CYBERQUEST

Industry-specific Use Cases Scenarios and Unique Advantages

CYBERQUEST provides not just advanced SIEM capabilities but acts as a foundational platform for cybersecurity, uniquely designed to support organizational resilience, regulatory compliance (including DORA compliance) and proactive threat detection across multiple sectors.

Contents

• Agriculture & Food Industry

Key Security Challenges:

- Securing operational technology (OT) and IoT devices critical for modern automated agriculture operations.
- Ensuring continuous regulatory compliance, data integrity, and complete traceability within complex supply-chain ecosystems.

Why CYBERQUEST?

- Provides agentless, deep network visibility (Layer 2 and 3) through **NETALERT**, which is particularly effective in remote or resource-constrained agricultural environments.
- Detects anomalies and security threats in real-time, specifically tailored for monitoring agricultural IoT devices and OT systems.
- Features extensive built-in connectors for straightforward integration with diverse IoT sensors, agricultural machinery, and supply-chain management systems.

Scenario:

A large agricultural enterprise relies heavily on IoT sensors for monitoring soil moisture, temperature, and automated control of machinery across distributed locations. CYBERQUEST identifies unusual communication patterns between these sensors, indicating potential sabotage or unauthorized access attempts. Using *NETALERT*'s agentless monitoring capability, CYBERQUEST quickly pinpoints the exact source of these anomalies within remote farm networks, allowing the security team to proactively mitigate the risk before any disruption or damage can occur.

Unique Advantages:

- Agentless, real-time network monitoring ideal for remote or bandwidth-limited agricultural environments.
- Customized anomaly detection specifically designed for IoT and OT devices used in agriculture.
- Ready-to-use connectors simplifying integration across diverse agricultural equipment, systems, and sensors.

• Banking & Insurance

Key Security Challenges:

- Detecting and preventing sophisticated financial fraud effectively and proactively.
- Ensuring continuous compliance with stringent financial regulations, including DORA and GDPR.

Why CYBERQUEST?

- Provides built-in, out-of-the-box DORA compliance reports (initial, intermediary, and final), offering clear visibility and transparency into the organization's regulatory posture.
- Utilizes advanced User and Entity Behavior Analytics (UEBA) powered by multi-layered AI, significantly improving the accuracy of fraud detection by correlating enriched data from internal systems and specialized anti-fraud platforms.
- Delivers extensive real-time data enrichment and correlation capabilities via over 270 native connectors, seamlessly integrating with existing financial systems and security tools.

Scenario:

A financial services provider faces the dual challenge of meeting the complex requirements of DORA compliance and proactively detecting fraudulent transactions. Leveraging CYBERQUEST, the organization quickly generates comprehensive DORA-compliant reports at every required stage. At the same time, CYBERQUEST 's integrated UEBA module automatically identifies unusual user activities indicative of fraud, correlating data in real-time from internal logs, specialized anti-fraud solutions, and external threat intelligence sources. This swift detection enables proactive intervention, significantly reducing the organization's exposure to fraud and non-compliance risks.

Unique Advantages:

- Immediate generation of detailed, DORA-compliant reports.
- Proactive, highly accurate fraud detection via AI-driven UEBA analytics.
- Seamless integration and data correlation capabilities through numerous built-in connectors.

• Communication & Networking

Key Security Challenges:

- Efficient management and analysis of massive log volumes generated by complex, geographically distributed telecom networks.
- Rapid identification and mitigation of cyber threats to ensure network integrity, service availability, and data privacy.

Why CYBERQUEST?

- Offers comprehensive network visibility through *NETALERT*'s agentless Layer 2 and 3 packet-level inspection, proactively uncovering threats and suspicious activity.
- Delivers lightweight yet powerful data processing optimized for scalability, effectively handling high-throughput telecom environments without excessive resource usage.
- Integrates an advanced correlation engine capable of rapidly correlating security events across network layers, enabling quick detection and response.

Scenario:

A telecommunications provider detects an unusual spike in network traffic indicative of a cyberattack. CYBERQUEST immediately activates *NETALERT*'s agentless Layer 2-3 packet inspection, quickly pinpointing suspicious lateral movements within the network. By correlating real-time event data from multiple network sources, CYBERQUEST provides analysts with clear, actionable context, allowing the security team to swiftly isolate and mitigate the threat, preserving network integrity and avoiding service disruption.

Unique Advantages:

- Immediate, detailed network visibility via agentless Layer 2-3 inspection (*NetAlert*).
- Efficient, lightweight processing suited to telecom's high-volume, distributed environments.
- Real-time, comprehensive event correlation tailored specifically for telecom infrastructure security.

• Education & NGOs

Key Security Challenges:

- Safeguarding personal and academic information of students, faculty, and donors.
- Meeting data protection obligations under regulations such as FERPA and GDPR.

Why CYBERQUEST?

- Provides an intuitive interface and user-friendly dashboards, enabling small or understaffed security teams to manage incidents effectively without deep technical expertise.
- Offers a flexible and affordable licensing model designed to accommodate the limited budgets of educational institutions and nonprofit organizations.
- Includes built-in UEBA that automatically detects unusual account behaviors, helping to identify compromised users and prevent data breaches.

Scenario:
A university observes irregular access to student records during off-hours. CYBERQUEST's UEBA module detects the deviation from normal behavior, flags the compromised faculty account, and alerts the security team. Using predefined incident response workflows, CYBERQUEST helps contain the threat and preserves audit evidence for internal review and regulatory reporting.

Unique Advantages:

- Easy-to-use interface supporting fast, effective incident handling.
- Affordable deployment aligned with the financial realities of schools and NGOs.
- Real-time behavioral analysis (UEBA) for early detection of unauthorized access.

• Healthcare & Hospitals

Key Security Challenges:

- Protecting sensitive patient data while maintaining compliance with healthcare regulations such as HIPAA and GDPR.
- Detecting insider threats and unauthorized access before patient confidentiality is compromised.

Why CYBERQUEST?

- Delivers built-in compliance reporting that simplifies audits and ensures continuous adherence to regulatory standards.
- Leverages integrated UEBA to identify abnormal access patterns and user behaviors in real time, enabling early detection of insider threats.
- Correlates and enriches data from both clinical and administrative systems, offering a unified, real-time view of security activity across the organization.

Scenario:
A hospital notices irregular access to electronic health records (EHRs) outside of standard working hours. CYBERQUEST automatically correlates access logs from EHR and identity management systems, identifying the user involved. Its UEBA engine detects behavioral deviations and triggers automated response playbooks that isolate the account and notify the security team, preventing further unauthorized access and ensuring regulatory compliance.

Unique Advantages:

- Continuous monitoring aligned with HIPAA and GDPR requirements.
- AI-powered UEBA for proactive detection of internal misuse or suspicious activity.
- Seamless data integration from clinical and operational systems for full-spectrum security insight.

• Hospitality & Travel

Key Security Challenges:

- Safeguarding customer payment data and personal information across booking platforms and POS systems.
- Maintaining security and operational consistency across geographically distributed sites with varied infrastructure and connectivity.

Why CYBERQUEST?

- Supports modular, lightweight deployments that can be easily scaled across remote hotel branches or travel offices, regardless of technical constraints.
- Correlates data from transaction systems, reservation platforms, and threat intelligence sources in real time, enabling rapid detection of fraud or misuse.
- Designed with an intuitive interface to ease the burden on local IT teams, ensuring quick adoption and effective day-to-day use.

Scenario:

A multinational hotel chain begins receiving reports of suspicious booking activity from multiple remote locations. CYBERQUEST ingests data from booking systems, payment gateways, and fraud databases, correlating it to detect recurring anomalies. Its UEBA module highlights abnormal user activity tied to fraudulent bookings, triggering an automated response that alerts analysts and blocks the suspicious transactions before financial loss or data compromise occurs.

Unique Advantages:

- Scalable deployment ideal for dispersed hospitality environments.
- Real-time fraud detection through cross-source data correlation and enrichment.
- Intuitive dashboards that streamline response and reduce the need for extensive training.

• Manufacturing

Key Security Challenges:

- Securing critical infrastructure such as Operational Technology (OT), Industrial Control Systems (ICS), and SCADA networks.
- Ensuring production continuity by detecting and containing threats without disrupting industrial processes.

Why CYBERQUEST?

- *NETALERT* provides deep, agentless visibility into OT and ICS environments, allowing continuous monitoring without interfering with sensitive control systems.
- Offers real-time correlation and enrichment across both IT and OT data sources, enabling early detection of threats that span physical and digital infrastructure.
- Optimized for deployment in isolated or air-gapped environments, ensuring full protection even in restricted networks with limited connectivity.

Scenario:
A manufacturing facility notices abnormal behavior in its ICS network. CYBERQUEST, using *NETALERT*, detects unauthorized changes to PLC communication without relying on agents. By correlating data from both OT systems and IT logs, CYBERQUEST provides a complete picture of the threat. The alert is escalated immediately, and automated workflows help isolate the affected systems, preventing operational downtime and minimizing business impact.

Unique Advantages:

- Agentless monitoring purpose-built for OT/ICS environments.
- Unified threat detection across both industrial and corporate systems.
- Secure and effective even in offline or segmented production networks.

• Oil, Gas & Green Energy

Key Security Challenges:

- Protecting critical infrastructure, including SCADA systems and industrial control environments, from cyber threats.
- Maintaining uninterrupted operations while meeting strict compliance requirements specific to the energy sector.

Why CYBERQUEST?

- *NETALERT* provides agentless, real-time Layer 2/3 visibility into sensitive environments without impacting performance—ideal for SCADA and remote field systems.
- Built-in UEBA and threat intelligence modules proactively detect complex attacks, including lateral movement, unauthorized access, and insider threats.
- Features energy-specific correlation rules that enable fast identification and containment of anomalies within production and distribution networks.

Scenario:

A renewable energy operator observes irregular data transfers between SCADA systems and remote wind turbines. CYBERQUEST immediately correlates network telemetry, device logs, and access events using its built-in connectors. *NetAlert* pinpoints an unauthorized device communicating with multiple endpoints. Automated response workflows are triggered, isolating the threat and preserving operational uptime without disrupting active energy production.

Unique Advantages:

- Real-time, agentless monitoring tailored for energy infrastructure.
- Context-rich detection powered by industry-specific correlation logic.
- Minimal operational impact—ideal for always-on, regulation-bound environments.

• Public Sector & Government

Key Security Challenges:

• Ensuring continuous compliance with stringent government security standards (ISO 27001, NIST, NIS2, GDPR).
• Protecting sensitive governmental and citizen data from internal misuse and external cyber threats.
• Detecting and mitigating advanced persistent threats (APT) and sophisticated insider threats.

Why CYBERQUEST?

• Built-in mapping of cyber threats to the MITRE ATT&CK framework allows security teams to quickly understand and counteract advanced threat actor behaviors.
• Out-of-the-box compliance reports for ISO 27001, NIST, NIS2, and GDPR deliver immediate regulatory visibility and simplify ongoing audits.
• Advanced UEBA module proactively identifies anomalous user behaviors and suspicious activities, rapidly mitigating insider threats and unauthorized access attempts.

Scenario:

A government department responsible for managing sensitive citizen records and critical national infrastructure must ensure compliance with NIS2 and GDPR regulations while defending against sophisticated internal and external threats. Utilizing CYBERQUEST, the department instantly accesses detailed, readily available compliance reports for ISO 27001, NIST, NIS2, and GDPR. Simultaneously, CYBERQUEST's integrated UEBA flags an insider account exhibiting unusual data access patterns. The platform maps the activity directly to specific MITRE ATT&CK techniques, triggering automated response playbooks that quickly isolate the compromised account, secure sensitive data, and generate complete audit trails for incident reporting and regulatory transparency.

Unique Advantages:

• Comprehensive built-in reporting for ISO 27001, NIST, NIS2, GDPR, and other governmental standards.
• Immediate mapping of cyber threats to the MITRE ATT&CK framework, enabling rapid detection and remediation of advanced threats.
• Advanced UEBA proactively identifies and mitigates insider threats and anomalous behavior, enhancing security posture and operational trust.
• Automated, auditable incident response workflows streamline compliance and significantly reduce time-to-response.

• Retail & eCommerce

Key Security Challenges:

- Preventing payment fraud and securing customer data across eCommerce platforms.
- Ensuring continuous compliance with industry standards such as PCI DSS and GDPR.

Why CyberQuest?

- Correlates and enriches data from payment systems, transaction logs, and customer activity, enabling accurate and timely fraud detection.
- Includes built-in compliance dashboards that monitor adherence to PCI DSS and GDPR requirements in real time.
- UEBA module identifies subtle behavioral anomalies across users and sessions, strengthening fraud prevention and customer trust.

Scenario:

A retail company detects a pattern of unusual transactions occurring across multiple regions. CYBERQUEST ingests and correlates data from payment processors, cart activity, and user accounts. The UEBA engine flags a series of anomalies linked to automated card testing attacks. Using predefined response playbooks, CYBERQUEST isolates affected sessions and prevents further unauthorized activity—protecting both the retailer's financial assets and customer data.

Unique Advantages:

- Comprehensive visibility and enrichment across all transactional layers.
- AI-driven fraud detection through behavioral analytics (UEBA).
- Real-time compliance tracking with PCI DSS and GDPR.

• Technology

Key Security Challenges:

- Safeguarding intellectual property and securing code repositories, build pipelines, and development assets.
- Monitoring complex, fast-moving environments that span on-premises, cloud, and hybrid infrastructure.

Why CYBERQUEST?

- Supports flexible deployment across on-prem, private cloud, and hybrid setups—adapting easily to evolving tech stacks and infrastructure models.
- Offers deep integration capabilities via 270+ built-in connectors, custom scripts, and API-driven automation—ideal for embedding security into DevSecOps workflows.
- UEBA module proactively detects unusual user activity, helping to prevent insider threats and intellectual property leakage.

Scenario:
A software development company detects anomalies in file access patterns within its source code repositories. CYBERQUEST correlates developer activity across version control systems, cloud storage, and internal chat logs using its built-in integrations. UEBA flags a compromised user account attempting to exfiltrate sensitive code, and automated playbooks lock down access, alert security, and preserve audit trails—protecting proprietary assets from unauthorized disclosure.

Unique Advantages:

- DevSecOps-friendly with native scripting and API integration.
- Proactive IP protection through behavioral analytics and contextual threat detection.
- Unified visibility and correlation across development, infrastructure, and collaboration platforms.

• Transportation & Logistics

Key Security Challenges:

- Monitoring and protecting logistics operations in real time, across fleets, warehouses, and data centers.
- Securing supply chain systems to ensure uninterrupted service and prevent fraud or operational disruptions.

Why CYBERQUEST?

- *NetAlert* provides real-time Layer 2/3 visibility without relying on agents, making it ideal for diverse and mobile logistics environments.
- Correlates data from logistics platforms, ERP systems, and network activity to detect anomalies such as routing manipulation or fraudulent transactions.
- Built on a streamlined architecture that supports high performance and responsiveness even across globally distributed operations.

Scenario:

A logistics provider detects irregularities in shipment routing and order processing. CYBERQUEST correlates data from the company's ERP system, transportation management software, and network traffic. *NETALERT* identifies unauthorized communication with key routing devices, while UEBA flags a user profile exhibiting abnormal access behavior. Automated playbooks isolate the threat, preserving system integrity and preventing delivery delays or data tampering.

Unique Advantages:

- Agentless, real-time visibility into distributed logistics environments.
- Cross-platform correlation between logistics systems and business operations.
- Fast, automated threat response that protects continuity across the supply chain.

Why CYBERQUEST

is more than a SIEM:

CYBERQUEST isn't just another SIEM.

It is comprehensive cybersecurity foundation

uniquely suited for any organization, delivering:

• **Advanced Compliance Readiness (including DORA)** - Built-in reporting simplifies complex regulatory requirements.

• **Extensive Data Correlation & Enrichment** - Over 270 native connectors facilitate comprehensive visibility and proactive threat detection.

• **UEBA & Multi-layered AI** - Enhanced threat detection accuracy reduces false positives and speeds up response times.

• **Agentless Network Visibility (*NETALERT*)** - Delivers real-time visibility into layers 2 and 3, particularly valuable for OT and sensitive environments.

• **Modular & Lightweight Deployment** - Easy to scale, especially suitable for distributed or resource-constrained organizations.

CYBERQUEST sets itself apart as a robust cybersecurity platform that builds resilience, proactively identifies threats, and simplifies regulatory compliance, making it a strategic asset for organizations across diverse industries.