

ESSG® - Enterprise Security Service Grid

User and Entity Behavior Analytics framework

Tipicamente la tecnologia UEBA viene impiegata per identificare le minacce interne alle organizzazioni, monitorando continuamente il comportamento delle entità che le compongono. Sfruttando le tecniche di apprendimento automatico (machine learning, deep learning), vengono continuamente appresi e aggiornati i modelli comportamentali, individuando le divergenze e segnalando immediatamente le entità anomale, come utenti o account compromessi.

UEBA consente di aggredire masse di dati provenienti dai molteplici sistemi di logging propri di ogni organizzazione, individuando tramite modelli comportamentali le reali minacce di attacco ai sistemi informatici e rilevando potenziali vulnerabilità.

Codin, nel proprio prodotto ESSG®, ha esteso il concetto UEBA verticalizzandolo sulle aree di applicazione specifiche del core business dei propri clienti, oltre cioè alla tipica protezione dei sistemi informativi; sviluppando algoritmi proprietari che consentono la modellizzazione di comportamenti provenienti da qualunque sorgente di dati esterna, quali ad esempio satelliti, radar, droni, sensori, telecamere.



www.codin.it



Completa visibilità

ESSG® consente un'accurata e dettagliata visione dei processi, delle infrastrutture e delle relazioni tra utenti in contesti complessi. Il motore euristico di ESSG®, composto da reti neurali e algoritmi topologici/geometrici, permette la modellizzazione e l'analisi in tempo reale di eventi e comportamenti, fornendo una visione globale dell'ambiente monitorato, identificando immediatamente minacce, rischi e riduzione delle performance, fornendo all'utente finale un affidabile sistema di Supporto alle Decisioni.

La piattaforma

ESSG® è un framework per lo sviluppo di soluzioni per analisi comportamentali specifiche per il caso d'uso o infrastruttura da monitorare. ESSG® rileva, per ciascuna entità coinvolta, comportamenti divergenti, considerando il loro impatto potenziale sugli asset, sui processi, sull'intera infrastruttura. Gli algoritmi di apprendimento (Machine Learning e Deep Learning), garantiscono la continua evoluzione del meccanismo di riconoscimento del modello comportamentale mentre gli algoritmi predittivi garantiscono di poter anticipare le criticità e un efficace Supporto alle Decisioni. ESSG® opera in tempo reale e implementa algoritmi tra i quali: Self Organizing Map, Feed Forward/Back Propagation, Persistent Homology, Predictive ANN.

Vantaggi

In scenari complessi, ESSG® consente di identificare ed isolare potenziali fattori critici attraverso l'analisi comportamentale delle entità e dei processi coinvolti nonché delle relazioni esplicite e non che insistono tra le stesse. Anche e soprattutto in ambiti complessi, ESSG fornisce all'utente una visione olistica dei fenomeni osservati. Algoritmi analitici e predittivi, supportano i decisori nell'identificare deviazioni e divergenze rispetto ai comportamenti attesi permettendo di poter individuare le azioni ed i correttivi necessari per prevenire l'occorrenza di una criticità o minimizzarne l'impatto al fine di ridurre tempi e costi di intervento.

I nostri Clienti

ESSG® è stato utilizzato per implementare soluzioni e studi di fattibilità per INPS, Marina Militare Italiane, Leonardo S.p.A., Agenzia Italiana del Farmaco.

USER ENTITY
AND ANALYTICS
BEHAVIOR FRAMEWORK



Le nostre soluzioni

Sicurezza Navale



La soluzione classifica i target sulla base di informazioni comportamentali, ne definisce la classe comportamentale, la confronta con i modelli appresi per identificare comportamenti omogeni e divergenti. La soluzione permette un monitoraggio proattivo per l'identificazione delle potenziali minacce e comportamenti illeciti.

Cyber Sicurezza



La soluzione permette la gestione ed il monitoraggio centralizzato dell'intera infrastruttura IT, inclusi i sistemi e gli strumenti di sicurezza. Analizza il modello di utilizzo delle risorse IT, apprende i modelli comportamentali normali, segnala divergenze ed evidenzia le minacce interne ed esterne. Identifica i rischi, le anomalie e gli scenari critici senza la necessità di conoscenza pregressa. La soluzione mitiga l'impatto di instabilità strutturali identificando potenziali attacchi in corso e vulnerabilità.

Protezione di Infrastrutture Critiche



La soluzione correla informazioni sensoristiche e di processo per identificare comportamenti standard e divergenti; L'aggiornamento continuo delle informazioni, unitamente alla storicizzazione dei guasti e difetti, permette l'individuazione di pattern premonitori di failure e generare allarmi in caso di criticità. Garantisce la possibilità di pianificare gli interventi manutentivi sulla base delle probabilità di guasto indotte da instabilità della infrastruttura.

Monitoraggio nelle Aziende Ospedaliere



La soluzione fornisce il monitoraggio dei trattamenti e delle prescrizioni somministrate ai pazienti da parte del personale medico. La soluzione identifica il modello di comportamento delle entità monitorate: dottori, pazienti, protocolli di trattamento, farmaci. Identifica comportamenti comuni e divergenti e segnala potenziali illeciti.

Analisi del Territori



La soluzione analizza dati di un'area geografica, acquisiti da strumenti di scansione (rilevatori aerei, satelliti ecc.), per estrarre informazioni e fornire analisi in tempo reale di eventi critici attuali o potenziali; in particolare contaminazioni, incendi, rischi idrogeologici, malattie della vegetazione. L'utilizzo della geo localizzazione delle aree da esaminare tramite il Sistema Satellitare di Navigazione Globale garantisce l'identificazione rapida e puntuale delle aree di interesse

Codin S.p.A. è una azienda a capitale italiano di carattere innovativo, attiva da oltre 30 anni, specializzata nello sviluppo, progettazione e implementazione di soluzioni informatiche in ambito "Safety and Security". Codin dispone di una propria unità organizzativa di Ricerca e Sviluppo, certificata CMMI Maturity Level 3, per la standardizzazione e miglioramento continuo dei processi di sviluppo e ingegnerizzazione del Software, che la fa annoverare tra le uniche due PMI certificate in Italia su un totale di sedici aziende (fonte: CMMI Institute-agg.to Nov. 2019). Codin è certificata ISO 27001 e 9001 per la "Progettazione e realizzazione di soluzioni informatiche e di prodotti software". Completano il patrimonio di competenze e professionalità dell'azienda oltre 30 certificazioni tra le quali : PMP, IFPUG 4.3, ITIL v3 foundation. Codin partecipa attivamente a progetti nazionali ed europei, in partnership con primarie entità italiane ed internazionali, per lo sviluppo e realizzazione di progetti innovativi nei principali settori emergenti ICT (Cyber Security, Controllo e Monitoraggio dell'Ambiente). Codin ha adottato un proprio Modello di Organizzazione e di Gestione e Controllo (ex D.lgs.231/2001) e tutti i bilanci civilistici di Codin sono stati certificati da Ernst & Young dal 2012.

Codin è presente a Roma, Taranto e Cosenza con circa 100 tra dipendenti e collaboratori, più della metà dei quali laureati in materie scientifiche.



INNOVATION@WORK

CODIN S.p.A.

Via del Pescaccio, 30
00166 Roma - Italy
Tel. +39 06 661 71 41
Fax +39 06 661 88 640
www.codin.it