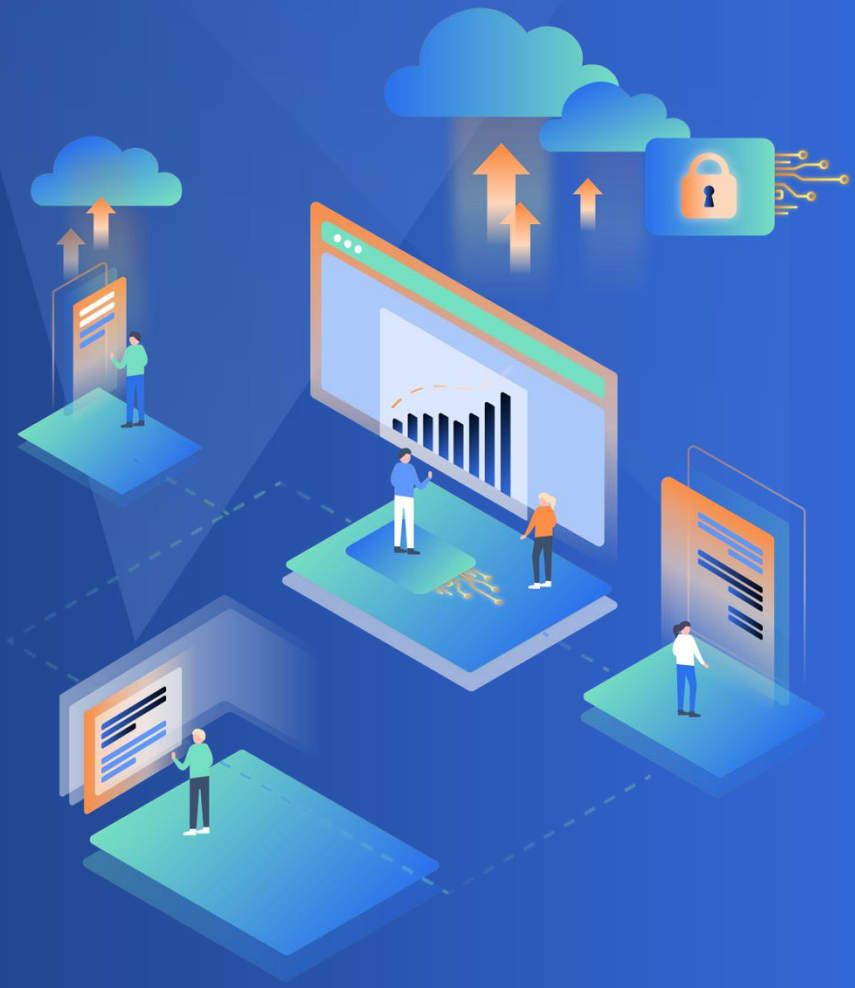
Från AD-auditing till komplett SIEM





Erik Tjärnkvist

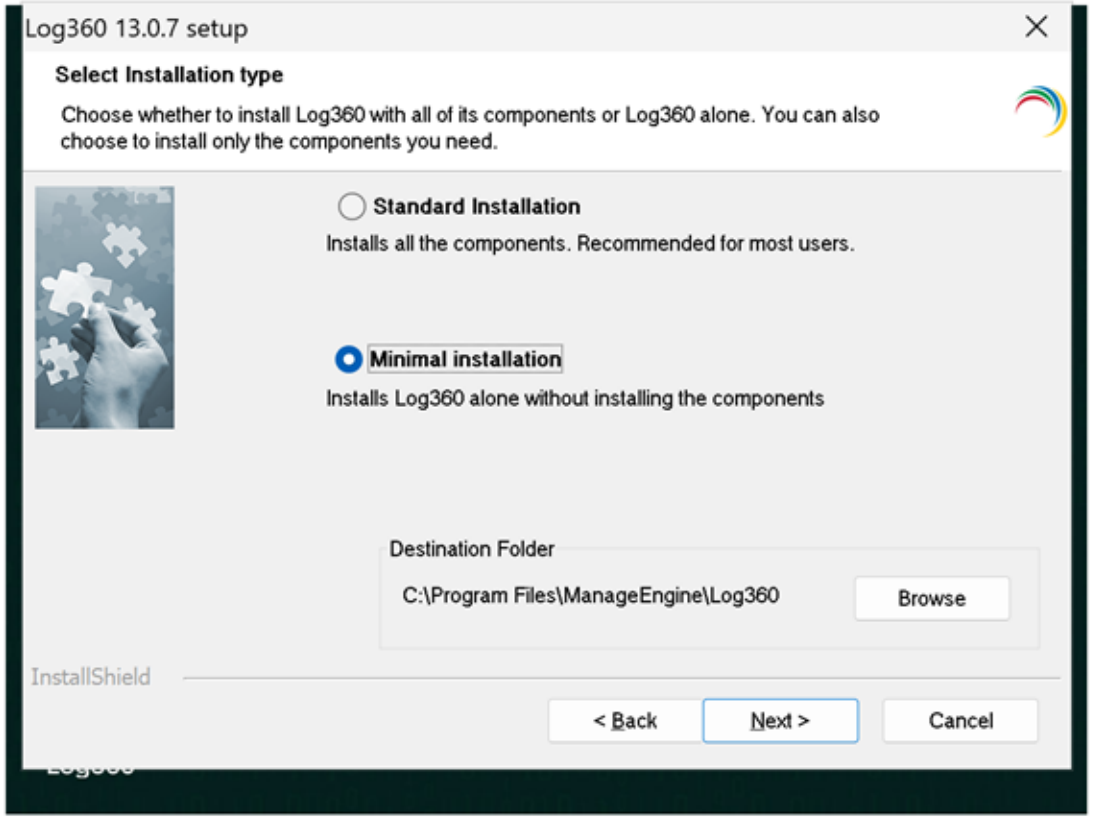
Product Manager

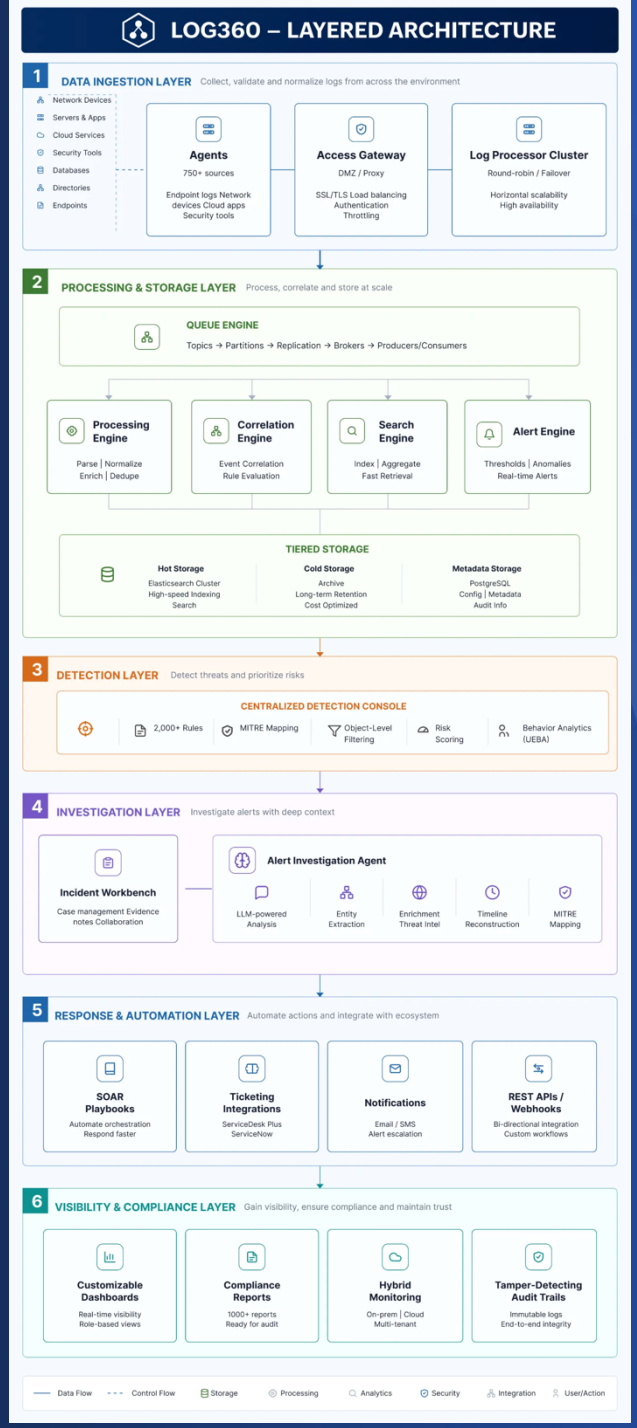
+46 (0)70 256 00 38

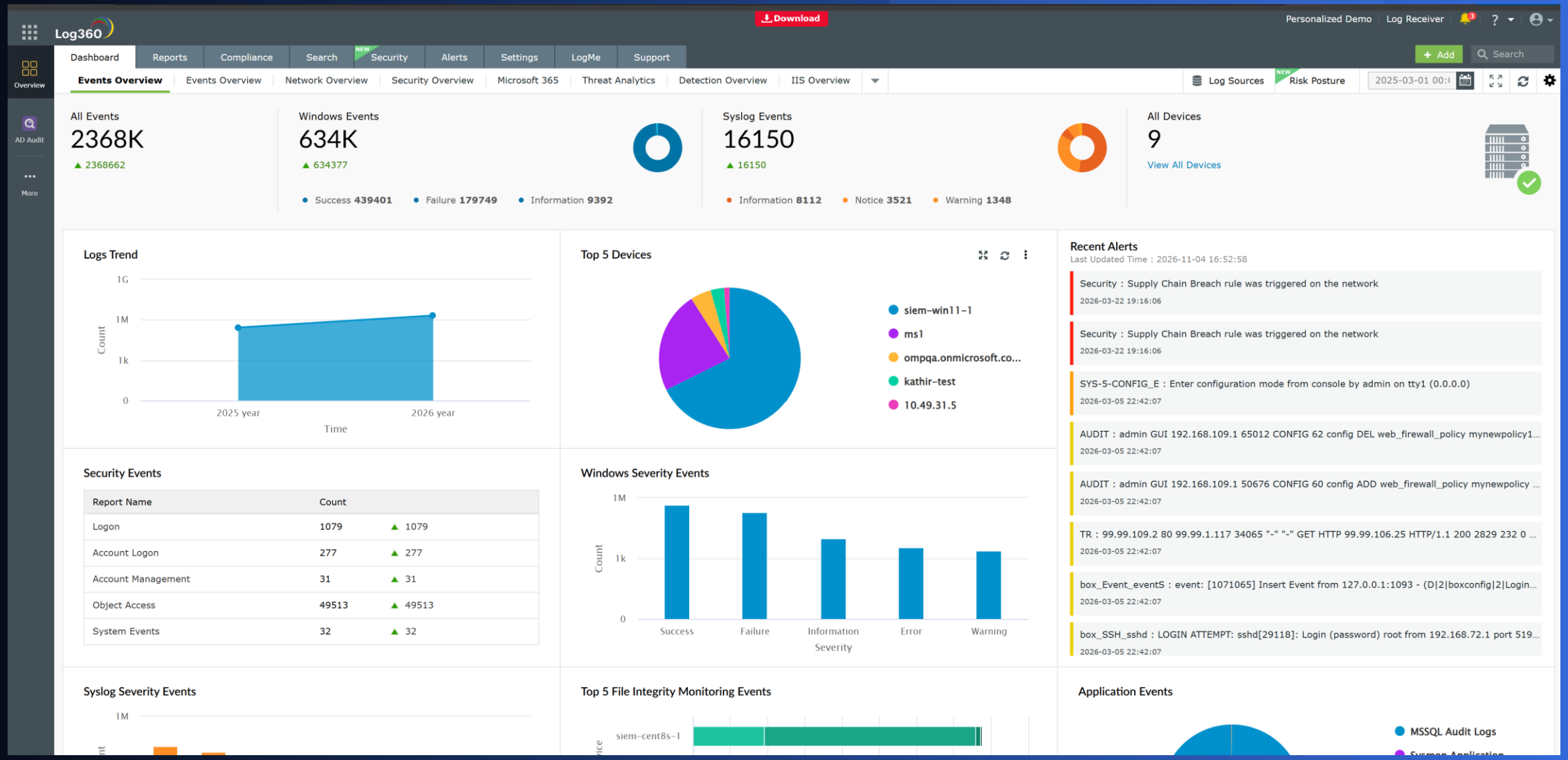
erik.tjarnkvist@inuit.se


ManageEngine
Log360


ManageEngine
Log360 Cloud


Log360 13.0.7 setup
Select Installation type
Choose whether to install Log360 with all of its components or Log360 alone. You can also choose to install only the components you need.
Standard Installation
Installs all the components. Recommended for most users.
Minimal installation
Installs Log360 alone without installing the components
Destination Folder
C:\Program Files\ManageEngine\Log360
Browse
InstallShield
< Back
Next >
Cancel


LOG360 – LAYERED ARCHITECTURE
1
DATA INGESTION LAYER
Collect, validate and normalize logs from across the environment
Network Devices
Servers & Apps
Cloud Services
Security Tools
Databases
Directories
Endpoints
Agents
750+ sources
Endpoint logs Network devices Cloud apps Security tools
Access Gateway
DMZ / Proxy
SSL/TLS Load balancing Authentication Throttling
Log Processor Cluster
Round-robin / Failover
Horizontal scalability High availability
2
PROCESSING & STORAGE LAYER
Process, correlate and store at scale
QUEUE ENGINE
Topics → Partitions → Replication → Brokers → Producers/Consumers
Processing Engine
Parse | Normalize Enrich | Dedupe
Correlation Engine
Event Correlation Rule Evaluation
Search Engine
Index | Aggregate Fast Retrieval
Alert Engine
Thresholds | Anomalies Real-time Alerts
TIERED STORAGE
Hot Storage
Elasticsearch Cluster High-speed Indexing Search
Cold Storage
Archive Long-term Retention Cost Optimized
Metadata Storage
PostgreSQL Config | Metadata Audit Info
3
DETECTION LAYER
Detect threats and prioritize risks
CENTRALIZED DETECTION CONSOLE
2,000+ Rules
MITRE Mapping
Object-Level Filtering
Risk Scoring
Behavior Analytics (UEBA)
4
INVESTIGATION LAYER
Investigate alerts with deep context
Incident Workbench
Case management Evidence notes Collaboration
Alert Investigation Agent
LLM-powered Analysis
Entity Extraction
Enrichment Threat Intel
Timeline Reconstruction
MITRE Mapping
5
RESPONSE & AUTOMATION LAYER
Automate actions and integrate with ecosystem
SOAR Playbooks
Automate orchestration Respond faster
Ticketing Integrations
ServiceDesk Plus ServiceNow
Notifications
Email / SMS Alert escalation
REST APIs / Webhooks
Bi-directional integration Custom workflows
6
VISIBILITY & COMPLIANCE LAYER
Gain visibility, ensure compliance and maintain trust
Customizable Dashboards
Real-time visibility Role-based views
Compliance Reports
1000+ reports Ready for audit
Hybrid Monitoring
On-prem | Cloud Multi-tenant
Tamper-Detecting Audit Trails
Immutable logs End-to-end integrity
Data Flow
Control Flow
Storage
Processing
Analytics
Security
Integration
User/Action


Log360
Download
Personalized Demo
Log Receiver
Dashboard
Reports
Compliance
Search
Security
Alerts
Settings
LogMe
Support
Add
Search
Overview
AD Audit
More
Events Overview
Events Overview
Network Overview
Security Overview
Microsoft 365
Threat Analytics
Detection Overview
IIS Overview
Log Sources
Risk Posture
2025-03-01 00:
All Events
2368K
▲ 2368662
Windows Events
634K
▲ 634377
Success 439401
Failure 179749
Information 9392
Syslog Events
16150
▲ 16150
Information 8112
Notice 3521
Warning 1348
All Devices
9
View All Devices
Logs Trend
1G
1M
1k
0
Count
2025 year
2026 year
Time
Top 5 Devices
siem-win11-1
ms1
ompqa.onmicrosoft.co...
kathir-test
10.49.31.5
Recent Alerts
Last Updated Time : 2026-11-04 16:52:58
Security : Supply Chain Breach rule was triggered on the network
2026-03-22 19:16:06
Security : Supply Chain Breach rule was triggered on the network
2026-03-22 19:16:06
SYS-5-CONFIG_E : Enter configuration mode from console by admin on tty1 (0.0.0.0)
2026-03-05 22:42:07
AUDIT : admin GUI 192.168.109.1 65012 CONFIG 62 config DEL web_firewall_policy mynewpolicy1...
2026-03-05 22:42:07
AUDIT : admin GUI 192.168.109.1 50676 CONFIG 60 config ADD web_firewall_policy mynewpolicy ...
2026-03-05 22:42:07
TR : 99.99.109.2 80 99.99.1.117 34065 "-" "-" GET HTTP 99.99.106.25 HTTP/1.1 200 2829 232 0 ...
2026-03-05 22:42:07
box_Event_eventS : event: [1071065] Insert Event from 127.0.0.1:1093 - (D|2|boxconfig|2|Login...
2026-03-05 22:42:07
box_SSH_sshd : LOGIN ATTEMPT: sshd[29118]: Login (password) root from 192.168.72.1 port 519...
2026-03-05 22:42:07
Security Events
Report Name
Count
Logon 1079 ▲ 1079
Account Logon 277 ▲ 277
Account Management 31 ▲ 31
Object Access 49513 ▲ 49513
System Events 32 ▲ 32
Windows Severity Events
1M
1k
0
Count
Success
Failure
Information
Error
Warning
Severity
Syslog Severity Events
1M
Top 5 File Integrity Monitoring Events
siem-cent8s-1
Application Events
MSSQL Audit Logs

Log360 från ManageEngine är en samlad SIEM-lösning (Security Information and Event Management) som hjälper dig att hålla koll på säkerheten i hela IT-miljön.

Den samlar, analyserar och övervakar loggar från servrar, brandväggar, applikationer, Active Directory, molntjänster (som Microsoft 365, AWS och Azure) och mer – allt från ett och samma gränssnitt.

Snabbare incidenthantering och automatisering

- Incident Workbench – centraliserad utredning med kontext från både AD och övriga loggkällor.

- SOAR-funktioner och färdiga playbooks för att automatisera respons.
  (Security Orchestration, Automation and Response)

- AI-stöd (Zia) som hjälper analytikerna att förstå och prioritera snabbare.

- **UEBA (User & Entity Behavior Analytics)** – maskininlärning som skapar beteendeprofiler och ger riskpoäng. Upptäcker insiderhot, kompromitterade konton och avvikande aktivitet som traditionella regler missar.

- **Threat Intelligence** – inbyggd hotintelligens och dark web-övervakning.

Compliance och rapportering på en helt ny nivå

- Färdiga rapportpaket för GDPR, NIS2, DORA, PCI DSS, HIPAA, ISO 27001 m.fl.
- Enklare att visa revisorer helhetsbilden – inte bara AD-förändringar.
- Bättre forensik och långsiktig loggarkivering.

Frågor?

Tack!