ELISA

Security Manager

novicom

Narzędzie do przechwytywania i ewaluacji zdarzeń cyberbezpieczeństwa

Novicom ELISA Security Manager to solidne i optymalne kosztowo rozwiązanie do gromadzenia, korelacji i analizy logów. System zapewnia wysoki poziom analizy wykrytych incydentów bezpieczeństwa i istotnych logów.

Interfejsem użytkownika jest przeglądarka internetowa. Sposób przeszukiwania bazy danych jest zbliżony do korzystania z wyszukiwarki internetowej. Nawet niedoświadczony użytkownik, po krótkim szkoleniu, będzie w stanie skonfigurować zaawansowane filtry. Narzędzie ELISA pierwotnie zostało opracowane jako **system zarządzania logami, który stopniowo rozszerzono do bardziej złożonego narzędzia typu SIEM.**

Novicom ELISA Security Manager posiada również funkcjonalność zaawansowanych korelacji kontekstowych w kilkumiesięcznym interwale czasowym. Gwarantuje to **wykrywanie zdarzeń cyberbezpieczeństwa** nie tylko poprzez pojedyncze incydenty, ale także np. rozprzestrzenianie się ukrytego malware'a czy logowanie użytkowników do aplikacji po kilku tygodniach bezczynności.

ELISA wzbogaca informację o wykrytym zdarzeniu o informacje ze źródeł zewnętrznych i oblicza "ocenę ryzyka" dla wszystkich zdarzeń, umożliwiając łatwe ustalenie priorytetyzacji działań dla rozwiązywania pojawiających się alarmów. ELISA obejmuje wsparcie regularnego monitorowania konfiguracji (tzw. Change Auditor) i innych zaawansowanych funkcji SIEM.

Jakie m.in. informacje może odkryć ELISA security manager?

Przegląd właściwości i możliwości narzędzia

ELISA

ALARMOWANIE
O BŁĘDACH APLIKACJI LUB SYSTEMU

- **ZAAWANSOWANA OCENA KORELACJI**
  - Wykrywanie cyber incydentów
  - Ograniczanie alarmów false-positive
- **KONKRETNE BŁĘDY**
  - Bardziej elastyczny niż konwencjonalny monitoring (Nagios, Zabbix,...)
- **PRZEJRZYSTOŚĆ**
  - Tłumaczenie błędów kodu
  - Tłumaczenie adresów IP na nazwy DNS

MONITORING
BEZPIECZEŃSTWA

- **CENTRALNA KONSOLA ALARMOWA**
  - System antywirusowy
  - System ochrony przed włamaniami (IPS)
  - System ochrony przed wyciekami danych (DLP)
- **ANALIZA WPŁYWU**
  - Komu dostarczono zainfekowany załącznik e-mail?
  - Które stacje wykazują objawy infekcji wirusowej?
  - Które konta użytkowników zostały skompromitowane podczas ataku ?

MONITORING
OPERACYJNY

- **ZINTEGROWANY SYSTEM ZABBIX**
  - Graficzne zobrazowanie dostępności i ruchu sieciowego
  - W pełni zautomatyzowane monitorowanie infrastruktury VMare
  - Monitorowanie aplikacji internetowych przez użytkownika końcowego
  - Ewaluacja spełnienia umowy SLA przez dostawcę

ANALIZA
RUCHU SIECIOWEGO

- **WEB PROXY**
  - Najczęściej odwiedzane strony
  - Pobierający najwięcej danych
- **SERWER SIECIOWY**
  - Z jakich miast ludzie mają dostęp do systemu?
  - Wykrywanie niedziałających linków na stronie internetowej firmy
- **FIREWALL, ROUTER**
  - Wykrywanie skanowania portów przez atakującego
  - Wykrywanie ataków DoS i DDoS
- **PRZEŁĄCZNIK WEWNĘTRZNY**
  - Które aplikacje najbardziej obciążają sieć?
  - Które urządzenia generują największy ruch w sieci?
  - Kontrola dostępu urządzenia do sieci zgodnie z 802.1x

AUDYT
ZMIAN I DZIAŁAŃ

- **BAZA DANYCH**
  - Kto zmienił numer konta bankowego?
  - Kto przeglądał dane osobowe pracowników?
- **DOKUMENTY I SYSTEM PLIKÓW**
  - Kto usunął doumenty przetargowe?
  - Kto skopiował nietypową liczbę dokumentów?
- **ZMIANY KONFIGURACJI**
  - Elementy sieciowe i urządzenia bezpieczeństwa
  - Usługi katalogowe i systemy operacyjne
  - Aplikacje i bazy danych
- **ZGODNOŚĆ Z NORMAMI**
  - ISO 27001
  - Ustawa o Bezpieczeństwie Cybernetycznym
  - PCI, SOX i więcej

Kluczowe właściwości

- Automatyczna ewaluacja
- Wykrywanie zagrożeń bezpieczeństwa
- Przejrzysty i prosty interfejs użytkownika
- Zgodność z ustawą o cyberbezpieczeństwie, GDPR, ISO, PCI
- Wbudowany Change Auditor
- Więcej zaawansowanych funkcji SIEM
- Integracja z narzędziami do monitorowania i zarządzania siecią
- Urządzenia fizyczne i wirtualne
- Rozproszony system gromadzenia logów
- Skalowalność pozioma
- Wysoka wydajność (do 10 000 EPS)
- Niskie koszty początkowe
- Zaprojektowany z myślą o wykorzystaniu zalet strategii aktywnych SOC

ELISA – zastosowane technologie oraz rozwiązania

Dzięki architekturze ELASTICSEARCH zapewnia błyskawiczne odpowiedzi nawet przy dużych indeksach/bazach danych. Podstawowy widok użytkownika przedstawia histogram z liczbą pasujących zdarzeń w wybranym przedziale czasu oraz tabelą podsumowującą.

Po prawidłowej konfiguracji, rozwiązanie ELISA rejestruje zdarzenia w analitycznej bazie danych w ich oryginalnej formie i strukturze wraz z obsługą znaków diakrytycznych.

Wybierając określone zdarzenie, użytkownicy mogą wykonać przegląd wszystkich jego atrybutów i przeprowadzić analizę typu drill-down.

Wybranie wartości atrybutu umożliwia statystyczny przegląd jego wartości, umożliwiając szybkie filtrowanie (w tym ujemne) zgodnie z podanymi wartościami.

NXLOG to agent **przeznaczony do instalacji w monitorowanych systemach**, który obsługuje przechwytywanie zdarzeń z logów tekstowych, logów zdarzeń systemu Windows, różnych typów logów strukturalnych (CSV, j2log i wiele innych) oraz tabel relacyjnych baz danych.

PODSTAWOWE FUNKCJE NXLOG:

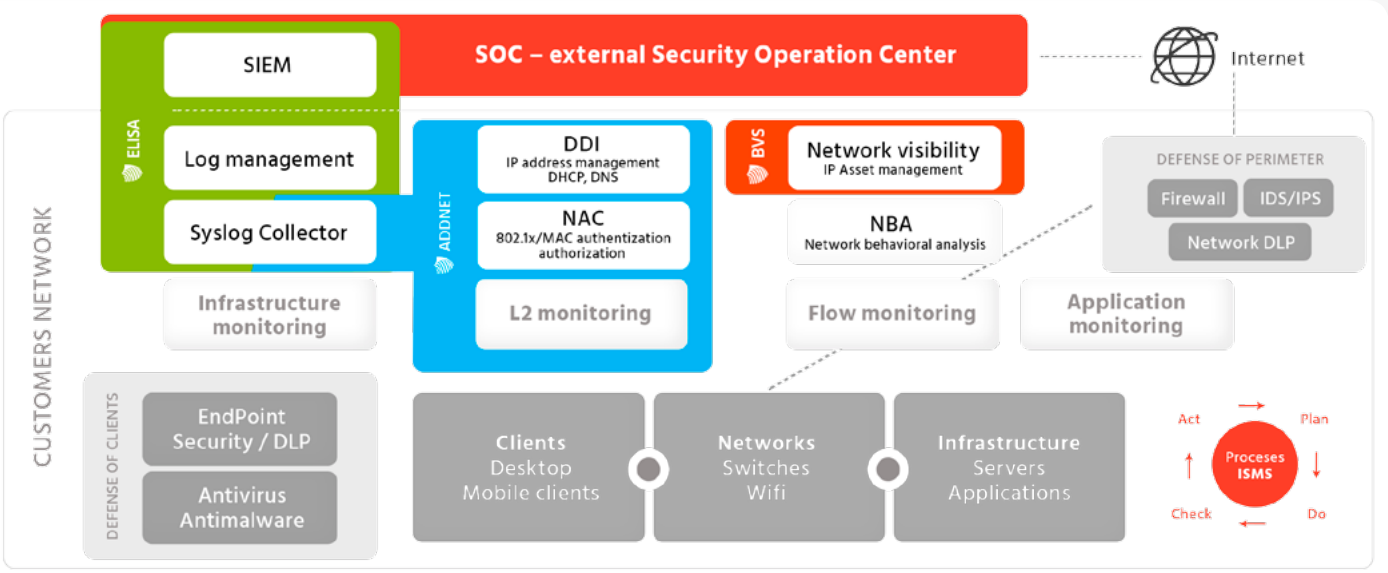
- Wieloplatformowy agent, który jest przyjazny dla zasobów.
- Tworzy bufor zdarzeń, jeżeli centralny system jest niedostępny.
- Zapamiętuje przetworzone zdarzenia nawet po restarcie.
- Obsługuje rotacyjne pliki logów, różne typy kodowania i rekordy wieloliniowe.
- Umożliwia filtrowanie i korelację zdarzeń w monitorowanym systemie.
- Obsługuje przesyłanie uporządkowanych rekordów w formacie binarnym i za pośrednictwem połączeń szyfrowanych (TLS).

Specyfikacja modeli Novicom ELISA w ofercie

Urządzenia fizyczne to **kompletny system Novicom ELISA Security Manager** w postaci wstępnie zainstalowanego fizycznego serwera wraz z pięcioletnim serwisem typu On-Site Next Business Day.

Model	Przepustowość (EPS)	Pojemność dysku	Oszacowanie retencji (połowa EPS)	RAID	Redundantny zasilacz
ESM Appliance XL	10 000	100 TB	12 Miesiące	2 Dyski	Tak
ESM Appliance L	6 000	42 TB	9 Miesiące	2 Dyski	Tak
ESM Appliance M	2 000	12 TB	8 Miesiące	1 Dysk	Tak
ESM Appliance S	1 000	4 TB	3 Miesiące	1 Dysk	Tak

Przepustowość systemu ELISA Security Manager i pojemność centralnego magazynu logów można zwiększyć poprzez skalowanie w poziomie, tj. poprzez zakup dodatkowych urządzeń i instalację klastrową. **Manager jest również dostępny jako urządzenie wirtualne** (VMware, Hyper-V). Przy wystarczającej alokacji zasobów analogiczne przepustowości można uzyskać w środowisku wirtualnym. **Wydajność rozproszonego systemu gromadzenia danych można również zwiększyć przez skalowanie pionowe.**



ELISA i Aktywny SOC

ELISA jest ważną częścią rozwiązania Active SOC (Security Operation Center), którą Novicom wraz ze swoimi partnerami SOC stara się promować na rynku. **ELISA, wraz z rozwiązaniem ADDNET** (do efektywnego zarządzania usługami sieciowymi i kontrolą dostępu do sieci) **oraz rozwiązaniem BVS** (do wizualizacji zasobów sieciowych, w tym ich wpływu na usługi biznesowe) **tworzą unikalne portfolio, które przygotowuje klientów do szybkiego i bezproblemowego połączenia z usługą SOC lub budową własnej tego typu usługi.** Klienci korzystający z tych produktów, mogą w pełni

Novicom ELISA jest doceniana nie tylko przez administratorów bezpieczeństwa lecz również administratorów IT.

korzystać z usług premium Active SOC. **Dzięki temu wybrani operatorzy SOC są w stanie zagwarantować w pełni kwalifikowaną, aktywną reakcję na cyberataki w trybie 24x7 bez koniecznej współpracy z administratorami systemu u klienta.** Jest to całkowicie zgodne z obecnym trendem polegającym na zastosowaniu najwyższego poziomu nadzoru bezpieczeństwa (SOC) jako usługi. **Klient nie musi już ponosić wysokich kosztów** związanych z budową wysoce wyspecjalizowanego zespołu do walki z hakerami oraz zakupu rónego rodzaju technologii.

novicom

Novicom, s.r.o.
Praga, Republika Czeska

www.novicom.eu
sales@novicom.eu

ELISA

NVC PL 2020-09