Infrastructure Security Using Linux

Computer science / Cybersecurity

SIEM & Firewall

Wazuh - Open Source XDR.
Open Source SIEM.

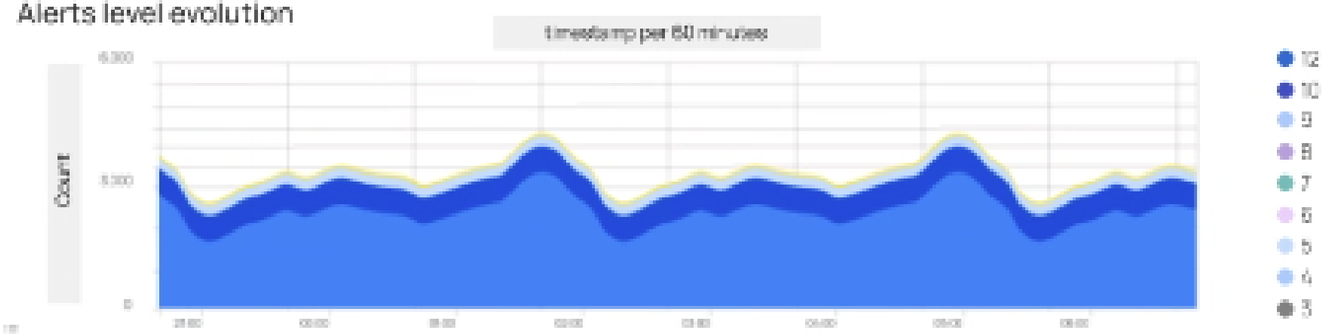
Threat Hunting

Dashboard | Events

Search | Jan-Feb | 2024 | Explore agent | Generate report

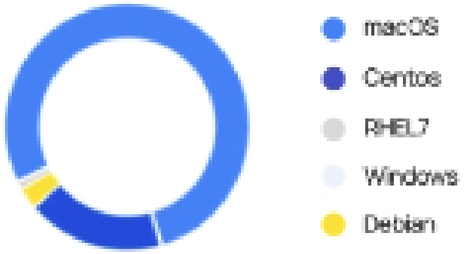
Total	Level 12 or above alerts	Authentication failure	Authentication success
178243	5	33624	58

Alerts level evolution

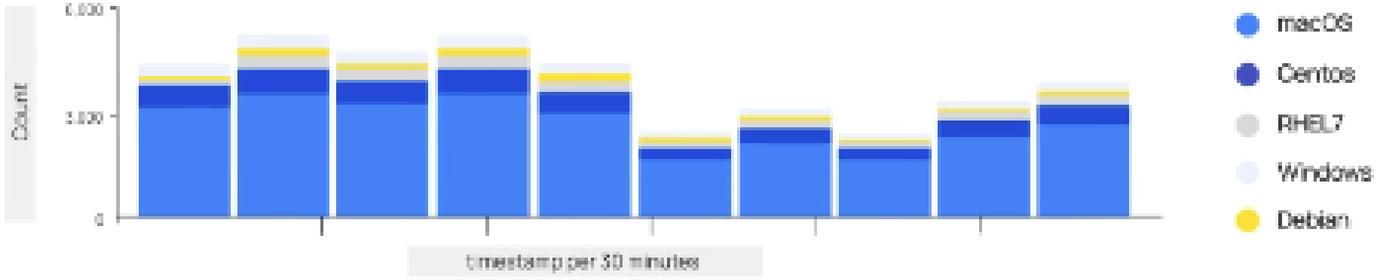


MITRE ATT&CK

Top 5 agents



Alerts evolution - Top 5 agents



Security alerts

Time	Agent	Agent name	Technique(s)	Tactic(s)	Description	Level	Rule ID
> Jan 22, 2024 @ 09:55:20.518	004	Windows	T1218	Defense Evasion	Signed Script Proxy Execution: C:\Windows...	10	255563

Introduction to Wazuh

- Open-source XDR & SIEM platform
- Unified security monitoring: logs, metrics, alerts
- Host-based agents for Linux, Windows, macOS
- Real-time threat detection & response

Core Architecture

- **Agents:** collect system events & send to Manager
- **Manager:** analysis engine, rule evaluation, alert generation
- **Elasticsearch:** scalable data store
- **Kibana:** visualization & dashboards
- **Wazuh API:** automation & integration

XDR Capabilities

- Endpoint visibility across your environment
- Behavior-based anomaly detection
- Active response: automated remediation scripts
- Malware & rootkit detection
- Threat intelligence feeds integration

SIEM Features

- Centralized log collection & normalization
- Correlation rules for multi-source analysis
- Prebuilt compliance reports (PCI-DSS, GDPR, HIPAA)
- Customizable dashboards & alerts
- Historical search & forensic analysis

Deployment Models

- **On-Premises:** full control over data & infrastructure
- **Hybrid:** use cloud storage with local processing
- **Cloud-Native (Elastic Cloud):** managed Elasticsearch & Kibana
- **Docker/Kubernetes:** containerized, easy scaling

Scalability & Performance

- Distributed Manager clusters for high availability
- Elasticsearch sharding for large-scale indexing
- Agent grouping to balance load
- Monitoring metrics: CPU, memory, I/O dashboards

Common Use Cases

- Threat hunting & incident investigation
- Compliance auditing & reporting
- Vulnerability detection & patch validation
- Insider threat monitoring
- Cloud workload protection

Integrations & Extensions

- Cloud providers: AWS, Azure, GCP logs
- Network devices: firewalls, proxies, routers
- DevOps pipelines: GitHub Actions, Jenkins alerts
- SOAR platforms: TheHive, Cortex XSOAR
- Custom scripts via Wazuh API

Community & Support

- Active GitHub repository & issue tracker
- Community Slack & mailing lists
- Official documentation & tutorials
- Commercial support from Wazuh Inc.
- Regular security content & rule updates

Next Steps & Best Practices

- Start with pilot: deploy agents on critical hosts
- Tune rules: minimize false positives
- Automate responses for common threats
- Schedule regular health checks & upgrades
- Engage with community for advanced use cases

OPNsense®

An open source, firewall and routing platform

What Is OPNsense®?

- Open-source firewall & routing platform
- Built on HardenedBSD for security & stability
- Intuitive web interface for management
- Regular releases with cutting-edge features

Core Architecture

- HardenedBSD base OS with minimal attack surface
- Modular design: decoupled services & plugins
- Web GUI backed by PHP/FreeBSD middleware
- REST API for automation & orchestration

Firewall Capabilities

- Stateful packet inspection with aliases & GeoIP
- Layer-7 filtering via Suricata IDS/IPS integration
- Traffic shaping & quality-of-service controls
- NAT (static, dynamic, 1:1, outbound)

Routing & Networking

- OSPF, BGP, RIP dynamic routing protocols
- Multi-WAN support with failover & load-balancing
- VLAN tagging and bridging
- DHCP server, relay, and DNS forwarding

VPN & Remote Access

- IPSec site-to-site & road-warrior tunnels
- OpenVPN with easy-to-use certificate management
- SSL VPN for clientless access
- WireGuard support for lightweight connectivity

High Availability & Performance

- CARP virtual IPs for gateway redundancy
- Stateful sync of connection tables & config
- Hardware offload for IPsec & NAT acceleration
- Scalability via clustered setups

Plugins & Extensibility

- Extensible via OPNsense Plugin System
- Popular plugins: Proxy (Squid), Webfilter (SquidGuard), Reporting (ntopng)
- Custom plugin development through API hooks
- Continuous updates from official & community repos

Security & Analytics

- Integrated IDS/IPS with Suricata rulesets
- Real-time log analysis and alerting
- Dashboard widgets for traffic, alerts, health
- Long-term reporting with Elastic stack integration

Deployment & Management

- ISO installer for physical & virtual environments
- Inline backup/restore of full configuration
- Role-based user accounts & two-factor authentication
- CLI tools for scripting and headless setups

Community & Roadmap

- Active GitHub repository & pull-request model
- Regular feature releases every six months
- Community forum, mailing list, and annual conferences
- Future roadmap: enhanced cloud integration, AI-driven threat prevention