CyberQuest în combaterea fenomenului de “Alert Fatigue”

O soluție integrată pentru reducerea volumului de alerte, prioritizarea riscurilor reale și susținerea eficienței operaționale în centrele de securitate moderne.

1. Ce este “Alert Fatigue” și de ce reprezintă o amenințare reală pentru orice organizație?

Alert fatigue descrie starea de epuizare operațională și pierdere a eficienței în echipele de securitate, cauzată **de volumul excesiv de alerte generate de instrumentele de detecție și monitorizare.** În loc să permită reacții rapide și precise, aceste fluxuri de alertare generează confuzie, întârziere și neîncredere în sistemele existente.

■ Simptome operaționale frecvente:

– Mii de alerte pe zi dintr-o singură sursă (ex: endpoint nepatchuit)
– Alerte duplicate sau cu severitate scăzută, care inundă consola analistului
– Timp crescut de răspuns la incidente reale din cauza volumului de zgomot
– Rata mare de ignorare a alertelor valide din lipsă de context sau prioritizare

■ Consecințe pentru organizație:

– Incidente reale pot trece neobservate sau sunt investigate prea târziu
– Analiștii cu experiență își pierd încrederea în sistemele SIEM și devin demotivați
– Escaladări inutile și investigații redundante cresc costurile operaționale
– Lipsa unei reacții rapide afectează conformitatea și expune organizația la riscuri reputaționale și legale

■ Surse tehnice comune ale alert fatigue-ului:

– Agenți EDR/AV care emit zeci de alerte identice pentru aceeași activitate (CrowdStrike, SentinelOne, Defender)
– Scanere de vulnerabilități care notifică repetitiv pentru aceleași riscuri neadresate (Tenable, Qualys)
– Reguli generice și slab optimizate în SIEM-uri tradiționale (Splunk, QRadar, Elastic), care nu integrează scoruri de risc sau corelare între evenimente
– Lipsa unui sistem nativ de deduplicare și agregare a alertelor înainte ca acestea să ajungă în fața analistului

→ Concluzie:

Fără un mecanism de filtrare, corelare și prioritizare integrat direct în pipeline-ul de alertare, organizațiile ajung să transforme un instrument de detecție într-o sursă de blocaj operațional.

2. Unde eșuează soluțiile SIEM tradiționale

Deși platformele SIEM consacrate oferă capacități robuste de colectare, stocare și interogare a datelor, ele nu au fost proiectate inițial pentru a combate suprasarcina generată de alertare excesivă. În lipsa unor mecanisme de optimizare a volumului și relevanței alertelor, aceste soluții ajung adesea să creeze mai multă complexitate decât să aducă eficiență operațională.

■ Limitări operaționale frecvente:

– **Deduplicarea are loc prea târziu**, de obicei doar în momentul în care analistul rulează o interogare manuală în interfață (ex: ***dedup*** în Splunk). Aceasta înseamnă că alertele duplicate sunt deja colectate, procesate și stocate - consumând resurse și atenția echipei.
– **Crearea regulilor este complexă și greu de întreținut**, necesitând limbaje specializate (SPL, Lucene, KQL etc.), ceea ce limitează capacitatea echipelor de a adapta rapid sistemul la scenarii noi de detecție.
– **Lipsa unui motor de corelare nativă între evenimente** înseamnă că fiecare activitate suspectă este tratată izolat, ducând la mii de alerte separate în locul unui incident contextualizat.
– **Fluxurile de tip alertă → incident → investigație sunt fragmentate**, iar gestionarea cazurilor depinde de integrarea cu aplicații externe (ex: SOAR, ServiceNow, Jira), ceea ce introduce latență și pierdere de context.
– **Scalarea vine cu costuri suplimentare de licențiere**, deoarece funcții critice precum corelarea, scoring-ul comportamental sau threat intelligence-ul necesită module plătite separat (ex: Splunk ES, QRadar UBA, Elastic Security).

■ Impact direct în organizație:

– Echipele SOC devin reactive, nu proactive
– Timpul de investigație și răspuns crește, dar în același timp scade încrederea în alerte
– Resursele tehnice sunt consumate pentru gestionarea „zgomotului” în locul riscurilor reale
– Lipsa de integrare a contextului face ca aceeași activitate rău intenționată să fie tratată ca 10 alerte disparate, în loc de un atac coordonat

→ Concluzie:

SIEM-urile tradiționale nu oferă, în configurația lor standard, funcționalitățile necesare pentru a filtra, prioritiza și agrega alertele înainte ca acestea să devină o povară pentru analiști. Fără un mecanism de deduplicare timpurie și corelare contextuală, organizațiile sunt expuse riscului de alert fatigue sistemic, iar investiția într-un SIEM performant poate deveni contraproductivă.

3. Răspunsul strategic al CyberQuest la fenomenul de alert fatigue

CyberQuest abordează fenomenul de alert fatigue nu doar prin filtrare sau reducerea volumului de date, ci printr-o repoziționare a întregului lanț: de la colectare și analiză, până la triere, corelare și gestionare a incidentelor. Arhitectura platformei este construită în jurul ideii de eficiență operațională - pentru ca analiștii să nu fie doar consumatori de alerte, ci coordonatori activi ai răspunsului la incidente.

Pentru fiecare capabilitate-cheie descrisă mai jos, CyberQuest poate fi folosit în două moduri strategice, în funcție de nevoile și maturitatea infrastructurii existente:

- **CQ ca înlocuitor complet de SIEM** - o arhitectură unificată, capabilă să preia rolul principal în colectare, alertare, corelare și gestionare a cazurilor
- **CQ ca strat de tip wrapper** - o suprastructură inteligentă care se conectează la soluțiile existente (Splunk, Elastic, Defender, SentinelOne, CrowdStrike, Tenable etc.), adăugând funcționalități esențiale precum deduplicare, corelare contextuală, prioritizare pe bază de risc și investigare unificată

Această flexibilitate face ca CyberQuest să poată fi adoptat gradual, fără presiunea unui proiect disruptiv de tip „rip and replace", dar cu rezultate tangibile încă din fazele de pilot.

3.1 Deduplicare în timp real la ingestie

Ce face CyberQuest:

CyberQuest permite definirea deduplicării direct în logica de generare a alertelor - per tip de alertă, pe baza unor câmpuri specificate de utilizator („Deduplicate on") și a unui interval de timp configurabil. Astfel, dacă mai multe alerte identice (ex: același **user** cu același **EventID** într-un interval de 60 de secunde) apar într-un interval definit, acestea nu vor genera notificări separate, ci vor fi consolidate într-un singur eveniment.

Sistemul actualizează automat atribute precum:

- ***`LastSeen`*** **:** ora ultimei apariții a aceleiași alerte
- ***`DuplicateCount`*** **:** contorul de apariții repetate

Mai mult, CQ permite și **deduplicare manuală** a alertelor din interfață, în cadrul investigațiilor - oferind flexibilitate completă în analiză.

Mod de utilizare	3.1 Cum ajută concret CyberQuest in funcție de tipul deploymentului
Înlocuitor SIEM	Deduplicarea se aplică direct în motorul de alertare, eliminând necesitatea aplicării ulterioare de filtre sau comenzi ***dedup***, ca în Splunk sau Elastic
Wrapper	CQ preia alerte din surse externe (ex: Splunk, Microsoft Defender, SentinelOne, Elastic etc.), aplică deduplicare automată și le prezintă analistului într-o formă deja consolidată

➤ Impact operațional:

– Se reduce semnificativ volumul de alerte prezentate în interfață
– Se evită "alert storm"-urile cauzate de endpointuri nepatchuite sau surse zgomotoase
– Analiștii au acces imediat la un context consolidat: când a apărut prima dată, cât de des, și cât timp a persistat evenimentul

3.2 Corelarea alertelor și reducerea volumului

Ce face CyberQuest:

CyberQuest include un **motor de corelare nativ**, activ încă din primele ediții comerciale, capabil să lege între ele evenimente disparate și să le transforme într-un singur incident contextualizat. Cu **sute de reguli de corelare predefinite**, platforma este pregătită să detecteze scenarii complexe, precum:

- Brute-force login urmat de logon reușit din aceeași sursă
- Crearea unui cont administrativ + modificare GPO + activitate de rețea anormală
- Evenimente din endpoint + date din rețea + acțiuni în Active Directory

Regulile de corelare pot fi definite de utilizator și permit:

- Setarea de **ferestre temporale** (ex: corelează evenimente în interval de 5 minute)
- Definirea de **pivot fields** (ex: IP, hostname, user)
- Utilizarea de **condiții numerice** (ex: >3 evenimente într-o fereastră)
- Corelare cu **date istorice** (ex: activitate anterioară pe o adresă IP)

Mod de utilizare	3.2 Cum ajută concret CyberQuest in funcție de tipul deploymentului
Înlocuitor SIEM	CQ înlocuiește modulele de corelare avansată (ex: Splunk ES, QRadar Use Case Manager) cu un engine integrat și ușor de configurat
Wrapper	CQ aplică logică de corelare peste evenimente colectate din alte platforme (ex: Splunk, Sentinel, Elastic, SecureX), generând incidente unitare cu context complet

➤ **Impact operațional:**

– Se evită tratarea fiecărui eveniment ca alertă separată
– Se creează o **viziune narativă** asupra atacului: ce s-a întâmplat, în ce ordine, și cine e implicat
– Analiștii se pot concentra pe **lanțul tactic**, nu pe zgomotul individual al fiecărei reguli

3.3 Alerte agregate și prevenirea „alert flood-urilor"

Ce face CyberQuest:

CyberQuest oferă un mecanism de alertare agregată de tip **Summary Alerts**, care analizează periodic rezultatele unor rapoarte definite de utilizator. Aceste alerte se bazează pe statistici aplicate pe evenimente istorice (ex: `count`, `sum`, `average`) și sunt declanșate **doar atunci când se depășesc anumite praguri definite** de analist (ex: număr de evenimente, valori maxime etc.).

Acestea nu sunt alerte generate în timp real, ci reprezintă o componentă **complementară** alertării clasice - oferind vizibilitate asupra comportamentelor recurente sau volumetrice. Sistemul permite alegerea câmpurilor pe care se face agregarea (SummaryOn Level 1, Level 2 etc.), setarea intervalului temporal și definirea unui Threshold pentru declanșare.

Exemplu aplicat: – Alertă dacă un utilizator eșuează autentificarea de **mai mult de 50 de ori** într-o zi (bazat pe EventID 4625 din raportul Windows Security Log)

Mod de utilizare	3.3 Cum ajută concret CyberQuest in funcție de tipul deploymentului
Înlocuitor SIEM	Permite definirea alertelor agregate fără scripting sau cron jobs externe, oferind detecție retrospectivă bazată pe volum
Wrapper	Rulează peste date colectate din alte surse (ex: scanere de vulnerabilități, EDR-uri, AD logs), generând alerte doar dacă pragurile configurate sunt depășite

➤ **Impact operațional:**

– Reduce semnificativ volumul de alerte inutile cauzate de comportamente repetitive dar necritice
– Permite analiză **cantitativă și istorică** a anomaliilor fără a bloca consola SOC cu evenimente individuale
– Crește valoarea investigațiilor prin scoaterea în evidență a abaterilor de la comportamentele normale

3.4 Prioritizarea alertelor pe bază de risc cu ajutorul UEBA

Ce face CyberQuest:

CyberQuest include un modul dedicat de **UEBA (User and Entity Behavior Analytics)** care evaluează comportamentul utilizatorilor și al entităților tehnice (ex: calculatoare, adrese IP, procese) în baza unor **tipare predefinite de detecție**. Fiecărui eveniment i se poate atribui un **scor de risc**, calculat pe baza severității, frecvenței și deviației de la comportamentele obișnuite.

Interfața UEBA oferă:

- vizualizări pentru utilizatori și sisteme cu cele mai multe abateri de risc
- timeline-uri cu scoruri de risc în evoluție
- topul alertelor riscante și grupări pe culori (verde = benign, galben = mediu, roșu = critic)
- filtrare rapidă pe intervale temporale (azi, ieri, săptămâna trecută)

Aceste scoruri pot fi utilizate direct în procesul de analiză pentru a **filtra sau prioritiza alertele** relevante în funcție de contextul real de risc.

Mod de utilizare	3.4 Cum ajută concret CyberQuest in funcție de tipul deploymentului
Înlocuitor SIEM	Oferă scoring comportamental nativ, fără a fi nevoie de module UEBA externe costisitoare (ex: QRadar UEBA, Splunk UBA)
Wrapper	Adaugă scoruri de risc peste alerte colectate din alte soluții (ex: Cortex XDR, Microsoft Defender, Trellix), facilitând trierea în SOC

➤ Impact operațional:

– Permite prioritizarea inteligentă a alertelor, bazată pe comportament și istoric, nu doar pe reguli statice
– Reduce timpul pierdut pe investigații false-pozitive
– Oferă o imagine dinamică a riscurilor la nivel de entitate (user sau mașină), utilă atât în triere, cât și în post-incident review

3.5 Fluxul unificat: de la alertă la caz, într-o singură interfață

Ce face CyberQuest:

CyberQuest integrează un sistem complet de **case management**, care le permite analiștilor să transforme instantaneu o alertă într-un **caz de investigație**. Fiecare caz conține:

- cronologie automată a evenimentelor asociate
- notițe și acțiuni documentate
- etichete personalizabile (tags)
- scoruri de risc în evoluție
- dovezi atașate și trasabilitate completă

Totul este gestionat **în interiorul platformei**, fără a fi necesară integrarea cu SOAR-uri externe sau sisteme ITSM. Acest lucru reduce timpul de răspuns, menține contextul tehnic și elimină întreruperile de flux între detecție, analiză și escalare.

Mod de utilizare	3.5 Cum ajută concret CyberQuest in funcție de tipul deploymentului
Înlocuitor SIEM	Înlocuiește complet nevoia de platforme externe de investigare sau SOAR-uri (ex: Splunk Phantom, ServiceNow SecOps)
Wrapper	CQ acționează ca un **plan de triere centralizat**, indiferent de sursa alertelor (Splunk, Sentinel, Cortex XDR etc.), unificând analiza într-o singură interfață

4. Scenariu de integrare: CyberQuest + orice ecosistem existent

CyberQuest este construit ca o platformă agnostică și extensibilă, capabilă să se integreze atât în infrastructuri existente cât și să le înlocuiască gradual. Prin suportul pentru colectare multi-protocol (API, syslog, ODBC, fișiere, agenți), CQ poate funcționa fie ca motor principal de detecție și analiză, fie ca strat de optimizare peste tool-uri deja implementate.

Această flexibilitate face posibilă o abordare de tip wrapper inteligent, unde CyberQuest preia datele deja procesate de alte soluții și le transformă în alertare contextuală, corelată, deduplicată și prioritizată comportamental.

■ Exemple concrete de integrare:

– CQ colectează alerte brute din Splunk, SentinelOne, Elastic sau Defender ATP, le deduplicatează în timp real, și le grupează într-un singur incident prioritar

– CQ primește evenimente syslog din Tenable, Rapid7 sau OpenVAS și aplică Summary Alerts pe baza rapoartelor periodice configurate, reducând flood-ul de notificări

– CQ preia jurnale din surse IAM (Active Directory, Okta) și le corelează cu evenimente din rețea și endpoint, construind o imagine completă a unui incident lateral

– CQ îmbogățește fiecare alertă cu scoruri UEBA pe entitate, astfel încât trierea și escaladarea să țină cont de risc real, nu doar de severitate statică

■ Canalizare și standardizare date:

– Acceptă input de la majoritatea soluțiilor comerciale și open-source

– Normalizează structuri diferite în schema proprie, fără cerințe de parsing extern

– Permite extragerea automată de metadate relevante pentru deduplicare, corelare și scorificare comportamentală

➤ Beneficii:

– Se pot păstra soluțiile existente (SIEM, EDR, scanere) fără pierderi investiționale

– Se obține o platformă centrală de triere și investigație, cu avantajele unei arhitecturi moderne

– Se reduce volumul și zgomotul fără refactorizare de reguli în produsele de bază

5. Beneficii operaționale în ambele scenarii

CyberQuest aduce valoare directă atât atunci când este implementat ca soluție principală (SIEM replacement), cât și atunci când este folosit ca strat suplimentar (tip smart wrapper) peste instrumentele deja existente. Această flexibilitate permite organizațiilor să adopte o strategie graduală de optimizare, fără a perturba procesele existente sau a înlocui componente critice dintr-o dată.

Beneficiu	CyberQuest ca Înlocuitor	CyberQuest ca Wrapper
Reducerea volumului de alerte	✓ Filtrare și deduplicare la sursă	✓ Deduplicare pe fluxuri externe
Prioritizarea bazată pe risc (UEBA)	✓ Scoring comportamental nativ	✓ Enrich peste alerte existente
Corelare contextuală între surse	✓ Cross-domain, în timp real	✓ Suprascrie logica limitată a altor soluții

Flux unificat alertă → caz	✓ Nativ, fără SOAR extern	✓ Centralizează răspunsul din surse multiple
Reducerea dependenței de produse terțe	✓ Nu necesită Phantom, ServiceNow, etc.	⚠ Poate coexista cu ele
Economii de licențiere și scalare	✓ Cost unic, toate funcțiile incluse	⚠ Costurile rămân în ecosistemul existent
Menținerea investițiilor curente	❌ Înlocuiește total actualul SIEM	✓ Retenție completă a infrastructurii

➤ Observație strategică:

Adoptarea modelului „wrapper" este ideală pentru organizațiile care doresc o evaluare inițială a beneficiilor CyberQuest fără a face schimbări disruptive. Ulterior, pe măsură ce eficiența este demonstrată, tranziția completă către CQ ca platformă principală se poate face incremental.

6. Concluzie: flexibil prin design

CyberQuest oferă un răspuns coerent și complet la una dintre cele mai mari provocări ale centrelor de securitate moderne: **suprasaturarea cu alerte nerelevante și pierderea focusului analitic**. Prin deduplicare timpurie, corelare contextuală, scorificare comportamentală (UEBA) și gestionare nativă a cazurilor, CQ transformă haosul operațional într-un proces clar, prioritar și acționabil.

Indiferent dacă este adoptat ca platformă principală sau ca suprastructură peste soluțiile existente, CyberQuest livrează valoare imediată:

- reduce zgomotul inutil
- concentrează atenția pe incidente reale
- accelerează investigațiile
- elimină dependența de module externe scumpe
- oferă vizibilitate unificată asupra riscului

Dar ceea ce diferențiază cu adevărat CyberQuest este arhitectura sa:

- o platformă **modulară, ultra-lean**, apropiată de microservicii, ce permite scalare fină și disponibilitate ridicată
- peste **270 de conectori nativi** pentru infrastructuri cloud (AWS, Azure, GCP), baze de date, servere, aplicații și dispozitive
- **timp de reacție redus** și **fiabilitate ridicată** inclusiv în rețele distribuite sau izolate (air-gapped)
- suport pentru ingestie prin orice canal - API, Syslog, agent, ODBC, fișiere - fără a necesita parsing suplimentar

Această **flexibilitate arhitecturală** permite adoptarea progresivă fără riscuri: organizațiile pot păstra ecosistemul curent (Splunk, Sentinel, Elastic, CrowdStrike etc.) și pot testa valoarea adăugată reală a CyberQuest în paralel. Iar dacă eficiența este demonstrată, tranziția completă poate deveni o alegere naturală - nu un risc impus.

CyberQuest clarifică. Prioritizează. Susține echipele de securitate.

- ✓ **Oferă o imagine unificată asupra riscurilor**, nu o listă de semnale disparate.
- ✓ **Degrevează analiștii de zgomotul operațional** și le oferă context.
- ✓ **Se adaptează arhitecturii existente**, reducând complexitatea.
- ✓ **Crește performanța operațională prin triere inteligentă,** investigații rapide și fluxuri clare.