PT FPT METRODATA INDONESIA

Pratical Cybersecurity with SecBox Pro

Frequency of Preventable Incidents

2/3

of security leaders said they have experienced an incident that could have been prevented if security operations were improved

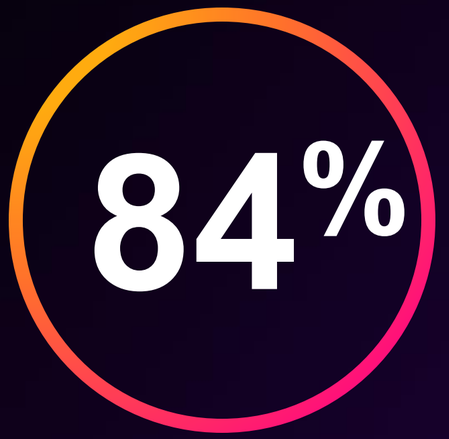
Digital Resilience
a Catalyst for SecOps Teams

90%

of CISOs say Digital Resilience factors into their organization’s SecOps strategies more than it did 12 months ago.

Driving SOC modernization

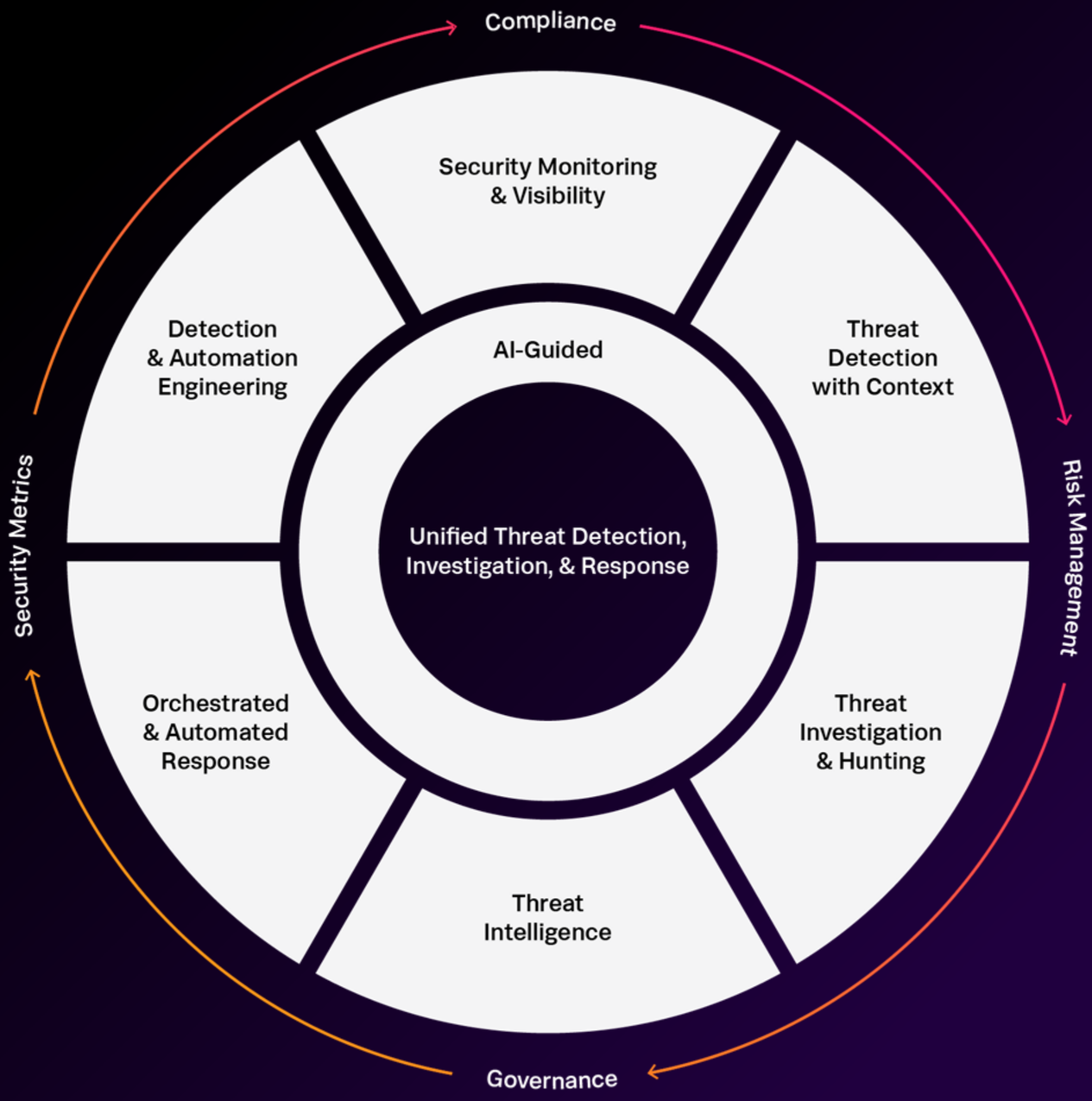
across detection, investigation, and response as a top priority to achieve **digital resilience**.



of organizations claim improving efficacy and efficiency of SecOps is a top 5 priority.

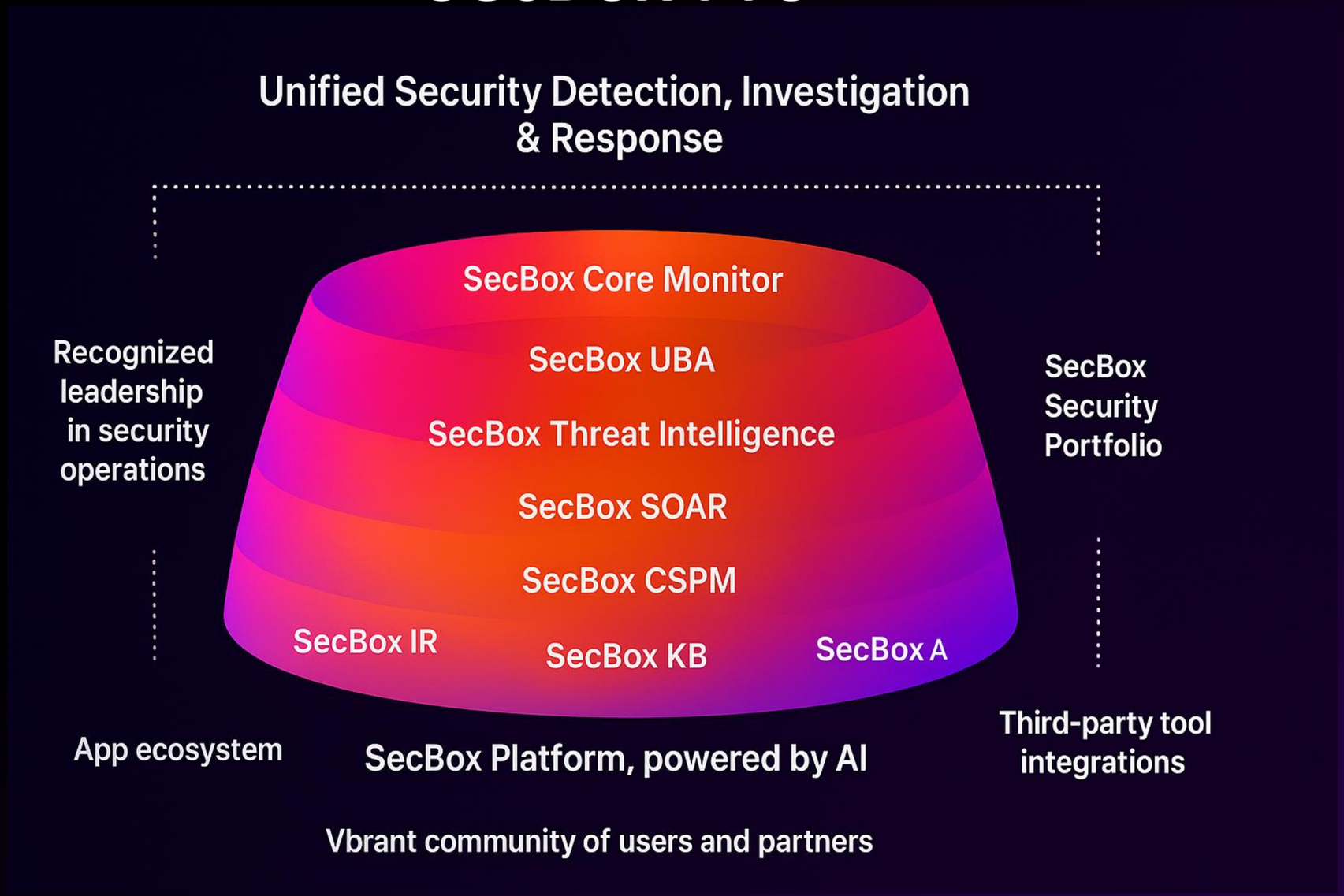
The SOC of the Future

Unified Threat Detection, Investigation and Response at the Core.



SecBox Security Portfolio

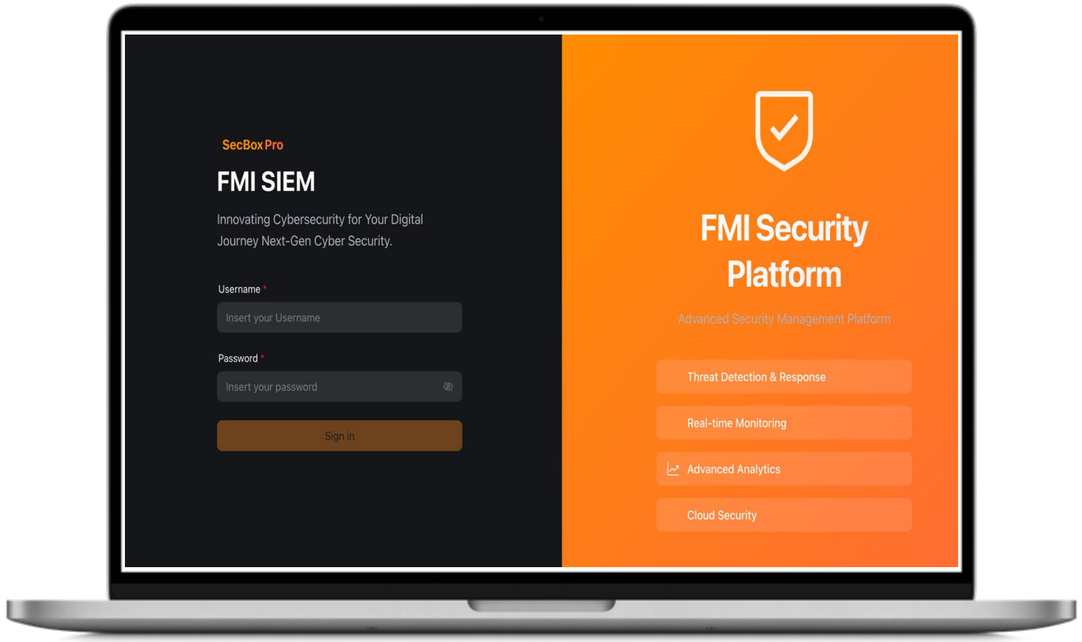
SecBox Pro


Unified Security Detection, Investigation & Response
Recognized leadership in security operations
SecBox Core Monitor
SecBox UBA
SecBox Threat Intelligence
SecBox SOAR
SecBox CSPM
SecBox IR
SecBox KB
SecBox A
SecBox Security Portfolio
App ecosystem
SecBox Platform, powered by AI
Third-party tool integrations
Vbrant community of users and partners

SecBox Core Monitor

SecBox Core Module

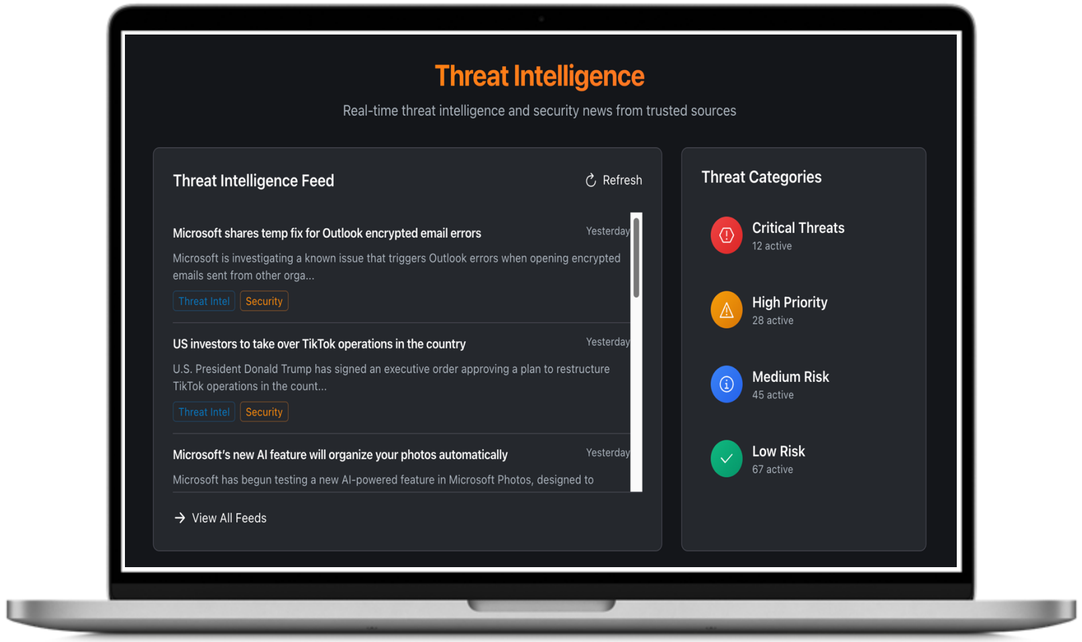
- **Gain unified visibility** combining Wazuh SIEM/XDR and Graylog log analytics.
- **Investigate faster** with powerful dashboards, search, and visualization.
- **Reduce false positives** through smart correlation and contextual rules.
- **Detect anomalies & threats** in real-time with AI-driven detection and **Vul Assessment.**
- **Optimize SOC operations** with a single, efficient monitoring surface, **compliance**.



SecBox Threat Intelligence

Turn global threat data into actionable intelligence for faster, smarter defense.

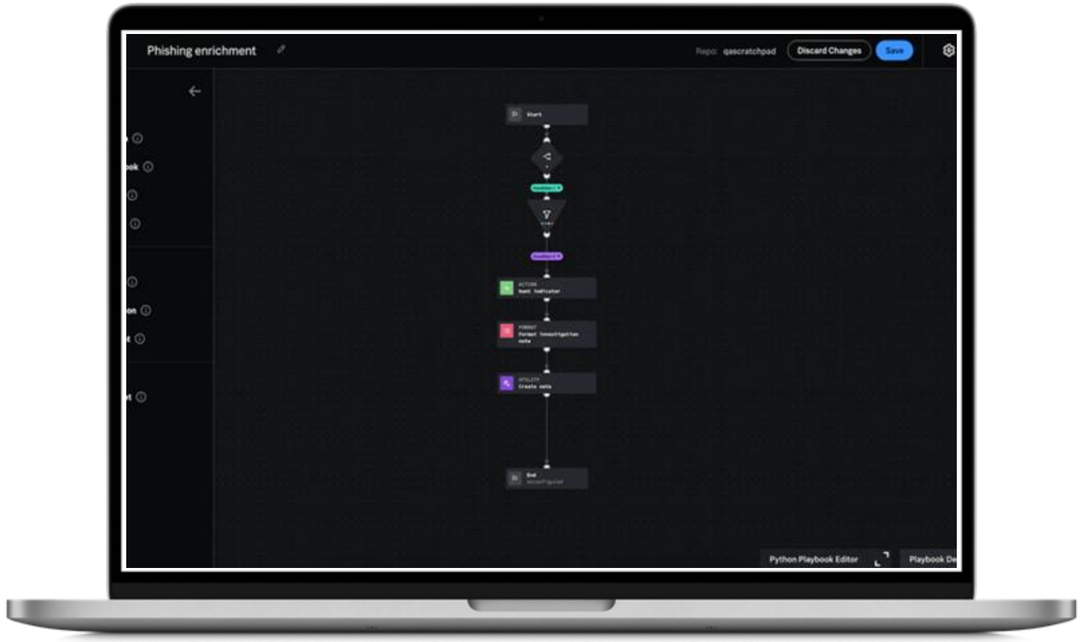
- **Centralize threat feeds** from global and local sources.
- **Enrich alerts** with real-time IOC, TTPs, and attacker profiling.
- **Prioritize with context** to focus on high-risk threats.
- **Accelerate investigations** with automated enrichment workflows.
- **Continuously updated** intelligence to stay ahead of emerging attacks.



SecBox SOAR

Work smarter by automating repetitive tasks, respond to security incidents in seconds, and increase analyst productivity.

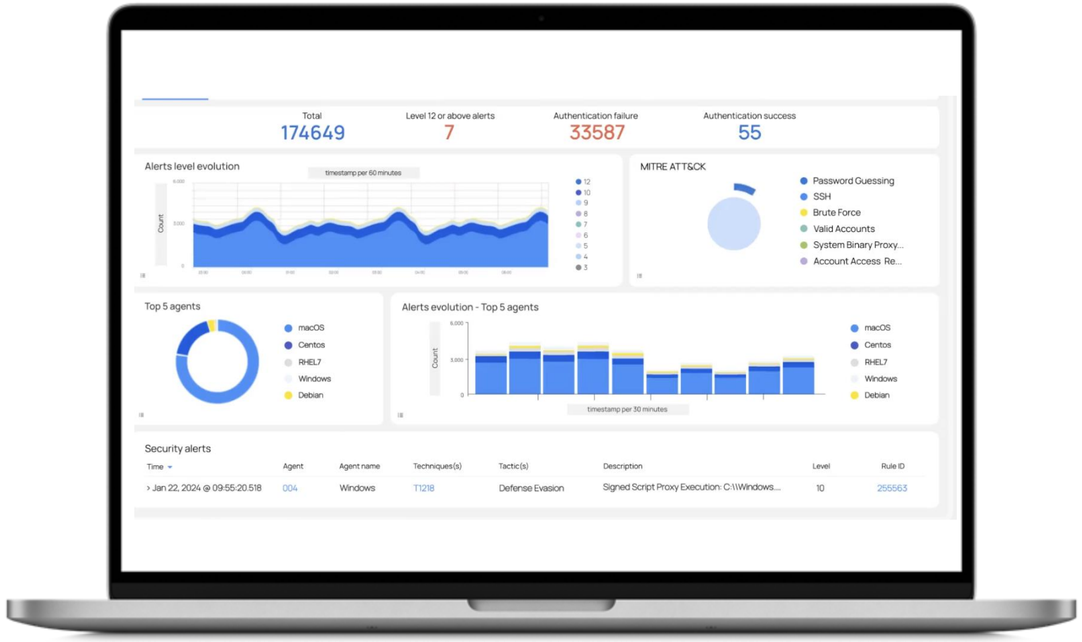
- **Enhance team productivity** with automation for speed and efficiency.
- **Take prioritized actions** to act on the most pressing threats.
- **Respond with threat context** for common threats automatically.
- **Automate with ease** using pre-built playbooks, integrations, or build customized playbooks.
- **Get more out of your security stack** by orchestrating workflows across teams and tools.
- **Foster collaborative investigations** for a cohesive investigative process.
- **Actionize your data** by integrating SOAR with SecBox Core



SecBox User Behavior

Detect unknown threat and anomalous behavior using machine learning.

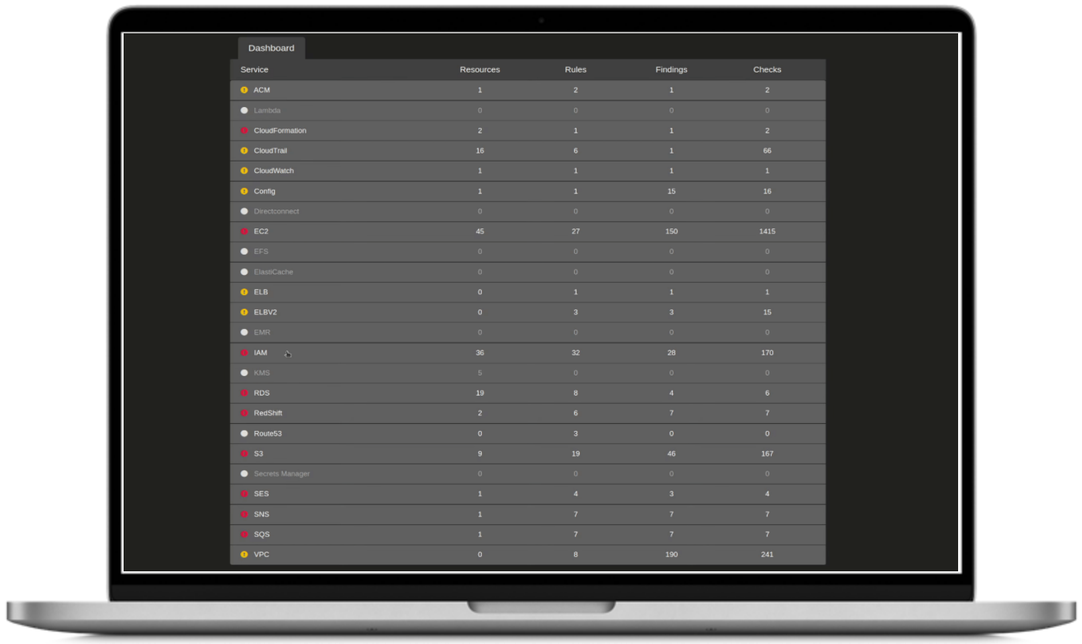
- **Enhance visibility and threat detection** with multi-entity profiling, unsupervised ML, and multidimensional identity correlation.
- **Accelerate threat detection** using ML modeling correlating anomalies into high fidelity threats.
- **Speed up investigations** using visual threat correlations and analytics.
- **Stay current** with continuous UBA content updates
- **Gain additional threat context** by easily integrating with SecBox Core



SecBox CSPM

Secure your cloud, continuously and intelligently.

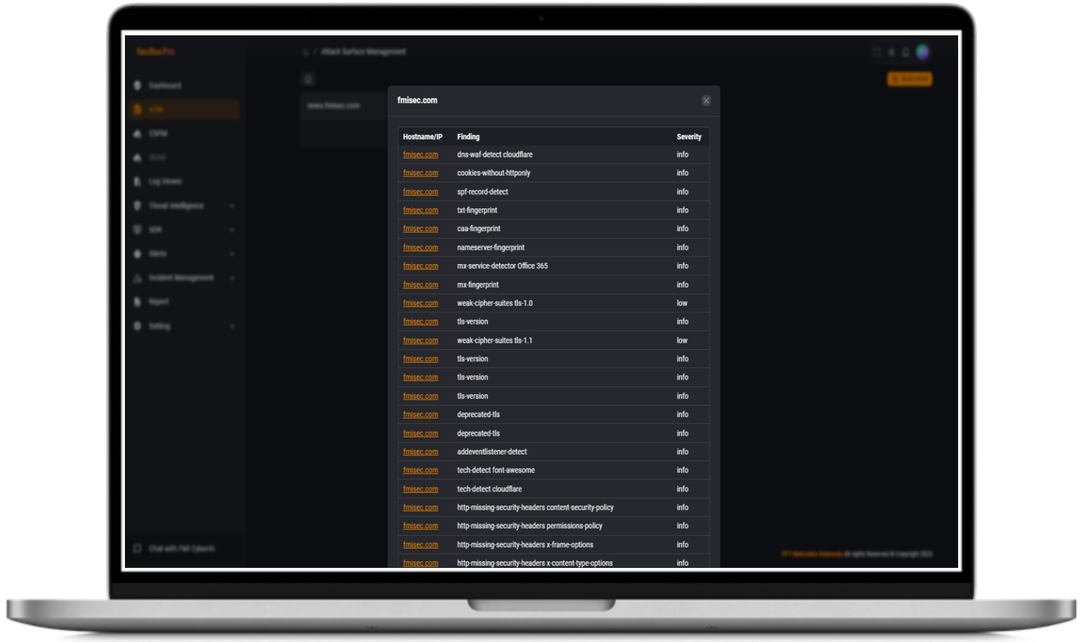
- **Gain cloud-wide visibility** across multi-cloud environments.
- **Detect misconfigurations** and compliance violations in real time.
- **Prioritize cloud risks** with context-driven insights.
- **Automate remediation** to reduce human error and response time.
- **Ensure continuous compliance** with industry standards and policies.



SecBox Attack Surface Management

See what attackers see — and fix it first.

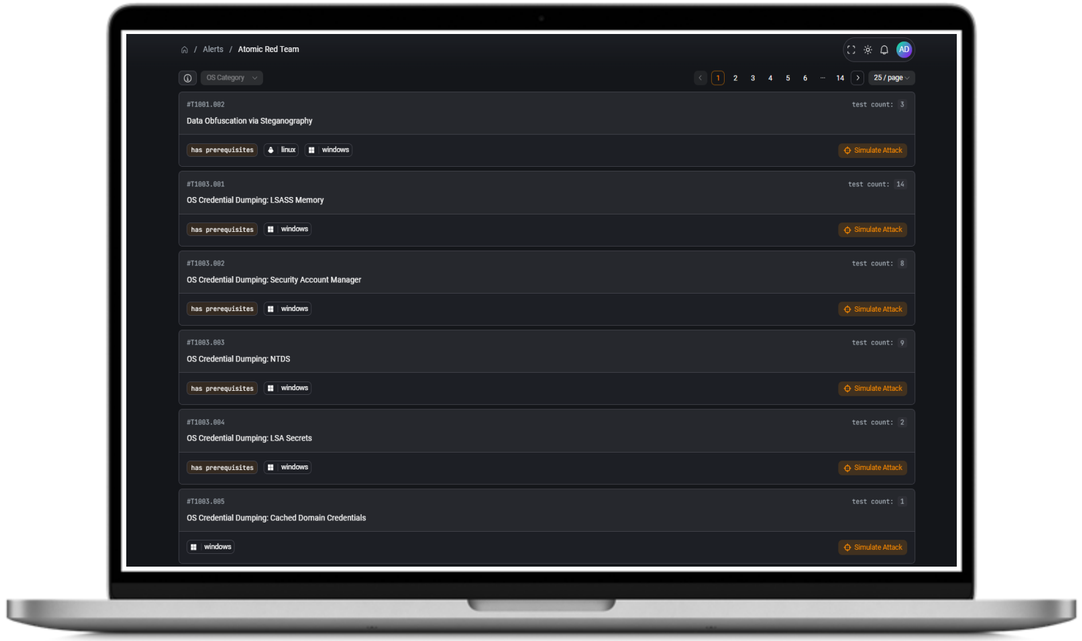
- **Continuously discover** internet-facing assets and shadow IT.
- **Map your attack surface** with real-time visibility.
- **Identify exposures** like misconfigurations and open ports.
- **Prioritize critical risks** before attackers exploit them.
- **Integrate with SOC** for proactive defense.



SecBox Attack Simulation

Train your defenses with real attacks — safely and continuously

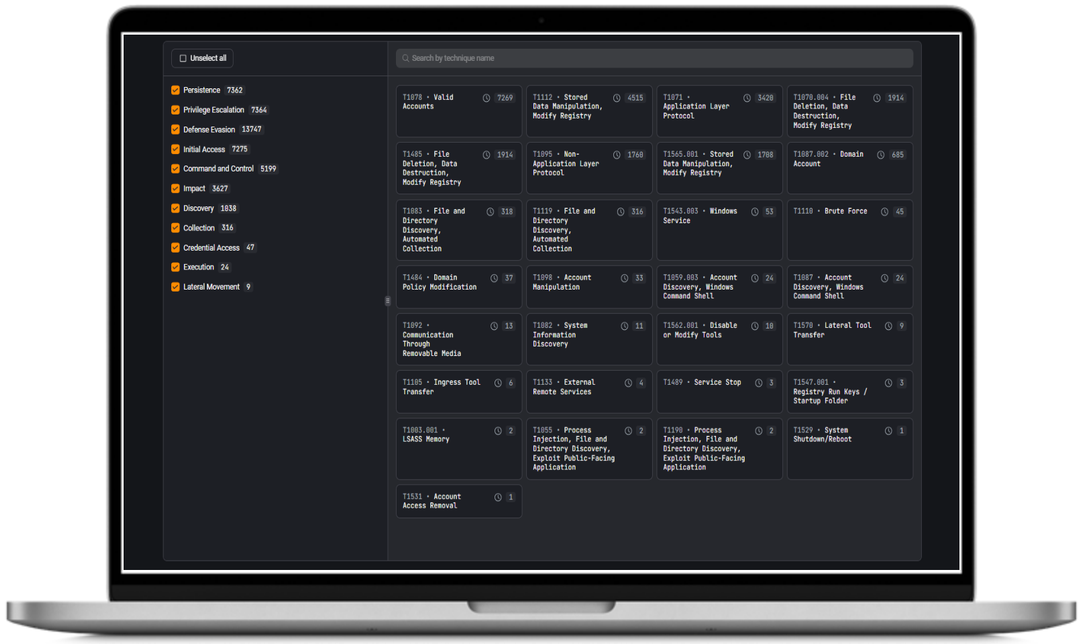
- **Simulate real-world attacks** across networks, endpoints, and cloud.
- **Test defenses proactively** to measure SOC readiness.
- **Uncover gaps** in detection, response, and configurations.
- **Enhance resilience** through continuous red team automation.
- **Validate controls** against latest TTPs and frameworks.



SecBox Knowledgebase

Turn knowledge into action for faster, smarter security operations.

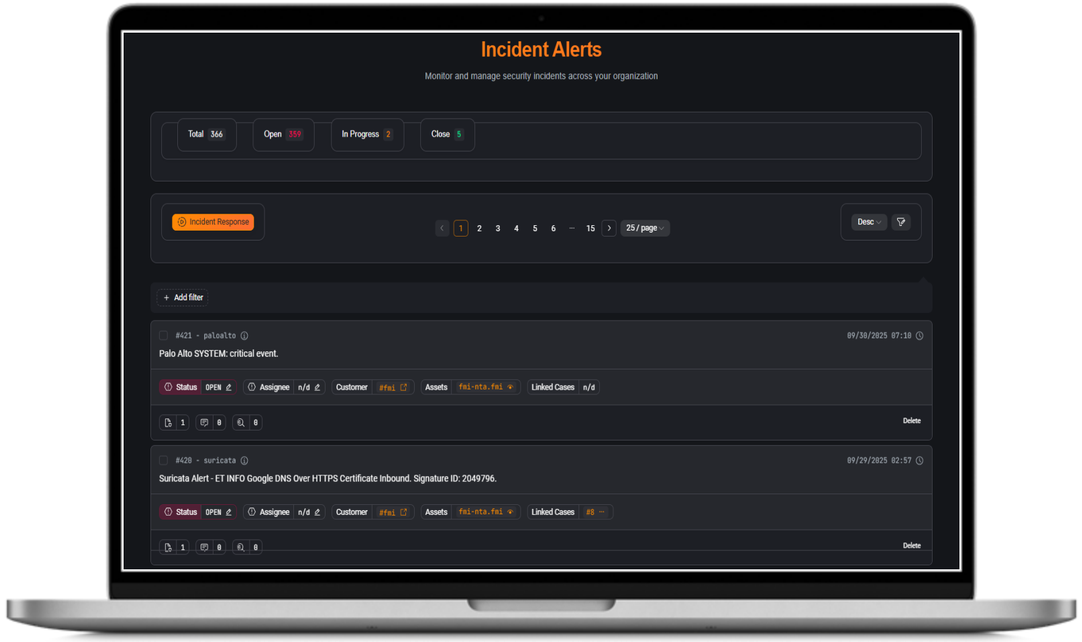
- **Centralize security knowledge** into one unified repository.
- **Leverage playbooks, IOCs, and best practices** for faster response.
- **Enable collaboration** across SOC, IR, and threat hunting teams.
- **Continuously updated** with latest threats and defense tactics.
- **Accelerate learning & decision-making** with contextual insights.



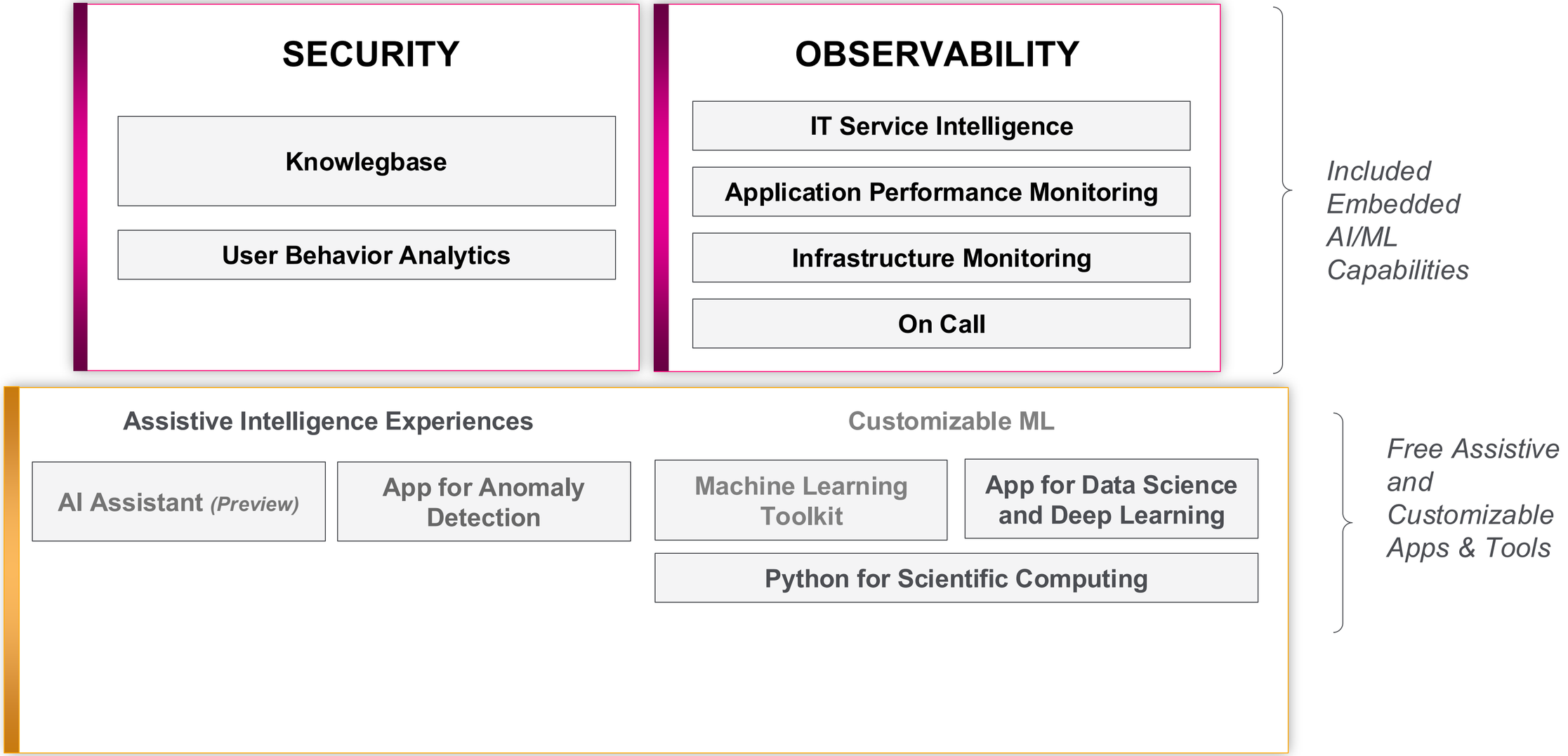
SecBox IR

Respond smarter, track better, resolve faster.

- **Centralize incident response** with structured workflows.
- **Automate case creation & tracking** from detection to resolution.
- **Collaborate across teams** with role-based access and evidence sharing.
- **Prioritize incidents** using risk and business impact.
- **Integrate with SOAR & KB** for faster investigation and closure.



SecBox AI


SECURITY
Knowlegbase
User Behavior Analytics
OBSERVABILITY
IT Service Intelligence
Application Performance Monitoring
Infrastructure Monitoring
On Call
Included Embedded AI/ML Capabilities
Assistive Intelligence Experiences
AI Assistant (Preview)
App for Anomaly Detection
Customizable ML
Machine Learning Toolkit
App for Data Science and Deep Learning
Python for Scientific Computing
Free Assistive and Customizable Apps & Tools

Security Expertise

Security content and research to help you stay ahead of threats

- **Rapid response to empower blue teams** with the latest insights for high-profile security incidents.
- **Security research** with actionable guidance and recommendations.
- **Verified research and content** in the form of detection searches, use cases, and playbooks.
- **Powerful threat research tools** to test your detection searches against cyber attacks.

Our critical security innovation areas

Unified TDIR with automated workflows

Continue to make products integrated for a seamless analyst experience to drive down MTTD and MTTI resulting in a strong security posture.

World-Class detections

Expand delivery of “ready-to-use”detections to effectively cover the expanding threat landscape with timely delivery of detections for emerging threats.

Insider threat, risk and compliance

Build new capabilities to effectively protect against insider threats and provide solutions to better identify risk and manage compliance.

Federation

Provide the best analytics and insights into data no matter where the data is stored.

AI-guided workflows

Integrate AI into TDRI workflows to help accelerate investigations helping analysts to make faster and better decisions.

Why SecBox?

Power the SOC of the Future with SecBox: fast, unified, and tailored

Deploy Fast & Light.

Rapid, lightweight deployment with minimal overhead.

Bundle of Solutions.

One integrated platform combining monitoring, SOAR, UBA, CSPM, ASM, IR, and mor

Tailored for You.

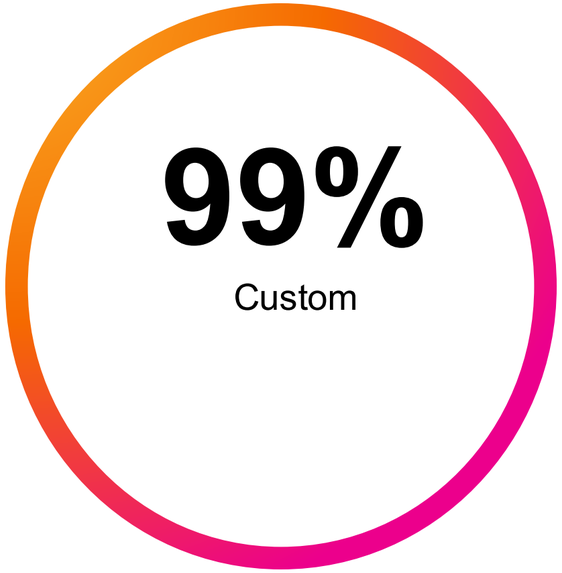
Flexible architecture customized to each customer’s needs and environment.

Criteria	SecBox Pro (FMI)	Splunk Enterprise Security (ES)	IBM QRadar	Wazuh
Purpose / Scope	Includes all Wazuh features + enterprise functions: AI integration, Incident Response, Threat Intel IOC, Case Mgmt, Web/Cloud Scan, SOAR automation, multi-customer support.	Advanced analytics-driven SIEM: log management, UEBA, threat detection, compliance monitoring, SOAR integration, ML-based anomaly detection.	SIEM with strong threat detection, compliance, correlation, and advanced offense management. Widely used in large enterprises & government.	Open-source SIEM & XDR: log collection, EDR, vulnerability detection, compliance monitoring, cloud & container security.
Threat Intelligence	Wazuh + FMI Threat Feed, IOC/TTP enrichment, correlation.	Integrated threat intelligence framework + Splunk Enterprise Security App. Supports premium threat feeds.	IBM X-Force Threat Intelligence, built-in feeds, strong enrichment.	Not available by default, complex to configure.
Rules Management	All default Wazuh rules + Custom FMI rules + proprietary rules.	Correlation searches, machine learning models, Splunk's Adaptive Response actions.	Out-of-box rules + customizable correlation, with strong offense prioritization.	Default rules & decoders, customizable. Many false positives.
Case Management	Full case management: ticket, workflow, incident→case→report.	Integrated with Splunk SOAR, case mgmt & automation workflows.	Built-in case management with incident lifecycle, AQL queries for root cause.	Not included; only alerts & response.
AI & Automation / SOAR	Advanced automation via SOAR opensource+ AI-based SOC chatbot, analysis, active respons	Strong SOAR : playbooks, automation, ML-driven detection.	Native SOAR + integrations. Playbooks, automated remediation.	Basic active response (block IP, quarantine host), integrate with SOAR opensource
Scanning	Wazuh scanning + Web/Cloud Scan (OWASP, compliance, misconfig).	Vulnerability scans via Splunk integrations (Tenable, Qualys, etc.).	Built-in vuln scanning + strong asset profiling.	vuln detection, container/endpoint monitoring.
Reporting	Wazuh reports + auto IR reports, export to PDF/Excel.	Rich reporting, dashboards, compliance kits, KPI tracking.	Detailed compliance & audit reports, strong for regulated industries.	Compliance dashboards (PCI, HIPAA, GDPR, NIST).
Commercial Model / Cost	Sold as Service: VSOC, deployment, ops, support.	License cost based on ingested data/day (very expensive at scale).	License based on events per second (EPS), storage – also expensive.	Free community edition, Wazuh Cloud subscription.
Scalability & Performance	Optimized FMI model, multi-customer, cloud-native scaling.	Very scalable (petabyte log ingestion), best for large enterprises.	Scales well for EPS-heavy environments, proven in Fortune 500/government.	Scales with effort, needs tuning for large envs.
Availability of Third-Party Integration	Integrates with FMI ecosystem + APIs, FMI support	Very strong ecosystem: Splunkbase marketplace (>1,000 apps).	Strong vendor ecosystem: integrates with IBM stack, security tools, 3rd-party apps.	Limited, needs manual work.
Support & Community	Vendor support (FMI) + managed SOC services.	Enterprise-grade support + large global community + Splunkbase.	IBM enterprise support, partner ecosystem, but smaller community than Splunk.	Strong open-source community, but limited enterprise support.
Summary	Extended Wazuh with enterprise functions + managed service.	Best for large enterprises needing scalability, automation, analytics, but very high cost.	Trusted in large enterprises/government, strong compliance & detection, expensive but robust.	Open-source SIEM/EDR, cost-effective, high effort for enterprise.

Enabling powerful security outcomes for our customers

Deploy Fast & Light

Bundle of Solutions



Tailored for You

Delivering Economic Benefits

- **64% operational savings** for organizations that did not have a previous SIEM and SOAR solution.
- **38% operational savings** with organizations that had a previous SIEM and SOAR solution.
- **30% improvement** in security team's operational efficiency.
- **2-3 different products were consolidated** as part of adopting SecBox.
- **267% ROI** by adopting SecBox.