



AccuKnox SIEM

Export logs from ONE dashboard



Certified & Accredited by



As Featured In



Available On



Table of Contents

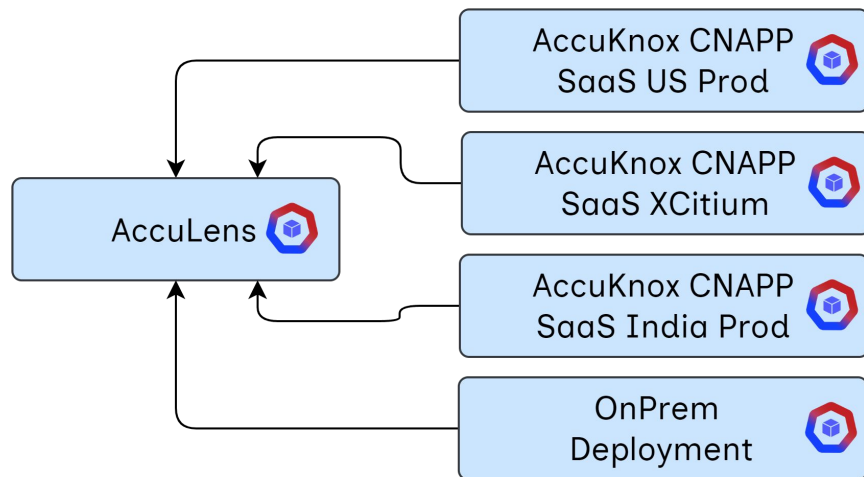


1	AccuKnox SIEM - Features
2	Architecture
3	AccuKnox SIEM Vision/Differentiation
4	How AccuKnox CNAPP benefits from AccuKnox SIEM?
5	NextGen SOC with AccuKnox SIEM, CNAPP, and GenAI
6	Data/Storage Handling
7	Integrations List

- Data/Logs Ingestion
 - Extensive Integrations/Log Types support
 - Out of the box Integrations
- Threat Analysis
 - Multivector correlation support
 - Anomaly Detection
- Snapshots support
- Native CNAPP Integration with AccuKnox
- External Channel Integrations

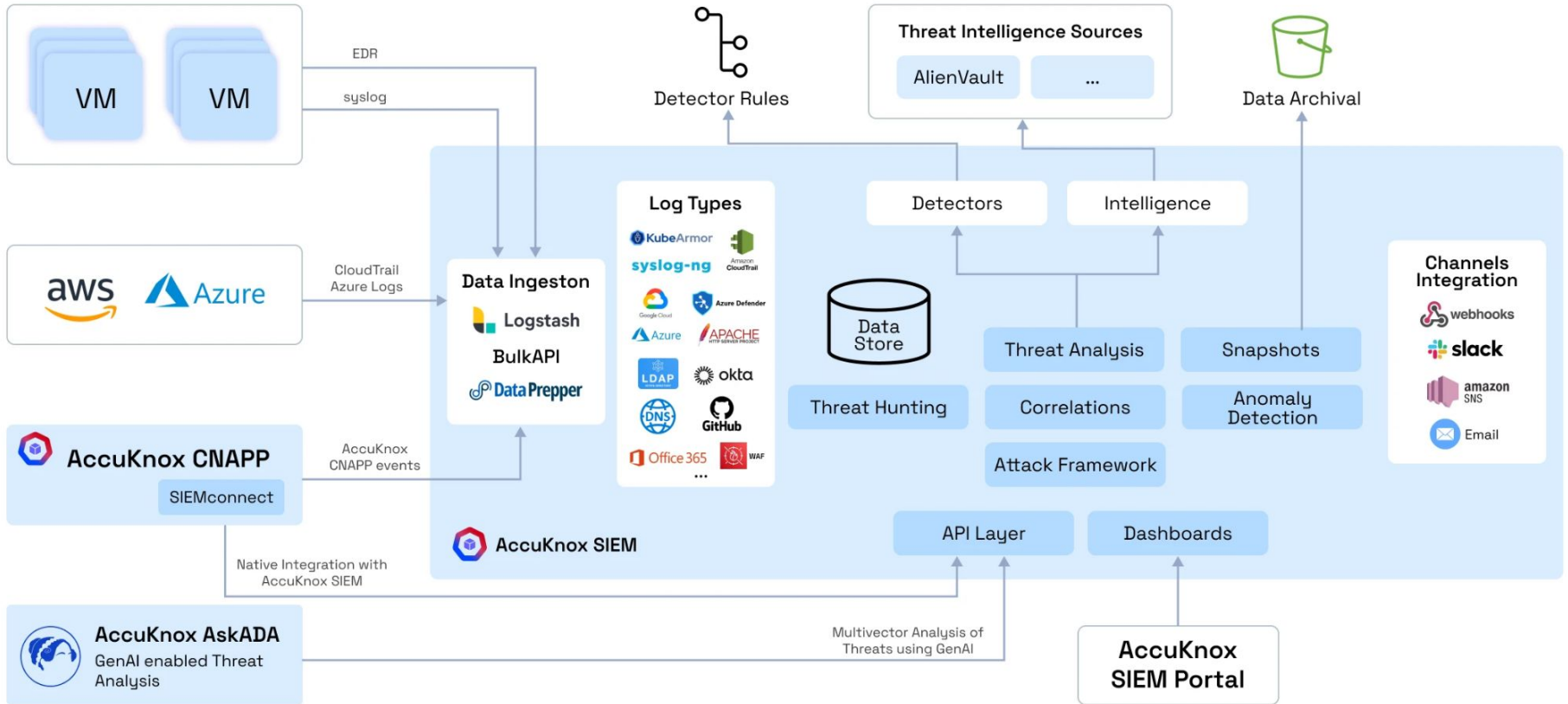
Data/Storage Handling

Index/Data Ingestion/Storage/Isolation



- AccuKnox SIEM is a separate SIEM product from AccuKnox
- AccuKnox SIEM will be available as SaaS solution
- All AccuKnox CNAPP deployments can leverage AccuKnox SIEM Integration
- Threat Analysis Alerts feeds will be available in AccuKnox CNAPP

Internal Architecture

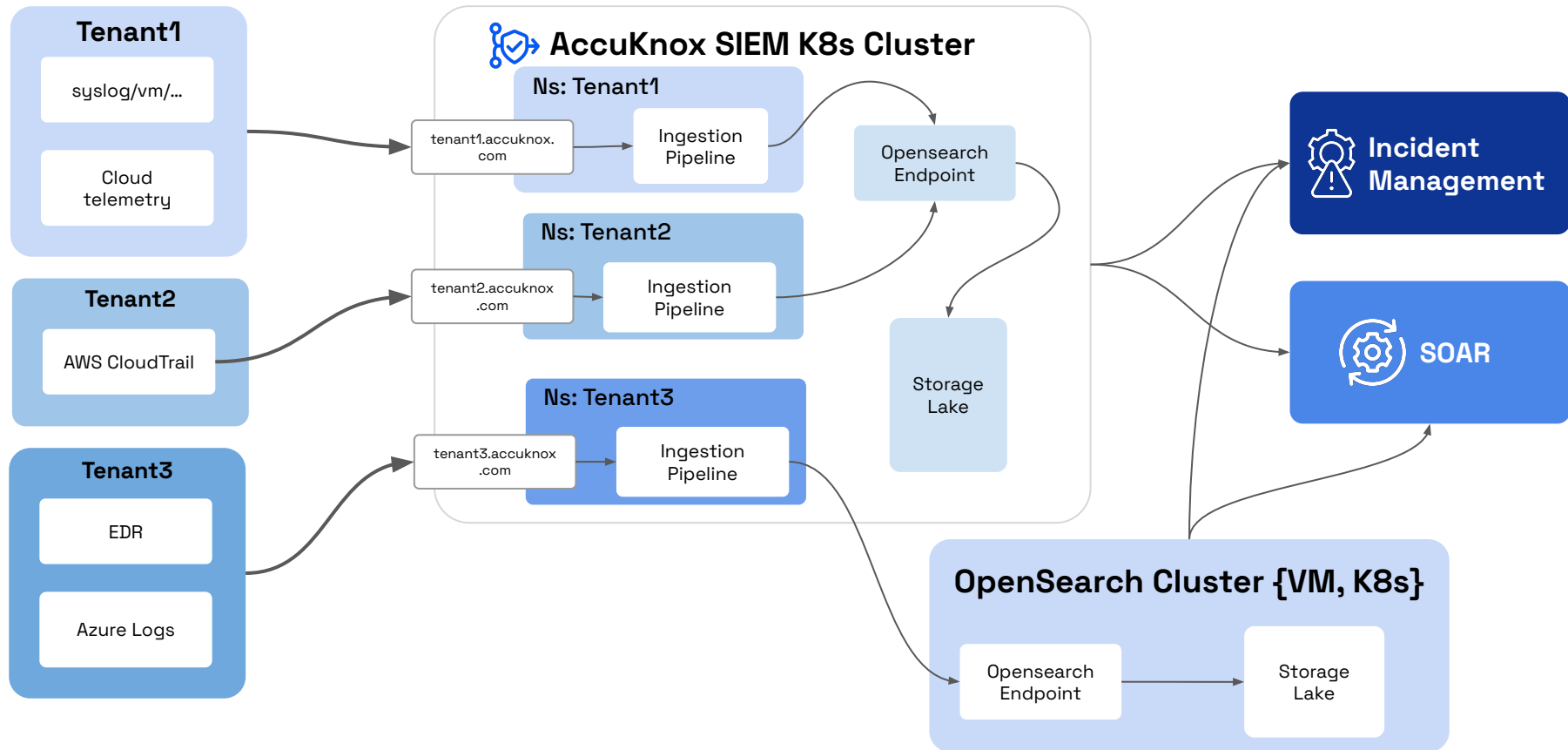


- Custom Rules/Detectors
 - Syslog, KubeArmor, EDR, CloudTrail, O365, ...
- Native Integration with CNAPP (AccuKnox)
- MITRE Attack Framework Integration
 - Container, Cloud, Endpoints
- NextGen SOC analysis with GenAI and SIEM+CNAPP sources
- NextGen OT Detection(??)
- Pricing
 - Low cost ingestion, storage, processors
 - Reduce SOC analysis cost

- AccuKnox CNAPP will have native integration with AccuKnox SIEM for SIEM integration
- Advanced Threat Analysis
 - AccuKnox Runtime solution will leverage AccuKnox SIEM for Threat Detection and Response
 - KubeArmor is supported as custom log type and AccuKnox provides custom rules/detectors based on KubeArmor
 - Integration with Threat Intelligence sources for suspicious IP detection.
- CIEM Integration (near future)
 - AccuKnox CNAPP can call AccuKnox SIEM APIs for CloudTrail, Azure Logs for access information

- AccuKnox CNAPP will have native integration with AccuKnox SIEM for SIEM integration
- AccuKnox AskADA leverages GenAI and feeds on Tenant specific data
- AccuKnox Agentic AI for SOC teams
 - Agent leveraging external threat intelligence connected with an agent leveraging customer findings sources.
- What do SOC teams get?
 - Faster ways to do threat analysis across Cloud and Endpoint assets
 - Leverage Asset Inventory in AccuKnox CNAPP with Findings database
 - GenAI supported threat analysis leveraging publicly available intelligence sources

Ingestion@scale: Using Ingestion pipelines



- Supported Ingestion types
 - LogStash
 - Bulk API
 - Data Ingestors
 - Http, kafka, otel, s3, kinesis, dynamodb, documentdb, fluentd
- Support Ingestion at scale
 - 10000 events per second
- Support storage at scale
 - 100GB per day data

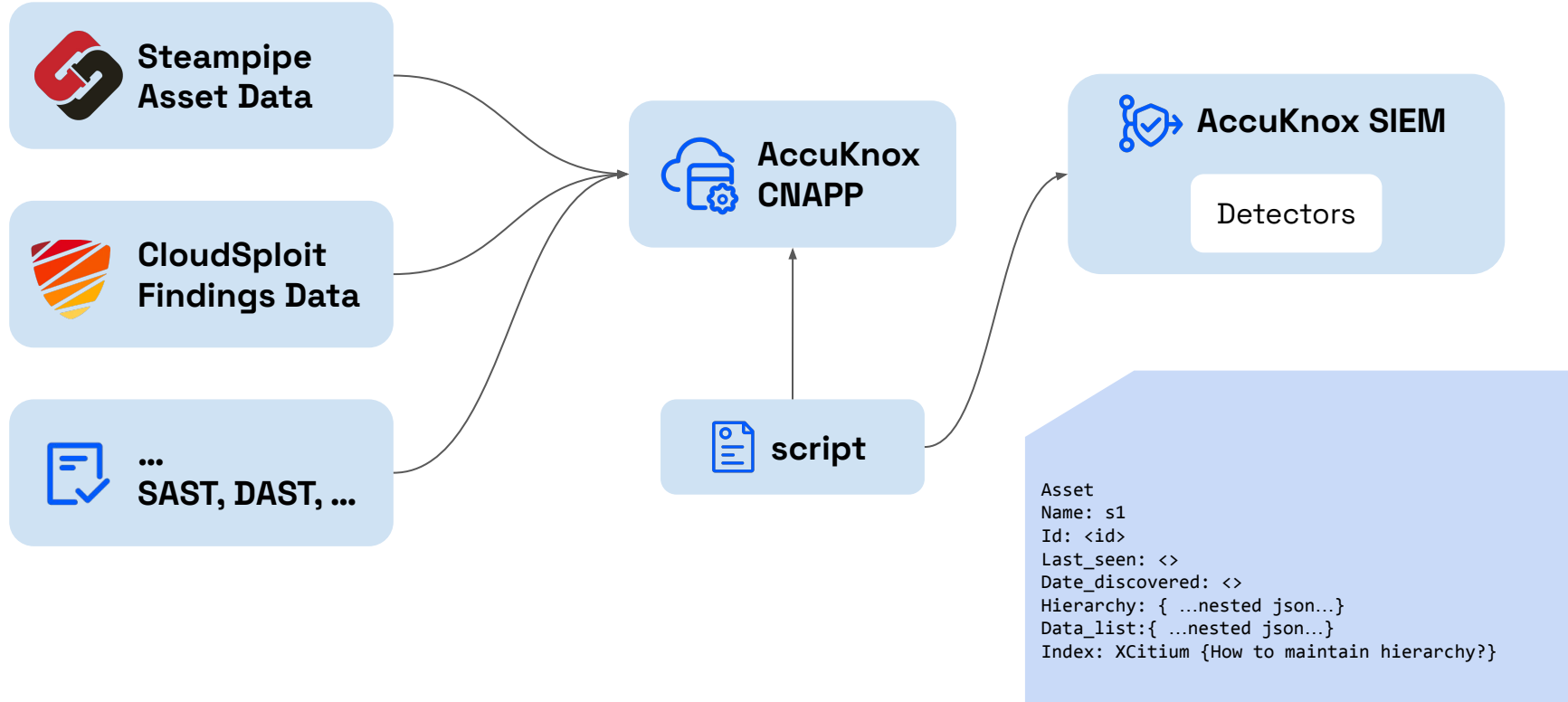
- Hard Data Isolation
 - Using separate instance of OpenSearch Cluster
 - The ingestion can still be handled by AccuKnox SIEM K8s Cluster
- Soft Data Isolation
 - Using separate indexes for different tenants across different envs
 - Index naming convention:
 - **Format:** {OPT-akenv}__{tenantname}__{tenantid}__{tool}__index
 - **Example:** akusprod__acmeinc__1324__syslog__index

- Limiting amount of data pumped in by the tenant
 - Controlling the ingestion
 - Controlling the upper limit of the indexes storage
- Data Retention
- Snapshots/Backup handling

Integrations List

- CSPs
 - AWS CloudTrail
 - Azure Logs
- Endpoints
 - Syslog
 - KubeArmor
 - MS Defender
 - Microsoft Windows
- Kubernetes
 - KubeArmor
 - K8s API Server Logs
- Identity
 - AD/LDAP
 - Okta
- MS 0365
- Github
- AccuKnox CNAPP
 - Cloud Findings

Integration: AccuKnox CNAPP



- Ingestion Pipeline
- Dashboards?

TODOs

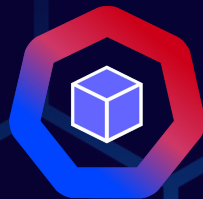
- Case/Incident Management [p1]
 - The Hive Project??
- Integrations list [p0]
 - Simplified onboarding (checkout AWS OpenSearch Onboarding)
 - Dashboards to be supported
- OT Telemetry/Alerts Integration
- Clear Pricing [p0]
- SOAR Integration [p1]
 - N8n open source, shuffler
- MITRE Attack Framework [p1]
- List the use-cases [p0]
- AI Enabled SIEM/SOC .. enlist the use-cases
- Competitive Analysis [p0]
 - StrikeReady, Reliaquest
- Threat Analysis [p0]
 - Correlation Rules
- CIEM Integration [p2]
- 5G SIEM/SOC [p2]
- Edge/IoT SIEM/SOC [p2]

Risks?

- SOAR Integration
- Incident/Case Management Integration

Milestone 1

- Hosted AccuKnox SIEM with AccuKnox Branding
 - Integrations supported
 - Ssh syslog, Cloudtrail, KubeArmor, AccuKnox CNAPP
 - Threat Intelligence
 - Per tenant ingestion
 - Custom Detectors
 - Integration with AccuKnox CNAPP
- Use-cases
 - Suspicious IP detection {KubeArmor logs, syslogs}
 - How many S3 buckets are publicly exposed?



ACCUKNOX

SEE US IN ACTION

support@accuknox.com

Certified by

