nextgen elevates your cyber security European technology. Local expertise.



Comprehensive protection
 User-centric design
 Customized solutions
 Simplified compliance

CYBERQUEST SIEM CQ Automation NETALERT NDR CQ Threat Intelligence CQ AI Assistant

nextgen PORTFOLIO



CYBERQUEST SIEM CQ Automation NETALERT NDR CQ Threat Intelligence CQ AI Assistant

Elevate your security operations. Comprehensive visibility & observability across organization. Unmatched detection with UEBA and over 400 correlation rules. Actionable insights for faster, smarter decisions.



	Advanced User and Entity Behavior Analytics - UEBA	 Scalable solutions for modern enterprises. Identify subtle behavioral patterns for risks.
	Analytics-powered experience for impactful decisions	 Actionable insights for faster, smarter decisions. Intuitive Interface: Simplifies complex tasks for smooth navigation and efficiency. Efficient Workflow: Al-assisted investigations and responses that streamline processes.
F8	Comprehensive observability & visibility	 Anticipate threats before they happen. Scalable solutions for modern enterprises. Identify subtle behavioral patterns for risks.
Ğ	Flexible deployment options, ready to scale up	 Adapts to any IT policy. Reduces infrastructure constraints. Enhances operational agility. Ultimate control and flexibility. Scales with your business needs and can run on hundreds of big information screens, in large, real-time situations environments.
+	Streamline threat detection, investigation & response	 Detection with UEBA and over 400 correlation rules. Endpoint forensic insights, real-time threat intelligence. High level overview for user devices incidents.

Detect, anticipate and respond with the power of Cyberquest SIEM - request your demo NOW!

Scalable and Flexible Log Collection

- Collect, Parse, Normalize, Index and Store security logs at very high speeds
- Out-of-the-box support for a wide variety of security systems and vendor APIs, both on-premises and cloud
- Windows Agents provide highly scalable and rich event collection including standard or non-standard windows logs, file processing, database tables
- Modify parsers from within the GUI and redeploy on a running system without downtime and event loss
- Create new parsers via integrated parser development Web Interface and share among users via export/import function
- Securely & reliably collect events for users & devices located anywhere

Easy Scale Out Architecture

- Available as Virtual Machines for on-premises and public/ private cloud deployments on the following hypervisors — VMware ESX, Microsoft Hyper-V, KVM, Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform (GCP)
- Scale deploying on multiple servers to increase performance
- Scale data collection by deploying multiple Collectors
- Collectors can buffer events when connection to Cyberquest is not available
- Log storage can be either the Cyberquest proprietary NoSQL database, or Elasticsearch which provides the ultimate in scalability





Automation and Incident Management

- Ability to trigger a remediation script when a specified incident occurs
- API-based integration to external ticketing systems
- Built-in Case Management system
- Incident reports can be structured to provide the highest priority to critical business services and applications
- Trigger on complex event patterns in real time

Rich Customizable Dashboards

- Specialized layered dashboards for business services, virtualized infrastructure, event logging status dashboard, and specialized apps
- Out of the box dashgroups for all connected data sources.

External Technology Integrations

- Integration with any external web site for IP address lookup
- API-based integration for external threat feed intelligence sources
- API for easy integration with provisioning systems

External Threat Intelligence Integrations

- APIs for integrating external threat feed intelligence
- Malware domains, IPs, URLs, hashes, Tor nodes







Cyberquest's Advanced UEBA module brings intelligent threat detection to the next level. By applying machine learning, it learns how users and systems typically behave, so it can quickly spot when something's off.

Whether it's a user logging in at an unusual hour, accessing sensitive files they normally wouldn't, or a device acting out of character, UEBA flags abnormal activity in real time. This helps your security team catch threats early - before they escalate.

What makes Cyberquest UEBA stand out? You can go beyond standard detection by using custom detection patterns. Tailor alerts to your organization's specific needs - like monitoring for unusual admin actions, rare file transfers or policy violations.

Get a unified view of risk, enriched alerts and powerful dashboards - all designed to help you respond faster and smarter.



ALERTS

Alert definition parameters

- Alert Name: Unique identifier for the alert.
- Alert Active: Boolean flag to enable/disable the alert.
- Sent as Alert: Allows backend correlation without user-facing notifications.

Time-based control

• Time Frame TTL (sec.): Defines how long the alert remains active after being triggered. This is crucial for time-sensitive correlation logic.

Security scoring system

- Alert Security Score: A dynamic score that starts from a baseline and adjusts based on rule matches and event frequency. Range: baseline to 100.
- Alert Security Level: Color-coded severity level that mirrors the score.

Notification system

- Send via Email: Enables email notifications to predefined recipients.
- Notification Template: Supports both built-in and custom templates for alert messages.





Alert execution

- Has Action: Enables execution of a custom script when the alert is triggered.
- Script Editor: Embedded editor to define logic in a scripting language. This script overrides all other rule conditions.
- **Predefined Action Execution**: Facilitates the automatic triggering of configured actions or operational playbooks upon alert activation.

Rule-based event correlation

- Rule Logic: Supports complex logical conditions using:
 - AND, OR, NOT operators
 - Field-based filters (e.g., =, not =, is in list, not in list, starts with, ends with, contains, range, contains any of, contain all of, regex match)
 - \circ Report-based triggers
 - Event correlation (e.g., sequence, absence, or timing of events)
- Rule Settings Pane: GUI for defining and managing rule logic.

	33902		0		33902
	O Alers		• Resolved		A Unvectived
 Reset A 	ens · titterit		🔈 Stat	tases Distribution	
h Deckard P Address Activity Internet	20545-010-02400				
h Descard PAthenAstry Hand	2025-05-15 02 47 31 000				
In Deck and P Address Activity Interest	0 15 May 28 2025-05-15 62-47 34-000	. and here .		andum	analasa analasa
	· 15 May 28		• NEW • ADVID	• FALSE POSTINE	
II Eb Latert A	un l	III) Security Sco	re Statistics		IIC Security Scores Ranges
h Deckard PAthenAdery Hand	2025-05-15 62-47 20 000	unique Kiert Security Score			
h Descard PAtternAstry Hand	0 15 May 28	fearing Alex Security Score			
b Deckard P Addres Addres Intered	0 15 May 28	fromum Alart Security Socre		-	
	· 15 May 28				Ren Court
	IRC Top Users		III Top Computers		IIC Top SroPs
.			7 <u></u>		J.,,,,
		A MULT WITH REPORT TO A LONG TO A	and an end of the set of the local data of the		

ALERTS

Event correlation capabilities

- Single event triggers
- Multi-event correlation:
 - Event order
 - Missing events in a sequence
 - Logical succession of events
 - Multiple event sequence
 - Count, average or sum on specific field values
 - Multiple data sources correlations

K Exit, without Saving B SAVE ALERT & EXIT		ALERTS	ETTINGS				
Aviet Name High data Transfer flow ALERT ACTIVE AGENT ACTIVE Defout notification CFFART DEDUPLIC	Time Frame TTL (sec.)	Alert Security Score 70	Alet Security	angi 54	end as Alert 😢 Has Action end via Email 🔳 Input email a	Zef Action Parameters	
+ ADD BALE + PISYOUS + NEXT	Rule number 2 Settings						
	Description	Rule's Trigger Type	Min Threshold	Max Threshold	TTL (sec.)	Pivet Field	
C1 - Rule No. 1 - detect flow	menin 256Mb and max 512Mb	Sum Preoffield and MaxTreats	21400000	51200000		12 _selwork TransferedDytes	
III Cand. 0: Events whose III EventID field is one of the following. case,case,case AND	▼ Rule Consilions ● AZO FI	ELD CONDITION ADD REPOR	т сомотнома — <i>а</i> й лоо 	CONDELATION CONDITION	↓ II Event0	I~	🖹 Dolete
Cond. 1: Events whose #network.TransferedBytes field is greater than: assee	2	₹ sa#	~] -	v Rain No. 1	v T See	•	@ Dolete
TIME FRAME will start on first event that will match the Conditions above.	3.	TealP	• -	v Relation	v ₹ 0m#P	I •	B Delete
C1 Editing - Rule No. 2 - minim 256Mb and max \$1200 Delete	4	🌲 _where SciPat	• •	v Rale No. 1	🛛 🗸 🛔 _network. SecP	wi v	Celete
Cond. 0: Events whose 18 EventID field is equal to: 18 EventID field value of the events that mached Rule No. 1	s	🛔 _echeck.DestFod	• -	V Rate No. 1	🛛 🗸 👗 _ network Deat	~ v	@ Delete
B Cond. 1: Events whose \$\phi_101\$ field is equal to: \$\phi_2\$ field whose of the events that mached Poly No. 1 ano	-						
	€ 2017 - 2023 Navi	yen Solware SHL Alf rights reserved. ["Wester	(238371) Privacy Publy Cook	• printy			
Multiple correlation	n rule for "l	ligh data]	Fransfei	-11			Ĭ.

REPORTS

Report Types

- **Technological Reports**: Summarized and detailed reports for specific technologies (e.g., Windows, Linux).
- Compliance Reports: Mapped to standards like:
 - ISO 27001
 - GDPR
 - HIPAA
 - PCI DSS
 - SOX
 - COBIT
 - FISMA
 - DORA, NIS2 ???
- **Best Practices**: Frequently used reports based on industry standards.
- **Custom Reports**: User-defined reports not included by default.
- **GDPR Reports**: Focused on data protection and privacy compliance.

151		●● ◆ ® · ¤ ± ♠ ♠ ♠
Reports	Compliance	
e 🚔 Reports		
Best Practices		
Compliance	Search	
COBIT		
P FISMA	Compliance	Actions
- HIPAA		
PCI	🖿 совіт	
P SOX		
Custom reports	💼 FISMA	
🗉 🖿 Demo		
🖷 🧰 GDPR	E HPM	
Access to Files		
Account Policy Changes	■ 1S0 27001	
Account successfully logged on		
Administrative Group Members	PCI	
Changes All Active Directions Changes		
All Logon Activity	SOX .	
All Windows Server Changes		
Audit Policy Changes		Rows per page: 10 + 1-6 of 6 (C > >)
Failed Account Logons		
File Read Attempt		
Local Audit Policy Changes		
Object Security Changes		
Password Policy Changes		
Password Resets by Administrator		
Permissions Changes		
System time changes		
User Account Locks and Linincks		
User Account Status Changes		
User Account was Changed		
User Accounts		
User Accounts - Expired		
User Accounts - Locked		
User Activity Summary		
User Logoffs		
Windows Settings Changes		
	Play P	

CO CYBERQUEST Automation | SOAR

Automated incident response with intelligent orchestration. Simplify integration, enhance collaboration and maximize the efficiency of your security stack.



Comprehensive case management

Effortless application integrations



Generative AI for faster, smarter decisions

Tailored for enterprise or managed services needs



- Simplify complex processes, reduce manual effort and focus on what matters most: mitigating threats.
- Execute actions across your security and IT tools in seconds, not hours.
- Speed up incident response by automating workflows and decision-making, ensuring faster, more efficient threat management.
- Supports custom templates and industrystandard frameworks.
- Efficient task segmentation, assignment and documentation for better organization.
- Collaborative process: Keeps teams aligned, ensuring thorough and detailed investigations.
- Connect with 95+ tools effortlessly.
- 1,230 automated actions for workflows.
- Enhance collaboration & optimize security operations.
- Automates tasks using natural language understanding.
- Enhances threat investigation, response and playbook creation.
- Boosts decision-making and streamlines complex workflows.
- Suited for enterprises with flexible solutions.
- Choose from on-prem or cloud hosting based on your needs.

Automate, orchestrate and outpace threats with CQ Automation - see it in action TODAY!

COCYBERQUEST Automation | SOAR

Playbook Automation Engine

Outlines how Cyberquest structures and executes automated response workflows (playbooks). It explains the graphical interface for building playbooks, the dynamic input system and the multiple triggering methods (automatic via alerts or manual via GUI).

- Playbook Structure:
 - A playbook is a sequence of actions grouped to perform a mitigation or response flow.
 - Actions are added/removed via a graphical interface.
 - Each action requires input parameters, which are dynamically evaluated at runtime.
- Execution Modes:
 - Automatic Triggering:
 - Triggered by specific alerts.
 - The alert instance becomes the global inputData for the playbook.
 - Configured via: web graphical interface.
 - Manual Triggering:
 - From the Event Browser: user clicks on a specific event.
 - From the Alert Browser: user clicks on a specific alert.
- Execution History:
 - Debugging tool to trace parameter values and action outcomes.
 - Helps identify failures or misconfigurations in playbook logic.

	*•• • 🛛 · 🗆 ± 🎮 🦗	
 ►	New Playbook: Income of indexes	
Andrewson Construction Market Marke	Biol Protein Biol Protein Bi	
Contract of the second	© 2017-2025 Nanjao Kolwan SML-Al fujita manoni (lannar 230.641 Pisany Palay Coole pelay	
Linux IP a	ddress block action	1

CO CYBERQUEST Automation | SOAR

Playbook Automation Engine

		<u> </u>
CYBERQUEST		*© < @· ī ± 🔗 🦳 🦳
Beenen Norse Rose	New Playbook: Divide Domain Account	Asser: Gents. C Gents.
		E Duale Lure 4 E Soutile Lure 4 E Soutile Lure 4 E Souti Sorice 4 E Souti Sorice 4 E Souti Sorice 4 E Resart Sorice 6
Hamathan Hamanathy Magdadata	Citable Une	EXD EXD Annihal Dar v v v Annihal Dar v v Annihal Dar v v Annihal Dar v v v Annihal Dar v v
		Annotat Users O Annotat Users O Annotat O
Anna 1 Barris II Anna II An	© 2017-2029 Neetyen Schware SHL All synta merindi (Iverain 1.202041 Polwary Pelary Cooke poly	Conser Conser
Disable domain accou	nt	
		•••• • •• • • • •
	Edit Playbook: Book malicous P	Armen Cranch. Colored Cylinologiatherita Cylinologiatherita V Windoweddana V
		Advertist A
Accession of the second		
Correction Control on	ind Ind	NO B. Foolbinder v 1 Hondb v 1 Hondb v
Block IP in vari <u>ous sys</u>	exer 2015 hadge Schere 20, stages energy (News 23) 451 Paragehety Gala pairs	

COCYBERQUEST Automation | SOAR

Playbook Automation Engine

Details the two main categories of actions used in playbooks: vendor-specific (integrated with external security tools) and functional (logic-based actions like conditions, counters, and custom scripts). These actions form the building blocks of automated responses.

- Vendor-Specific Actions:
 - Integrated with a growing list of security vendors.
 - Uses vendor APIs for:
 - Blocking IPs
 - Isolating hosts
 - Updating firewall rules
 - Sending alerts or notifications
 - Updated automatically with new vendor integrations.

• Functional Actions (under "CYBERQUEST Playbook"):

- **IF**: Conditional branching based on Boolean logic.
- **Count**: Counts elements in an array-type variable.
- Code: Executes a DTS object (custom logic written in JavaScript).



Smart Playbook Features

- Highlights advanced features that enhance flexibility and reusability in playbooks, such as dynamic parameter evaluation, modular logic blocks, and support for custom scripting using JavaScript (DTS objects).
- Dynamic Parameters:
 - Input values are computed at runtime using placeholders and context variables.
- Reusable Logic:
 - $\circ\;$ Actions and logic blocks can be reused across multiple playbooks.
- Custom Scripting:
 - Supports JavaScript via DTS objects for advanced logic and data manipulation.

Audit & Forensics

- Covers the logging and traceability features of CQ Automation/ SOAR. It explains how every action is recorded for compliance, debugging, and forensic analysis, ensuring transparency and accountability in automated responses.
- Execution Logging:
 - $\circ~$ Every action is logged with:
 - Input parameters
 - Execution result
 - Timestamp and user ID (if manual)
- Forensic Reports: Generated from execution history for compliance and incident review.







Advanced network defense. Agentless network visibility. Al-driven threat detection. Eliminate blind spots and take control. Single fabric integration with Cyberquest SIEM/ SOAR.



- Monitor every session, device and user to identify potential threats efficiently.
- Al-powered analytics uncover suspicious behaviors, data exfiltration attempts and other malicious activity.
- Automate detection, prioritize alerts.
- Comprehensive traffic monitoring. Supports TAP, SPAN and ERSPAN for complete visibility.
- Advanced threat detection: utilizes both supervised and unsupervised AI/ML models.
- Continuous network insights: analyze network metadata and traffic in real time.
- Uncover hidden incidents: analyze historical network activity to identify past security events.
- Detect anomalies early: spot unusual behavior before it escalates into a threat.
- Strengthen your defense: identify and secure vulnerable assets to prevent future attacks.
- Faster incident response: investigation and mitigation within a single console.
- Enhanced security efficiency: reduce manual workload and accelerate threat resolution.
- Maximum confidentiality and compliance. Purpose-built for highly secure and regulated environments.
- Full network visibility: maintain security without sacrificing insight into network traffic.

Agentless network visibility

Al-driven threat detection

Conduct threat hunting

, The second se

Enable orchestrated incident response



Perfect for air-gapped environments

Eliminate blind spots and take control with Netalert NDR - deploy advanced network defense NOW!



Threat Detection Capabilities

NetAlert NDR uses a combination of signature-based, heuristic and machine learning techniques to detect a wide range of threats. These include DDoS attacks, brute-force attempts, TOR traffic, lateral movement, crypto-mining and anomalies in DNS, SMTP and SSL traffic. It also integrates with threat intelligence feeds to detect known Indicators of Compromise (IOCs):

DDoS Detection

- Mechanism: Monitors for volumetric anomalies in traffic (e.g., SYN floods, UDP floods).
- **Techniques**: Rate-based thresholds, entropy analysis of source IPs and protocol-specific heuristics.
- Indicators: Sudden spikes in traffic, repeated requests to a single endpoint or protocol misuse.

TOR Endpoint Detection

- **Mechanism**: Matches outbound connections against known TOR exit node IPs.
- Data Source: Regularly updated threat intelligence feeds.
- Use Case: Identifies attempts to anonymize traffic, often used in exfiltration or C2 (Command & Control) channels.

							<u>/</u>			î
Santon Lank	Search	core × 📴 Alert Name × 🛛 Alert IP	× ¥ Flow ID	Q 2025-05-0	01 22:09 🗎 20 Severity × 2 Attac	25-06-02 22:09 曽 🔻 UTC_ISO8601 D kStage × 💥 MitrelD × 🙆 Duration × 1	DESC Ø Repea		ert Name	
A	@ View	UTC Time (UTC_ISO8691)	ML Score (ML,score)	Alert Name (AlertName)	Q Alert IP (Alert,IP)	4t Flow ID (Flow,ID)	85	PortScan	61237	
<u>.</u>								DeviceAbnormatBehaviour	23743	
								LateralMovement		
		2025-06-02719:10:45.125959+00:00		DNSRequests	192.168.200.99	528F2271-4462-053F-C33E-A4090ED172EC		Invalid\$31.		
								Heartbleed		
	• v	2025-06-02119:10:44/286265+00:00	50 🔒	DNS not in WhiteList	192.168.200.135	05505632-0764-961E-AA3C-2A978CAF0E61	MEC	CryptoMining		
								Mysql activity		
	• •	2025-06-02119:10:41.842973+00:00	30 🔋	New External Device Detected	NJ 109.191.139.4			TLS over non standard port		
								DNSTunnelingStatistically	878	
								TOR	855	
	• •	2025-06-02T19:10:37.025480+00:00	30 📒	New External Device Detected	nu 37.99.223.16			IOCDomains		
								Volume alert		
								High volume connections		
								Communication over non standard port		
								Slow Network Scan		
	Total Results: 122 M	B						Possible APTAlert - Test		
	Alert stat	istics – last	: 30 c	lays						



Dynamic DNS (DDNS) Usage

- Mechanism: Flags DNS queries to known DDNS providers (e.g., No-IP, DynDNS).
- Use Case: Common in malware C2 infrastructure to maintain persistence.

Crypto-Mining Detection

- Mechanism: Identifies mining pool traffic (e.g., Stratum protocol) and high CPU usage patterns.
- **Indicators**: Outbound connections to known mining pools, unusual traffic from non-user-facing devices.

IOC-Based Detection

- Mechanism: Matches traffic against curated lists of IPs, domains, and file hashes.
- Sources: Threat intelligence feeds (STIX/TAXII, MISP, etc.).

APT Behavior Detection

- **Mechanism**: Correlates multiple low-level indicators (e.g., lateral movement, privilege escalation).
- Techniques: Behavioral analytics and ML-based anomaly scoring.

								supersonan a
Search				01 22:09 📋 21	025-06-02 22:09 🛗 🔻 UTC_ISCIB601 D		Fa /	Alert Name
O UTC Time X 4 ML	icore 🗴 📴 Alert Name 🗴 🖗 Alert IP	× M Flow ID	× Bb Impact × Ga	Severity × 2 Atta	ckStage × X MitrelD × 🖸 Duration × 🤉	C Repea	Connections	294534
@ View	UTC Time	ML Score	Alert Name (AlertName)	Q Alert IP (Alert IP)	¹ 1 ² Flow ID (Now ID)	8	New External Device Detected	
@ \$	2025-06-02719:14:35:501826+00:00	30 🔋	New External Device Detected	nu 92.248.253.54			BruteForce	
							DeviceAbnormalBehaviour	
	2025-06-02119:14:34.352355+00:00	so 🥛	DNS not in WhiteList	192.168.200.99	E88F8C90-8280-9453-185F-3149E8FE2181		LateralMovement	
Ø 	2025-06-02119:14:34:329894+00:00	so 🤋	DNS not in WhiteList	192.168.200.121	A3EBF88A-D1F4-F2A4-8268-9A6C0EA3C417		Invalid531	
			New External Device				Heartbleed	
•	2025-06-02119.14064834998+0000	30 📙	Detected	NL 178.162.174.43				
							CryptoMining	
							Mysql activity	
							TLS over non standard port	
•	2025-06-02119.13:59.922869+00:00		DNSRequests	192,168,200.99	052723E7-1607-F062-07A1-A99929EB4284		DNSTunnelingStatistically	
							IOCDomains	
							Volume alert	
							Communication over non standard port	
Total Results: 122 M							Slow Network Scan	



Threat Detection Capabilities

Failed DNS Requests

- Mechanism: Tracks DNS query/response pairs and flags unresolved queries.
- Indicators: High volume of NXDOMAIN responses, which may indicate domain generation algorithm (DGA) activity.

Heartbleed Exploit Detection

- Mechanism: Deep packet inspection (DPI) of TLS heartbeat messages.
- **Signature-Based**: Looks for malformed heartbeat requests that attempt to read memory beyond buffer limits.

Invalid SSL Certificate Connections

- Mechanism: Parses SSL/TLS handshakes to validate certificate chains.
- Checks: Expired certs, self-signed certs, mismatched CN/SAN fields, or untrusted CAs.

Port and Address Scanning

- Mechanism: Detects horizontal (same port, many IPs) and vertical (many ports, same IP) scans.
- **Techniques**: Flow analysis and connection attempt patterns.

Search			Q 2025-05-2	12.05 🗰 20	125-05-27 12:05 🗰 🔻 UTC_ISO8601 D	ESC				
OUTC Time × Fa ML	Score × 🕞 Alert Name × 🛇 Alert IP	× 부 Flow ID :	× 🖾 Impact × 🚳 S	ieverity × 🖉 Attac	kStage × X MitrelD × ODuration ×	🕒 Alert Name				
@ View	UTC Time	(ML,score)	Alert Name	Alert IP (Alert_IP)	Flow ID	80 (m	Quick Search	■ 10 × ◆E		
\$ \$	2025-05-27110:12:10.877080+00:00	50 📕	DNS not in WhiteList	192.168.200.167	8A889561-8990-86E6-5D8D-C7CAD7C136EC	MED	8000-			
() ()	2025-05-27110-12:08:075015+00:00	10	DNSRequests	192.168.200.153	687C798E-DE47-A208-CE88-02821E5EF606	ιc		Count		
							Field DNS not in WhiteList	Count 14318		
	2025-05-27110:12:08.778216-00:00	10	DNSRequests	192,168,200,153	86864490-8876-7728-8460-384956631039		DNSRequests	12538		
						LC	New External Device Detected	9144		
@ \$							DNSTunnelingStatistically	63		
							Slow Network Scan	5		
							Volume alert	4		
Total Results: 36.08 K	C.						BruteForce	3		
							PAV7	·		
			© 2017 - 202	25 Nextgen Software	SRL All rights reserved. Version: 1.1					



Threat Detection Capabilities

Malware Lateral Movement

- Mechanism: Detects SMB, RDP, or WMI-based lateral movement.
- Indicators: Unusual peer-to-peer connections, credential reuse, or privilege escalation attempts.

Abnormal Network Behavior

- **Mechanism**: Uses statistical baselining and ML to detect deviations in traffic volume, protocol usage, or peer communication.
- Models: Time-series anomaly detection, clustering, and outlier detection.

DNS Anomalies

- Mechanism: Flags suspicious DNS patterns like:
 - High entropy domains (DGA)
 - Fast-flux DNS
 - Unusual TTL values

SMTP Traffic Monitoring

- Mechanism: Parses SMTP headers and payloads.
- Use Case: Detects spam, phishing attempts, and data exfiltration via email.

ML-Based Anomaly Detection

- Mechanism: Ensemble of unsupervised models (e.g., Isolation Forest, Autoencoders).
- **Output**: Alerts with confidence scores and contributing features.

IDS Rule-Based Alerts

- Mechanism: Integrates with Suricata/Snort rule engines.
- Use Case: Signature-based detection of known exploits, malware, and protocol violations.



The system passively captures traffic via TAP/ SPAN ports, aggregates TCP sessions and collects flow data across VLANs. It decodes binary protocols like DNS, SMTP and HTTP, and supports PCAP recording for forensic analysis. This enables deep visibility into network behavior and supports both real-time and historical analysis.

Passive Traffic Capture

- Method: Uses TAP (Test Access Point) or SPAN (Switched Port Analyzer) ports.
- **Deployment**: Works in both VMware virtual environments and physical network setups.
- **Purpose**: Enables full visibility into network traffic without interfering with it (non-intrusive).

Connection Grouping for TCP

- Function: Aggregates individual TCP packets into logical connections or flows.
- Benefits:
 - Simplifies analysis by treating a session as a unit.
 - Enables detection of session-level anomalies (e.g., long-lived connections, retransmissions).

VOT Dest	P:10.0.0	0*		10 11 UF Q	2025-05-26 12:05	25-05-27 12:05	▼ UTC_ISO8601 DESC		Destination IP		
Local T	ime ×	🕓 UTC Ti	me × 🏾 숙 Source IP × 🖉 🛛 D	estination IP 🗙 🐨 Source Port 🗴	Destination Port × Prot						
	@ Vie	•	Local Time (LocalTime)	UTC Time (UTC_ISO8601)	Source IP	Destination IP (DestIP)	Source Port (SecPort)	Quick Search	8	10 ~	Φ Exit
۲	0		2025-05-27710:11:22+0000	2025-05-27710:11:22.221310+00:00	192.168.200.135	us 54.83.44.15		450000-			
۲	0		2025-05-27710:11:22+0000	2025-05-27710:11:22.210252+00:00	192.168.200.121	us 54.83.44.15		300000-			
۲	۰		2025-05-27710:11:22+0000	2025-05-27710:11:22.209464+00:00	192.168.200.12	192.168.200.128		150000			
۲	0	4>	2025-05-27T10:11:22+0000	2025-05-27710:11:22.201575+00:00	192.168.200.184	192.168.200.228					
۲	0	4>	2025-05-27T10:11:21+0000	2025-05-27710:11:21.780429+00:00	192.168.200.99	192.168.200.240	15817	A. 3. 30	a. A. A. A	1. M. M.	alle .
۲	0	\diamond	2025-05-27110:11:21+0000	2025-05-27710:11:21.755510+00:00	192.168.200.110	192.168.200.255	137	1.45 1.45 1.46	Count	100 / 100 / 1	a ia
۲	0	ϕ	2025-05-27710:11:21+0000	2025-05-27710:11:21.536101+00:00	192.168.200.1	192.168.200.130		Field	Count		
۲	0	ϕ	2025-05-27710:11:21+0000	2025-05-27710:11:21:311973+00:00	10.10.0.63	10.10.0.76		52.122.140.24	555556		
۲	0	$\langle \rangle$	2025-05-27T10:11:21+0000	2025-05-27710:11:21:311973+00:00	10.10.0.63	10.10.0.1		192.168.200.240	177286		
۲	0	$\langle \rangle$	2025-05-27T10:11:21+0000	2025-05-27710:11:21:311973+00:00	10.10.0.63	10.10.0.76		79 110 100 200	153601		
۲	0	<>>	2025-05-27T10:11:21+0000	2025-05-27710:11:21:311973+00:00	10.10.0.63	10.10.0.1		73.110.190.200	136341		
۲	•		2025-05-27110:11:21+0000	2025-05-27710:11:21.290416+00:00	192.168.200.99	192.168.200.240	15817	192.168.200.239	106399		
۲	0		2025-05-27710:11:21+0000	2025-05-27710:11:21.256660+00:00	fe80:8ac9:8d5e:505d:9e3f	f102::fb	5353	192.168.200.10	64060		
۲	0		2025-05-27710:11:21+0000	2025-05-27710:11:21.255977+00:00	192.168.200.110	224.0.0.251	5353	192.168.200.21	56368		
Total R	esults:	2.28 M	D•					192.168.200.108	52069		
								103.1(0.399.10	61013		
				0	2017 - 2025 Nextgen Software	SRL All rights reserved.	Version: 1.1				



Traffic Monitoring & Analysis

Connection Statistics

- Metrics Collected:
 - Packet loss
 - Packet size distribution
 - Round-trip time (RTT)
 - \circ Flow duration
- Use Case: Helps in performance monitoring and anomaly detection (e.g., degraded service quality).

Flow Collection Across VLANs

- Integration: Can ingest NetFlow/IPFIX/sFlow data from third-party devices.
- **Cross-VLAN Visibility**: Enables monitoring of traffic that spans multiple VLANs, which is crucial in segmented networks.

Binary Protocol Decoding

- Supported Protocols:
 - \circ DNS
 - \circ SMTP
 - \circ HTTP
- Function: Parses and extracts structured data from protocol payloads.
- **Use Case**: Enables deep inspection for threat detection (e.g., DNS tunneling, phishing emails, malicious HTTP headers).

PCAP Recording

- Limit: Up to 32 KB per session.
- Purpose: Stores raw packet captures for forensic analysis.
- **Trigger**: Typically initiated upon detection of suspicious activity or policy-defined events.



Machine Learning Integration

NetAlert supports a modular ML framework using models from PyOD, Graphomaly and Prophet. Users can configure detection behavior via JSON files, adjust contamination levels and apply ensemble voting strategies. It supports multiple anomaly detection tasks (e.g., Kerberos, TCP, DNS) and allows fine-tuning for accuracy and false positive reduction.

Contamination Level

- **Definition**: A key hyperparameter in unsupervised anomaly detection.
- **Purpose**: Specifies the expected proportion of anomalies in the dataset.
- Impact: Affects the sensitivity of models like Isolation Forest, LOF, and others.
- **Configuration**: Set independently from other parameters due to its critical role.

ia I									
	NOT SrdlF	**0.0.0.0* AND ru			15-06-01 22:08 🛄 20	125-06-02 22:08 🗰 🔻	UTC_ISO8601 DESC		Destination IP
5	Cocar I	ime x Olici	ine x - source in x - or ce	Sunauon IP X Y Source Port X Q	Destination Port A	otocol x Ze nostnames x		Quick Search	10 V 0-D
•		⊘ View	(Local Time (Local Time)	UTC Time (UTC_ISO8601)	Source IP (SrdP)	(DestiP)	Source Port (SrcPort)	320	
ļ		•	2025-06-02T19:22:26+0000	2025-06-02T19:22:26.658515+00:00	192.168.200.187		64918	240	
		• •	2025-06-02119:22:06+0000	2025-06-02119:22:06:657020+00:00	192.168.200.187	mu 213.149.10.0	64918	160	
			2025-06-02119:20:56+0000	2025-06-02T19:20:56.652216+00:00	192.168.200.187		64918	80	
			2025-06-02T19:20:51+0000	2025-06-02T19:20:51.652026+00:00	192.168.200.187	mu 212.164.64.200	64918		
			2025-06-02T19:20:21+0000	2025-06-02T19:20:21.649613+00:00	192.168.200.187	mu 178.206.203.47	64918	1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1	at the are and a start
			2025-06-02719:20:16+0000	2025-06-02T19:20:16.649418+00:00	192.168.200.187		64918	10.00	रफ्डिय, २३ कि कि कि कि
			2025-06-02T19:20:01+0000	2025-06-02T19:20:01.648349+00:00	192.168.200.187		64918	Field	Count
			2025-06-02719:19:01+0000	2025-06-02T19:19:01.643974+00:00	192.168.200.187	nu 94.140.134.216	64918	92.248.253.54	
			2025-06-02119:16:00+0000	2025-06-02T19:16:00.984588+00:00	192.168.200.187	nu 92.248.253.54	64918		
			2025-06-02719:15:51+0000	2025-06-02T19:15:51.981623+00:00	192.168.200.187	mu 92.248.253.54	64918	90.150.16.137	
			2025-06-02719:15:05+0000	2025-06-02T19:15:05:974920+00:00	192.168.200.187	nu 92.248.253.54	64918	89.151.189.166	
			2025-06-02119:15:01+0000	2025-06-02T19:15:01.972104+00:00	192.168.200.187	nu 92.248.253.54	64918		
			2025-06-02119:14:57+0000	2025-06-02T19:14:57.975884+00:00	192.168.200.187	nu 92.248.253.54	64918		
			2025-06-02T19:14:53+0000	2025-06-02T19:14:53.986651+00:00	192.168.200.187	nu 92.248.253.54	64918		
	Total R	esults: 1.67 K						46.183.128.13	
► et				© 2017 - 2	1025 Nextgen Software SR	L. All rights reserved. Versio	n: 1.1		



Machine Learning Integration

JSON-Based Configuration Files

- Purpose: Allow detailed customization of ML models for different traffic types.
- **Structure**: Each file defines:
 - Model type
 - Parameters (e.g., thresholds, contamination)
 - Voting schemes
 - Feature selection
- Upload/ Edit: Users can upload or modify these files via the UI.

Supported ML Algorithms

NetAlert integrates multiple ML methods from PyOD, Graphomaly and Prophet:

From PyOD:

- **kNN**: Distance-based anomaly detection
- Isolation Forest (IForest): Tree-based isolation of outliers
- COPOD: Copula-based probabilistic outlier detection
- LODA: Lightweight online anomaly detection
- MCD: Minimum Covariance Determinant for robust multivariate outlier detection
- LOF: Local density-based anomaly detection
- HBOS: Histogram-based outlier scoring.

From Graphomaly:

- Autoencoder (AE): Neural network for reconstructing normal behavior
- Variational Autoencoder (VAE): Probabilistic version of AE for uncertainty modeling.

From Prophet:

• **Time-Series Forecasting**: Uses uncertainty intervals to detect deviations in DNS/SMTP traffic patterns



Architecture & Integration

NetAlert is built on a modular Docker Compose architecture, supporting both single-node and distributed deployments. It provides real-time alerting, integrates with SIEM platforms, and is designed to scale based on available hardware resources, with no hardcoded limits on throughput or device count.

Modular Architecture with Docker Compose

- Deployment Modes:
 - **Single-node:** All services run on one host.
 - **Distributed**: Services (e.g., capture, ML, UI) can be deployed across multiple nodes.
- Technology: Uses Docker Compose to orchestrate containers.
- Benefits:
 - Easy to scale horizontally.
 - Simplified updates and maintenance.
 - Isolation of components (e.g., ML engine, database, frontend).





Architecture & Integration

Real-Time Alerting

- **Mechanism**: Alerts are generated and pushed as soon as anomalies or threats are detected.
- Sources:
 - Signature-based (e.g., Suricata rules)
 - ML-based anomaly detection
 - Behavioral heuristics
- **Delivery**: Alerts can be visualized in the UI or forwarded to external systems.

SIEM Integration

- Purpose: Centralizes alert management and correlation with other security data.
- Supported Formats:
 - Syslog
 - JSON over HTTP(S)
 - Kafka or other message brokers (depending on configuration)
- Use Case: Enables integration with platforms like Splunk, ELK Stack, IBM QRadar, etc.

Performance Scaling

- **Design Principle**: No hardcoded limits on:
 - $\circ~$ Number of monitored devices
 - Events per second (EPS)
- Scalability: Performance is hardware-dependent:
 - More CPU/RAM allows higher throughput.
 - Distributed deployment can handle large-scale environments.

co CYBERQUEST Threat Intelligence

Outsmart every threat proactively. Stay ahead of cyber threats with high-value, relevant and actionable intelligence.



Outsmart every threat - act on real, high-value intelligence tailored to your risk landscape, in real time.

COCYBERQUEST Al Assistant

Smarter data exploration. Empower your SOC team with Al-driven insights. Al Assistant that works, learns & secures by your side.



Ask, learn, act - ignite your SOC team with CQ AI Assistant NOW.



The cybersecurity edge you need. Now.







