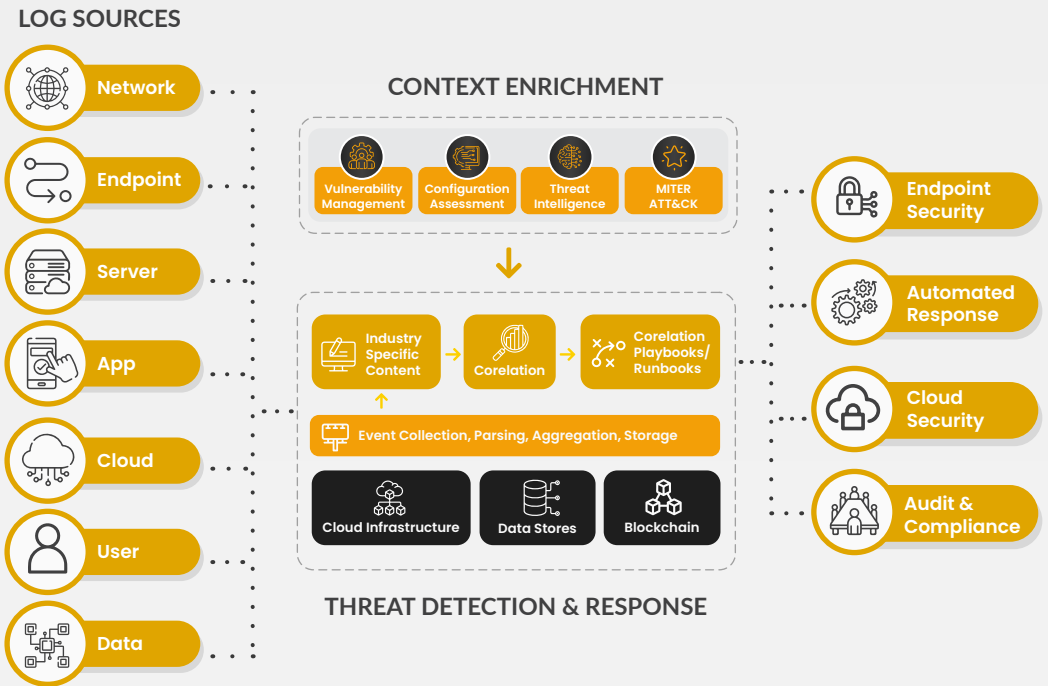**Overwhelming:** Riddled with too many false positives that overwhelm the team and systems

*Furthermore, the niche technical capabilities required puts a traditional SOC out of reach of SME's as well as select enterprises*

# THE SOLUTION:

Block Armour blends decades of hands-on experience in security operations with best-practice processes and leading open-source tools to deliver HyperVigil

*... a modular, affordable, and 'agile' SOC*

Provided on-premise as well as via Cloud and MSSP marketplaces, the solution is easily deployable and include industry specific use cases for accurate monitoring and early detection of security breaches

## LOG SOURCES

- Network
- Endpoint
- Server
- App
- Cloud
- User
- Data

## CONTEXT ENRICHMENT

- Vulnerability Management
- Configuration Assessment
- Threat Intelligence
- MITER ATT&CK

- Industry Specific Content
- Corelation
- Corelation Playbooks/ Runbooks

Event Collection, Parsing, Aggregation, Storage

- Cloud Infrastructure
- Data Stores
- Blockchain

## THREAT DETECTION & RESPONSE

- Endpoint Security
- Automated Response
- Cloud Security
- Audit & Compliance

With matured threat detection content and best-practice processes, HyperVigil helps SMEs to efficiently manage and respond to security incidents / vulnerabilities

*Available 'Out-of-the-Box', HyperVigil is easy to implement, easy to manage, and is a smarter cost-effective alternative to proprietary options available in the market. The integrated alerting and reporting capabilities simplifies compliance with regulations.*

# GET THE HYPERVIGIL ADVANTAGE:

Deploying a smart affordable SOC will enable SME to improve cybersecurity posture, comply with regulations, and in-turn effectively thwart supply chain attacks

**Cost Effective:** Save on expensive proprietary software license costs

**Integrated:** Alerts & reporting for compliance with regulations

**Smarter:** Automated response for efficient breach containment/remediation

**Accurate:** Better detection accuracy with Context Enrichment

*HyperVigil is democratizing SOCs and making it easy for organizations – large and small – to afford, set up, and manage one*