ELISA

SECURITY MANAGER

Tool zum Abfangen und Auswerten von Cyber-Sicherheitsereignissen

Der Novicom ELISA Security Manager ist eine robuste, leistungsstarke und dennoch sehr kostengünstige Lösung für das Sammeln, Korrelieren und Analysieren von Logs. Das System bietet ein hohes Maß an Komfort bei der Analyse von erkannten Sicherheitsvorfällen und den dazugehörigen Logs.
Die Benutzeroberfläche ist ein Webbrowser. Die Suche in der Datenbank ist vergleichbar mit der Verwendung einer Internet-Suchmaschine. Nach einer kurzen Schulung ist selbst ein unerfahrener Benutzer in der Lage, komplexe Filter zu erstellen. Das ELISA-Tool wurde ursprünglich als Log-Management-System entwickelt, das schrittweise zu einem komplexeren SIEM-Tool ausgebaut wurde.
Novicom ELISA Security Manager nutzt außerdem eine fortschrittliche Korrelations-Engine, die eine kontextbezogene Korrelation auch über mehrere Monate hinweg unterstützt. Dies ermöglicht die Erkennung von Cybersecurity-Ereignissen, nicht nur durch wiederholte elementare Vorfälle, sondern auch durch die Verbreitung von versteckter Malware über ein Netzwerk oder durch Benutzer, die sich nach mehreren Wochen der Inaktivität bei Anwendungen anmelden.
ELISA ermöglicht die Anreicherung der Ereignisse mit Informationen aus externen Quellen und berechnet einen „Risiko-Score" für alle Vorfälle, der es Ihnen ermöglicht, die notwendigen Schritte zur Behebung von Alarmen leicht zu priorisieren. ELISA unterstützt die regelmäßige Überwachung von Konfigurationen (den so genannten Change Auditor) und andere erweiterte SIEM--Funktionen.

Welche Informationen kann die Elisa-Lösung aufdecken?

Übersicht der Funktionsmerkmale:

ELISA

ANWENDUNGS- ODER SYSTEMFEHLER

- **Anspruchsvolle Korrelationsbewertung**
  - Erkennung von Sicherheitsvorfällen
  - Unterdrückung von Fehlalarmen und Benachrichtigungen
- **Spezifische Individuelle Fehler**
  - Flexibler als herkömmliche Leistungsüberwachung (Nagios, Zabbix,...)
- **Verständlichkeit**
  - Übersetzung von Fehlercodes
  - Übersetzung von IP-Adressen in DNS-Namen

SICHERHEITSÜBER-WACHUNG

- **Zentrale Alarmkonsole**
  - Antivirus-System
  - Intrusion Prevention System (IPS)
  - System zur Verhinderung von Datenverlusten (DLP)
- **Wirkungsanalyse**
  - An wen wurde ein infizierter E-Mail-Anhang übermittelt?
  - Welche Stationen weisen Symptome einer Virusinfektion auf?
  - Welche Benutzerkonten wurden während des Angriffs kompromittiert?

BETRIEBSÜBER-WACHUNG

- **Integriert Zabbix System**
  - Grafische Darstellung der Verfügbarkeit und des Netzverkehrs
  - Vollständig automatisierte Überwachung der VMware-Infrastruktur
  - Endbenutzerüberwachung von Webanwendungen
  - Bewertung der SLA-Erfüllung durch den Lieferanten

ANALYSE DES NETZVERKEHRS

- **WEB PROXY**
  - Meistbesuchte Seiten
  - Größte Datenabrufer
- **WEB SERVER**
  - Von welchen Städten aus haben die Menschen Zugang zu diesem System?
  - Erkennung von fehlerhaften Links auf der Unternehmenswebsite
- **FIREWALL, ROUTER**
  - Erkennung von Port-Scans durch einen Angreifer
  - Erkennung von DoS- und DDoS-Angriffen
- **Interner Schalter**
  - Welche Anwendungen belasten das Netz am stärksten?
  - Welche Geräte erzeugen den meisten Netzverkehr?
  - Zugangskontrolle zum Netzwerk 802.1x

PRÜFUNG VON ÄNDERUNGEN UND AKTIVITÄTEN

- **Datenbank**
  - Wer hat die Kontonummer geändert?
  - Wer hat die persönlichen Daten der Mitarbeiter eingesehen?
- **Dokumente & Dateisysteme**
  - Wer hat die Ausschreibungsunterlagen gelöscht?
  - Wer hat eine ungewöhnliche Anzahl von Zeichnungen kopiert?
- **Konfigurationsänderungen**
  - Netzelemente und Sicherheitseinrichtungen
  - Verzeichnisdienste und Betriebssysteme
  - Anwendungen und Datenbanken
- **Einhaltung von Normen (Richtilinien)**
  - ISO 27001
  - Cybersicherheitsgesetz
  - PCI, SOX und mehr

Wichtige Eigenschaften

- Automatische Auswertung
- Erkennung von Sicherheitsrisiken
- Eine klare und einfache Web-Benutzeroberfläche
- Einhaltung des Cybersicherheitsgesetzes, GDPR, ISO, PCI
- Integrierter Change Auditor
- Weitere erweiterte SIEM-Funktionen
- Integration mit Tools für das Netzwerk Überwachung und Verwaltung
- Physische und virtuelle Geräte
- Verteilte Protokollsammlung
- Horizontale Skalierbarkeit
- Hohe Leistung (bis zu 10 000 EPS)
- Niedrige Anfangskosten
- Entwickelt, um die Vorteile der Strategie der aktiven SOC-Vorteile zu nutzen

ELISA

ELISA – verwendete Technologien

Dank seiner Architektur liefert ELASTICSEARCH auch bei großen Indizes/Datenbanken blitzschnelle Antworten. Die grundlegende Benutzeransicht zeigt ein Histogramm mit der Anzahl der übereinstimmenden Ereignisse in einem ausgewählten Zeitintervall und eine seitenweise Tabellenzusammenfassung.
Wenn die ELISA-Lösung richtig konfiguriert ist, werden Ereignisse in der analytischen Datenbank in ihrer ursprünglichen Form und Struktur aufgezeichnet, wobei diakritische Zeichen nahtlos unterstützt werden.
Durch Auswahl eines bestimmten Ereignisses kann der Benutzer eine Übersicht über alle Attribute öffnen und Drilldown-Analysen durchführen.

Die Auswahl eines beliebigen Attributs gibt einen statistischen Überblick über die Verteilung seiner Werte und ermöglicht eine schnelle Filterung (auch negativ) nach einem bestimmten Wert.

NXLOG ist ein Agent, der für die Installation auf überwachten Systemen entwickelt wurde, die nicht in der Lage sind, Log-Einträge selbstständig zu verarbeiten und zu versenden. NXlog unterstützt das Abfangen von Ereignissen aus Textprotokollen, WindowsEreignisprotokollen, verschiedenen Arten von strukturierten Protokollen (CSV, j2log und viele mehr) und relationalen Datenbanktabellen.

HAUPTMERKMALE VON NXLOG

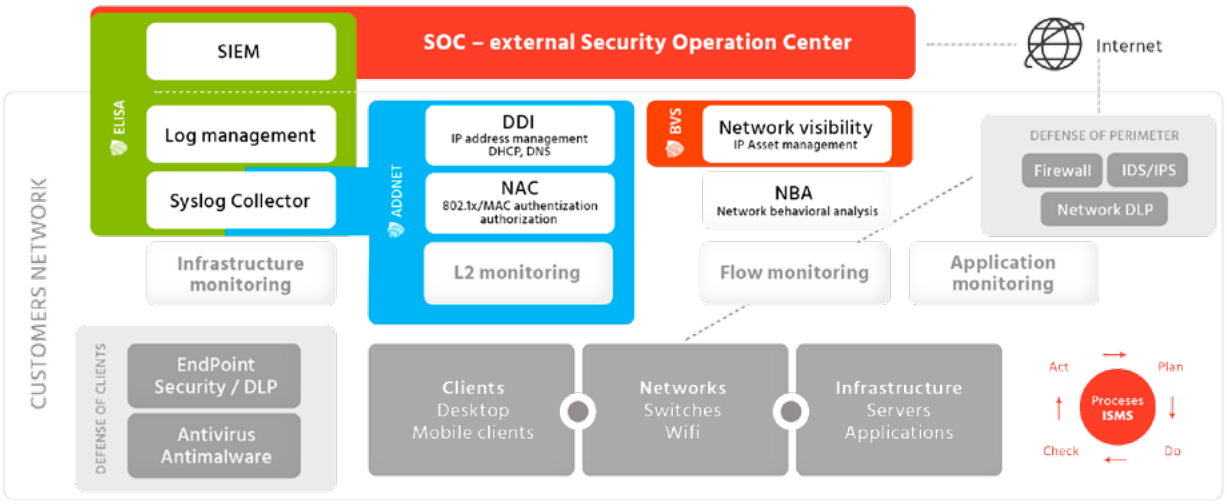
- Multiplattform-Agent, der die Ressourcen schont
- Erzeugt einen Puffer von Ereignissen, wenn das zentrale System nicht verfügbar ist.
- Merkt sich die Position der verarbeiteten Ereignisse auch nach einem Neustart.
- Unterstützt rotierende Protokolldateien, verschiede ne Kodierungsarten und mehrzeilige Datensätze.
- Ermöglicht, die Filterung und Korrelation von Ereignissen im überwachten System.
- Unterstützt die Übertragung von strukturierten Aufzeichnungen in einem binären Format und über verschlüsselte Verbindungen (TLS).

Spezifikationen der von Novicom angebotenen ELISA-Modelle

Physische Appliances sind ein komplettes Novicom ELISA Security Manager System in Form eines vorinstallierten physischen Servers mit „Vor-Ort-Service"-Hardware „am nächsten Arbeitstag" für 5 Jahre.

Model	Thourgput (EPS)	Capacity storage	Retention estimate (half EPS)	Storage resistance (RAID)	Redundant power supply
ESM Appliance XL	10 000	100 TB	12 Monate	2 disks	Ja
ESM Appliance L	6 000	42 TB	9 Monate	2 disks	Ja
ESM Appliance M	2 000	12 TB	8 Monate	1 disk	Ja
ESM Appliance S	1 000	4 TB	3 Monate	1 disk	Ja

Der Leistungsumfang des ELISA Security Manager Systems und die Kapazität des zentralen Logspeichers können durch horizontale Skalierung, d.h. durch den Kauf weiterer Geräte und die Implementierung eines Clusteraufbaus, erhöht werden.
Der Novicom ELISA Security Manager ist auch als virtuelle Appliance (VMware, Hyper-V) verfügbar. Bei Bereitstellung ausreichender Leistungsressourcen können auch in einer virtuellen Umgebung analoge Leistungsdaten erreicht werden. Die Leistung des verteilten Datenerfassungssystems kann auch durch vertikale Skalierung gesteigert werden.



ELISA und aktiver SOC

ELISA ist ein wichtiger Bestandteil der Active SOC (Security Operation Center) -Strategie, die Novicom zusammen mit seinen SOC-Partnern auf dem Markt vorantreiben will. ELISA bildet zusammen mit der ADDNET-Lösung (für effizientes Management von Netzwerkdiensten und Netzwerkzugangskontrolle) und der BVS-Lösung (für die Visualisierung von Netzwerk-Assets, einschließlich ihrer Verbindung zu Business-Services) ein einzigartiges Portfolio, das die Kunden auf eine schnelle und nahtlose Anbindung an den SOC-Service vorbereitet. Kunden, die diese Produktplattform nutzen, können dann die Premium-Dienste von Active SOC in vollem Umfang in Anspruch nehmen.
Dadurch sind ausgewählte SOC-Betreiber in der Lage, eine voll qualifizierte aktive Reaktion auf Cyber-Attacken im 24x7-Modus zu gewährleisten, ohne dass eine Zusammenarbeit mit den Systemadministratoren beim Kunden erforderlich ist. Dies entspricht dem aktuellen Trend, Top Security Survaillance (SOC) als Dienstleistung zu nutzen. Dieser Ansatz beseitigt den wirtschaftlichen Nachteil der Anschaffung einer kompletten Palette von Einzwecktechnologien und die Notwendigkeit, über ein eigenes hochspezialisiertes Team zu verfügen, das jederzeit in der Lage ist, professionellen Hackern zu begegnen.

Novicom ElISA wird nicht nur von Sicherheitsverantwortlichen geschätzt, sondern auch von Administratoren, die für den Systembetrieb zuständig sind.

NOVICOM – CYBER SECURITY & NETWORK MANAGEMENT HAS NEVER BEEN EASIER

novicom

Novicom, s.r.o.
Prag, Tschechische Republik
www.novicom.eu
sales@novicom.eu

ELISA

NVC DE 2022-02