

Subhash Bharadwaj.

Security Engineer | Bengaluru, India
subhashb.dev@zohomail.in | subhashb05.in | github.com/Sbharadwaj05
linkedin.com/in/subhash-bharadwaj-c-s-391209281

Security engineer working on detection systems, OT/ICS security and the infrastructure underneath both. 79 detection rules and a 28-tool MCP server for Wazuh shipped in the open under MIT and Apache 2.0.

EXPERIENCE

Software Engineer, Parivartan Technologies Oct 2025 - Present

Promoted April 2026

- Brought up the full Parivartan infrastructure: RKE2 Kubernetes on 3-hypervisor libvirt/KVM (air-gap capable) via Terraform and Ansible, with CloudNativePG, Strimzi Kafka, MinIO, cert-manager and Longhorn operators.
- Designed the ConnectorState FSM, CapabilityUrn system and three-layer separation rule for the 16-tool compliance connector framework.
- Built the Entra ID connector (Microsoft Graph API, async aiohttp) and the mock_security connector, shipped with a unit/mapping/live test triad through automated CI certification.
- Debugged and stabilised a 5-service Rust gRPC microservice chain, restoring end-to-end data flow from evidence ingestion through cryptographic sealing, evaluation and remediation dispatch.
- Built an OT digital twin annotation engine: 3 mesh segmentation strategies producing 52-component assemblies with IEC/ISA taxonomy manifests in Unreal Engine 5.

OPEN-SOURCE PROJECTS

sb-siem-mcp - Wazuh AI Agent Python, FastMCP, Docker | MIT

- Model Context Protocol server exposing 28 tools across 9 security domains, letting LLM agents query Wazuh SIEM, correlate events, audit compliance and trigger incident response. Tested against live Wazuh 4.14.5 instances.
- Defence in depth: input validation with shell-metacharacter blocking, token-bucket rate limiting, credential redaction on all model-bound output, append-only JSONL audit log, two-step confirmation gate on destructive tools, and RBAC across four roles.
- Operational surface: 7 Prometheus metrics, OpenAPI 3.0 spec with Swagger UI, CI test matrix, and Dependabot / pip-audit / CodeQL scanning on every push.

OT Sentinel - ICS/OT Detection Rules Wazuh XML, Sigma, Python | Apache 2.0

- 29 detection rules for Modbus, DNP3, IEC 104, MQTT and OPC-UA, shipped in both Wazuh XML and SIEM-agnostic Sigma, mapped to 7 MITRE ATT&CK for ICS techniques.
- All 29 validated via wazuh-logtest on Wazuh 4.14.5; the 8 Modbus rules additionally hardware-tested end to end against OpenPLC in a GNS3 lab with pymodbus attack scripts.
- Addresses a real gap: major SIEM platforms ship no OT protocol coverage, and commercial alternatives start around \$50K per site.

Wazuh NIST CSF 2.0 Rule Pack Wazuh XML, Python | Apache 2.0

- 50 detection rules carrying their NIST CSF 2.0 subcategory and MITRE ATT&CK technique inside the alert JSON, so compliance evidence is produced by detection rather than reconstructed from spreadsheets afterwards.
- Automated evidence harness with a trigger and benign log corpus per rule: 57 PASS, 0 FAIL across Ubuntu 22.04 and Windows Server 2022, via Sysmon, auditd, syslog and iptables.
- One rule per file with no batch dependencies, organised by primary NIST function.

SKILLS

Security	Wazuh SIEM/XDR, detection engineering, MITRE ATT&CK and ATT&CK for ICS, NIST CSF 2.0, Sigma, Sysmon, auditd, threat hunting, incident response
OT / ICS	Modbus, DNP3, IEC 104, MQTT, OPC-UA, OpenPLC, GNS3, digital twins
Infrastructure	Kubernetes (RKE2), Terraform, Ansible, libvirt/KVM, Docker, CloudNativePG, Strimzi Kafka, MinIO, Longhorn, cert-manager, Prometheus
Languages	Python, TypeScript, Bash, Rust (reading and debugging), gRPC, aiohttp, FastMCP