

Net++

GOLDEN EYE



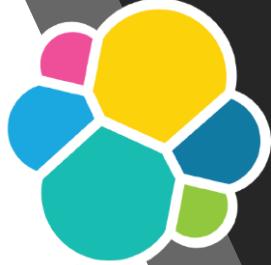
Šta je “Golden Eye”?

James Bond?

ili

Net++ technology ideja/proizvod/inicijativa za veću vidljivost radi poboljšanja IT sigurnosti/bezbednosti i zaštite sistema?

Golden Eye platforma



- ELK stack
- Modularna/docker
- Skalabilna
- Distribuirana, klasterizovana
- Laka vizualizacija prikupljenih podataka
- Lako pretraživanje

Logovi...

- Svi sakupljaju logove – dnevnike događaja – Windows events, mrežni uređaji, firewall uređaji, antivirus logovi, mail logovi... more ili šuma podataka...
- Neki koriste SIEM kako bi povezali događaje i kreirali incidente...
- Neki moraju, radi usklađenosti sa propisima...
- **Koliko vas ih je zapravo pretraživalo?**



Kako u šumi pronaći iglu?

- Logovi sadrže koriste informacije, ali su često sakrivene među milionima manje korisnih
- Kako povezati logove sa različitim sistema?
- Šta ako nam treba novi izveštaj, novi način povezivanja – a vaš SIEM ga ne podržava?
- Novi format logova – uređaja – da li ga vaš SIEM prepoznaće?
- Kako pretražujete sve te logove i događaje?
- Da li i dalje koristite Excel?
- Kako izgledaju izveštaji? KPI?



Želite lepe, pregledne izveštaje?

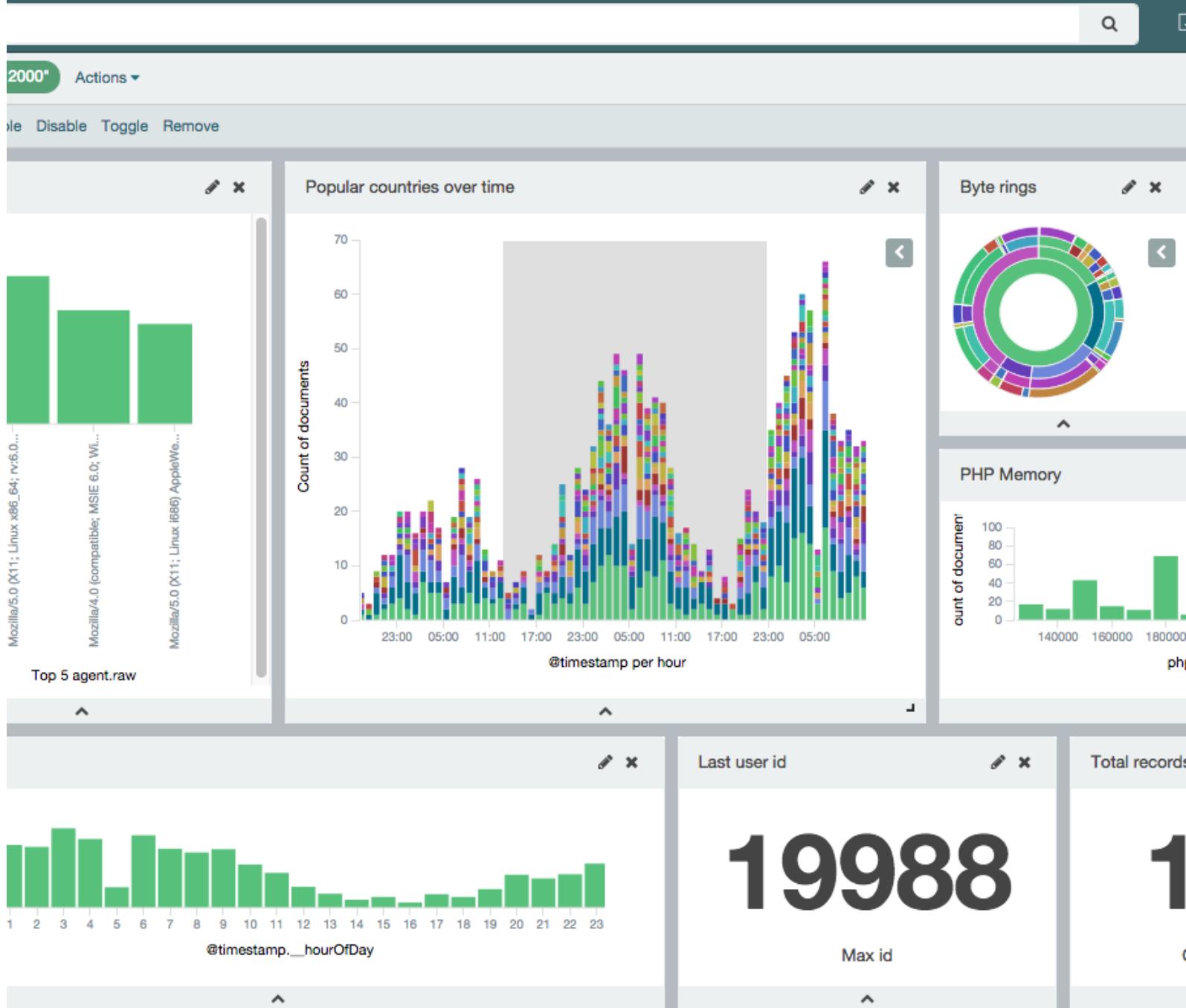


- Umesto Excel tabela želite da izveštaj vidite odmah?
- Želite da se podaci prikažu grafički, umesto niza redova sa teško razumljivim sadržajem?
- Želite da povežete različite izvore podataka i generišete zajedničke izveštaje?
- Želite da definišete i pratite sopstvene KPI?
- Želite da u svakom trenutku imate uvid u usklađenost sa regulativom (NBS, PCI DSS, CIS...)?



Demo time

- Pogledajmo šta sve možemo sa ELK platformom...
- PAN firewall logovi, Windows, Apache...



Šta nas čeka...

NetPP mini SOC – **Golden Eye**

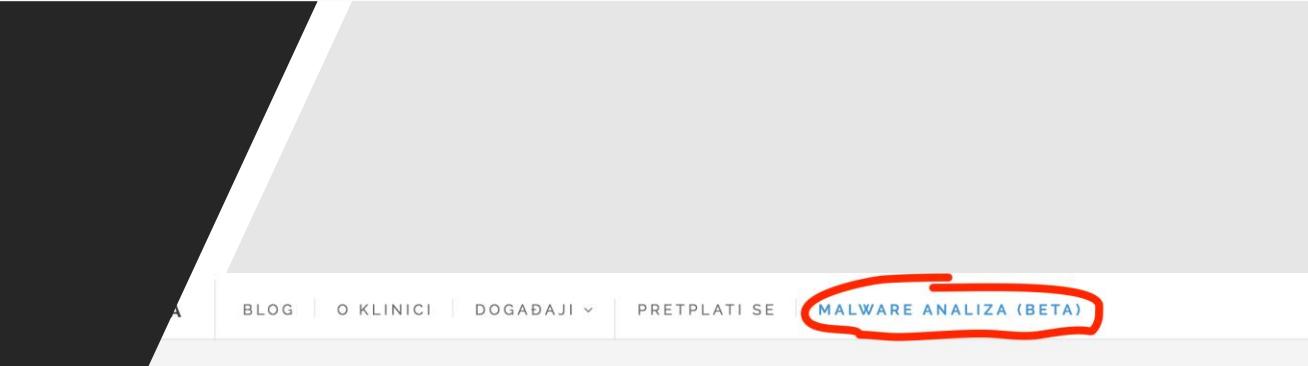
- Symantec Endpoint Protection
- Cisco ASA
- ... i ostali uređaji i rešenja
- Incident Response
- **mini SOC** (on premise ili cloud)



Malware analiza – IT klinika

Sajt IT klinike ide korak dalje
– nudimo analizu malware-a

- u saradnji sa VirusTotal servisom
- kroz "detonaciju" u sandbox-u za nove pretnje
- detaljni izveštaji za nove pretnje
- liste MD5/SHA hesh-eva



The image shows two screenshots of the IT Klinika website. The top screenshot displays the main navigation bar with a red circle highlighting the 'MALWARE ANALIZA (BETA)' link. The bottom screenshot shows the 'MALWARE ANALIZA (BETA)' page itself, which features a large red spider icon centered on a target-like background with binary code patterns.

Demo time

- Malware analiza...

POŠALJITE FAJL NA MALWARE ANALIZU

Izaberite fajlove (maksimalno 5) koje želite da pošaljete na analizu. Fajlovi mogu biti i komprimovani (.zip). Nakon slanja fajlova na analizu, prikazuju se rezultati osnovne analize (da je fajl prepoznat kao malware ili ne, za šta se koristi [VirusTotal](#) servis), a ukoliko je potrebno fajl se šalje dalje na "detonaciju" tj. izvršavanje i na osnovu njegovog ponašanja donosi se izveštaj da li je fajl malware ili ne. Ukoliko ostavite vaš email, detaljan izveštaj se šalje emailom nakon "detoniranja" i analize.

EMAIL

Unesite vašu email adresu (opciono)

UPLOAD FAJLOVA

Drop your files here or **click in this area**

CAPTCHA *

I'm not a robot

reCAPTCHA
Privacy - Terms

POŠALJI NA ANALIZU

RESET



Šta nas još čeka...
EDUKACIJA!!!



- Povećanje svesti o IT bezbednosti – kursevi
 - Borba protiv fišinga – obuke, alati
 - IT Security – kursevi
 - CISSP obuka

Obuka za sticanje CISSP® sertifikacije



Šta je CISSP sertifikat

- CISSP (Certified Information Systems Security Professional) sertifikat je:
 - Najcenjeniji međunarodno priznati sertifikat na polju bezbednosti
 - Osmišljen od strane neprofitne organizacije (ISC)², nezavisan od proizvođača opreme i rešenja
 - Potvrda znanja kvalifikovanog profesionalca obučenog da stručno projektuje, izgradi i održava bezbedno poslovno okruženje



Certified Information
Systems Security Professional

Šta dobijate sa CISSP sertifikatom:



- Ozvaničujete Vašu stručnost dobijenu kroz godine iskustva i rada u oblasti informacione bezbednosti
- Prikazujete svoje tehničko znanje, veštine i sposobnost da efikasno razvijete sveobuhvatno bezbednosno rešenje po globalno prihvaćenim standardima
- Izdvajate se u odnosu na ostale kandidate prilikom apliciranja za željeni posao na brzo rastućem tržištu informacione bezbednosti
- Naglašavate svoju posvećenost profesiji i značaju bezbednosti stalnim profesionalnim usavršavanjem i upoznavanjem s aktuelnim najboljim praksama
- Dobijate pristup resursima vrednim za vašu karijeru, kao što je povezivanje i razmena ideja sa drugim CISSP profesionalcima



Certified Information
Systems Security Professional

Testira se stručnost u domenima:



- Security and Risk Management
- Asset Security
- Security Engineering
- Communications and Network Security
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- Software Development Security



CISSP obuka u Beogradu

- 19-23. decembar - u preduzeću Net++ technology
 - jedini zvanični CISSP kurs, ovlašćen od strane ISC2 i izvođen od ISC2 Official Training Provider-a,
 - sa ovlašćenim međunarodnim predavačem,
 - polaznici dobijaju originalne ISC2 trening materijale,
 - polaznici mogu da nadograde CISSP u pravcu specijalizacije na HCISPP – “HealthCare Information Security and Privacy Practitioner”,
 - stručni predavač s velikim iskustvom,
 - priprema za polaganje ispita
- Popust za prijave do 9. decembra



HVALA

Pitanja?



Net++
TECHNOLOGY