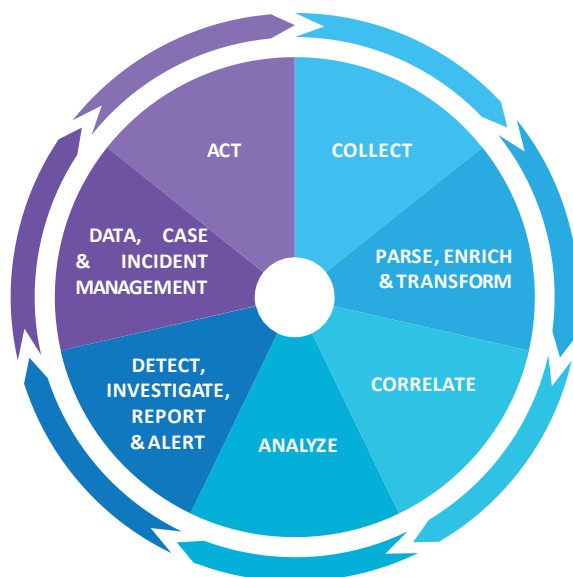


Security-Driven Analytics Platform

In the chaotic security environment, CyberQuest gathers valuable data from multiple technology sources and empowers users to take actionable, critical decisions in real-time.




Technology Follows Real Life

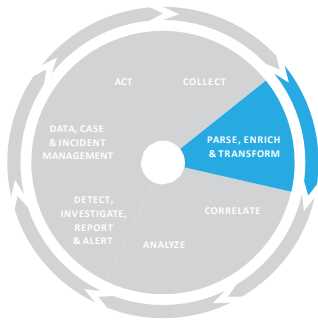
By constantly challenging cross-platform and multi-technology metadata aggregation and correlation, we managed to understand the equation of information overload that our customers are facing and to solve it. CyberQuest is a fast and efficient platform for IT security investigation, with advanced capabilities for monitoring and investigating IT incidents in a highly intuitive graphic environment, with run-time analytics and fast returning reports, essential in real-time combating of fraudulent activities on National Critical Infrastructure and enterprise environments, across industries varying from cyber defence to telecommunications, healthcare, banking or insurance.



Collect

CyberQuest collects and correlates data from the entire infrastructure, from existing SIEM systems, business applications and other security tools, such as vulnerability management solutions, IDS / IPS, Data Loss Prevention tools, Firewalls.

-  **Agents /agentless** data collection
-  **Unify** all security and relevant data sources to quickly correlate / investigate any incident
 - ✓ Business & security applications
 - ✓ SIEMs
 - ✓ Databases
 - ✓ Cloud
-  **Real-time /schedule-based connectivity** to classical SIEM systems for data feeds



CyberQuest intelligently enriches, transforms, manages, correlates and integrates data and adds business intelligence to security data, from Active Directory, business applications or IAM solutions.

- 🔗 **Enrich** events at runtime
- 🔗 **Correlate** events with built-in business centric information (AD, IAM, HR Databases, other relevant data-sources)
- 🔗 **Greater flexibility** by using programmatic based event log parsing / transformation / duplication and decision
- 🔗 **Generate events** based on custom criteria at log parsing runtime
- 🔗 **Allow if-then-else statements** on how to treat events, incidents and security data



Correlate

CyberQuest brings order into chaos by ensuring multiple data-source and platform correlation, regardless of the technology used.

- 🔗 **Get new insight** from multiple custom correlation rules
- 🔗 **Correlate** Network / security with application data / Active Directory / IAM
- 🔗 **Offline or online** data correlation



Analyze

CyberQuest offers one single point of access to security data and makes it available for fraud detection, cybersecurity, internal security or compliance: all in one place, for enhanced decision-making capabilities.

- Quick access to event data: 5 seconds access across billions of events
- Unique drill up / drill down investigative process
- Visual interactive investigations
- Integrate physical security data - access cards, video
- Turbocharge existing data with configurable anomaly detection patterns in network / applications



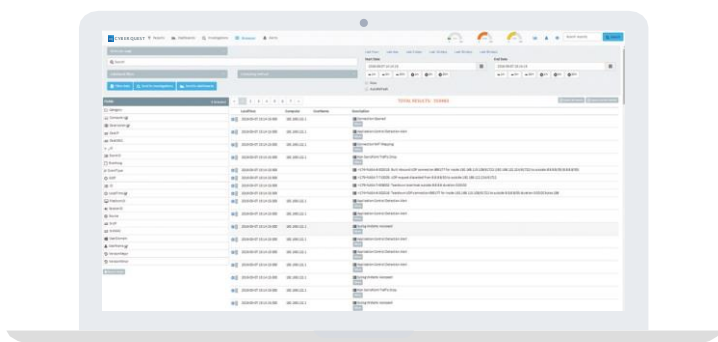
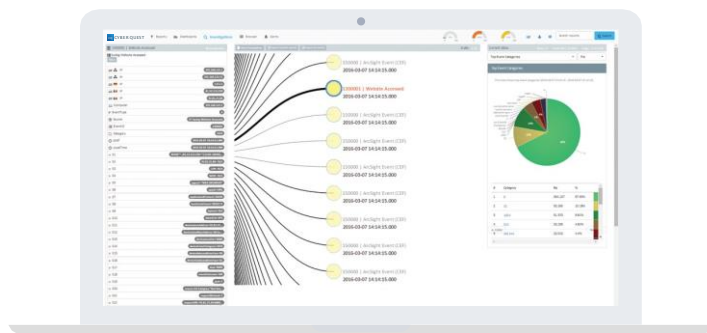
Detect, Investigate, Report & Alert

DETECT INCIDENTS AND ANOMALIES: GET INFORMATION BASED ON USER, IP, COMPUTER

CyberQuest uses latest generation No-SQL database, being able to find related data based on specific criteria in terms of seconds, instead of hours in the case of traditional database technologies.

INVESTIGATE & CORRELATE: USE GRAPHICAL, INTERACTIVE DRILL UPS / DRILL DOWNS

The investigation module presents the audited data using a graphical interface, enabling security investigators to access the correlated view of security information through a single dashboard. Audit trees are context sensitive and contain correlated data based on predefined user criteria.

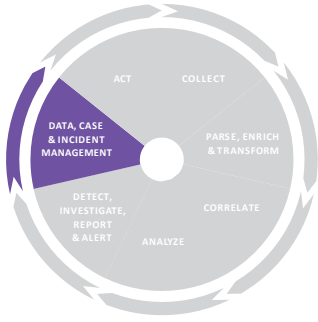


READY-TO-USE TECHNOLOGY & COMPLIANCE REPORTS

CyberQuest's set of predefined, scheduled reports ensure compliance based on internationally recognized standards and frameworks ISO 27001, COBIT, FISMA, HIPPA, PCI/DSS, SOX.





USER-DEFINED OR BUILT-IN REAL-TIME ALERTS: TECHNOLOGY, APPLICATIONS, INCIDENTS, FRAUD

CyberQuest contains an innovative alerting system with user-defined alerts, addressing the most specific security requirements, ensuring great accuracy and minimum false alerts, in order to enable immediate measures.





Data, Case & Incident Management

DATA MANAGEMENT

-  **Ensure non-repudiation**
-  **Archive**, encrypt, compress, digitally sign, leverage existing storage space
-  **Easy scale**, both horizontally and vertically
-  **Distribute** event log data on multiple machines

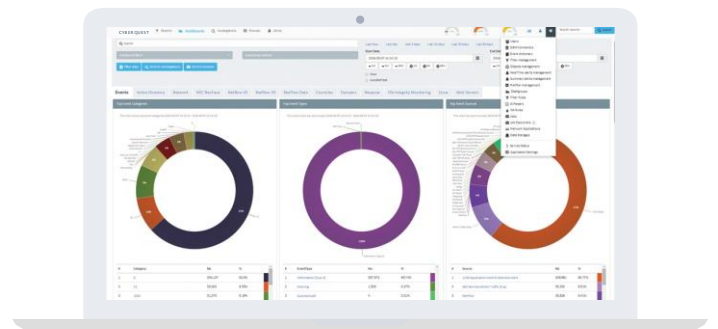
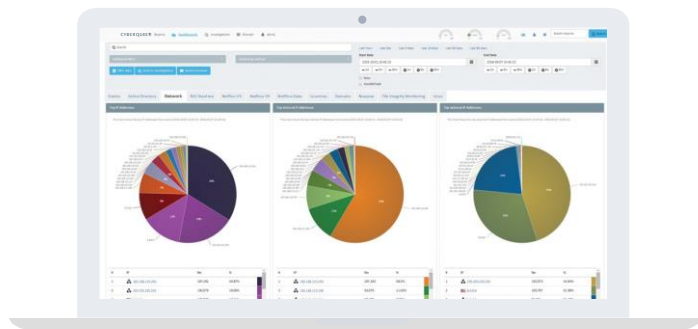
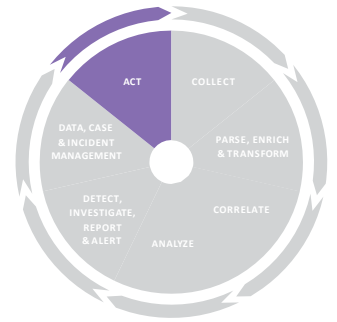
CASE & INCIDENT MANAGEMENT

-  **Manage and collaborate** on incidents and investigation cases
-  **Access** on a 'need-to-know' basis

Act

With CyberQuest's powerful dashboards, you can make rapid, informed decisions and react to alerts, incidents and anomalies in real-time.

Data is quickly sliced and thoroughly organized into multiple categories of information, to offer real-time, context-sensitive overviews. This context can be very simple, from data filtered on just a plain user, machine, IP address or any combination of these, to very complex, based on logical expressions.



About Us

Nextgen Software is an agile European technology company that delivers innovative cybersecurity software solutions based on more than 15 years of worldwide experience in successful implementations with both government and enterprise sectors.

Our solutions ensure full visibility, compliance to international standards and regulations, and powerful analytics that keep your company safe and strong.