BLUDIS
VALUE ADDED DISTRIBUTOR

ManageEngine

Il SIEM ManageEngine: Sicurezza informatica e compliance. Come ottenere visibilità e controllo dell'infrastruttura IT.

ManageEngine **DISTRIBUITED BY** BLUDIS VALUE ADDED DISTRIBUTOR

- SCELTO DA OLTRE 280.000 AZIENDE IN TUTTO IL MONDO
- UTILIZZATO DA 9 SU 10 DELLE SOCIETÀ "FORTUNE 100"
- SCELTO DA OLTRE 3 MILIONI DI AMMINISTRATORI IT
- 15 ANNI DA DISTRIBUTORE UNICO ITALIANO MANAGEENGINE
- 28 ANNI DI ESPERIENZA NEL SETTORE ICT
- NEXT GEN VENDOR DISTRIBUTOR DEL GRUPPO ESPRINET

Il SIEM ManageEngine: sicurezza informatica e compliance. Come ottenere visibilità e controllo dell'infrastruttura IT

Un'adeguata strategia di cybersecurity dovrebbe prevedere il monitoraggio costante degli eventi che si verificano sulla infrastruttura aziendale per rilevare incidenti che indicano potenziali minacce. Per rispondere ad una sfida di questo tipo è necessario individuare prontamente ogni evento sospetto, analizzare nel dettaglio gli incidenti, monitorare applicazioni, sistemi e comportamento degli utenti per anticipare le situazioni critiche che potrebbero verificarsi provocando danni al business dell'azienda.

Nel corso dell'intervento si parlerà dell'importanza di una corretta gestione e risposta agli incidenti di sicurezza e i vantaggi dell'utilizzo di una soluzione SIEM per raggiungere questi obiettivi.

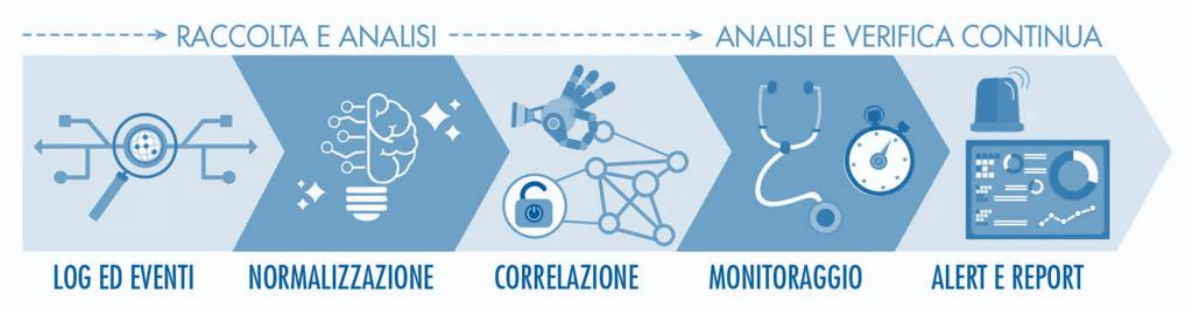
Speaker

Andrea Balestrero
Sales Engineer ManageEngine

BLUDIS
VALUE ADDED DISTRIBUTOR

ManageEngine

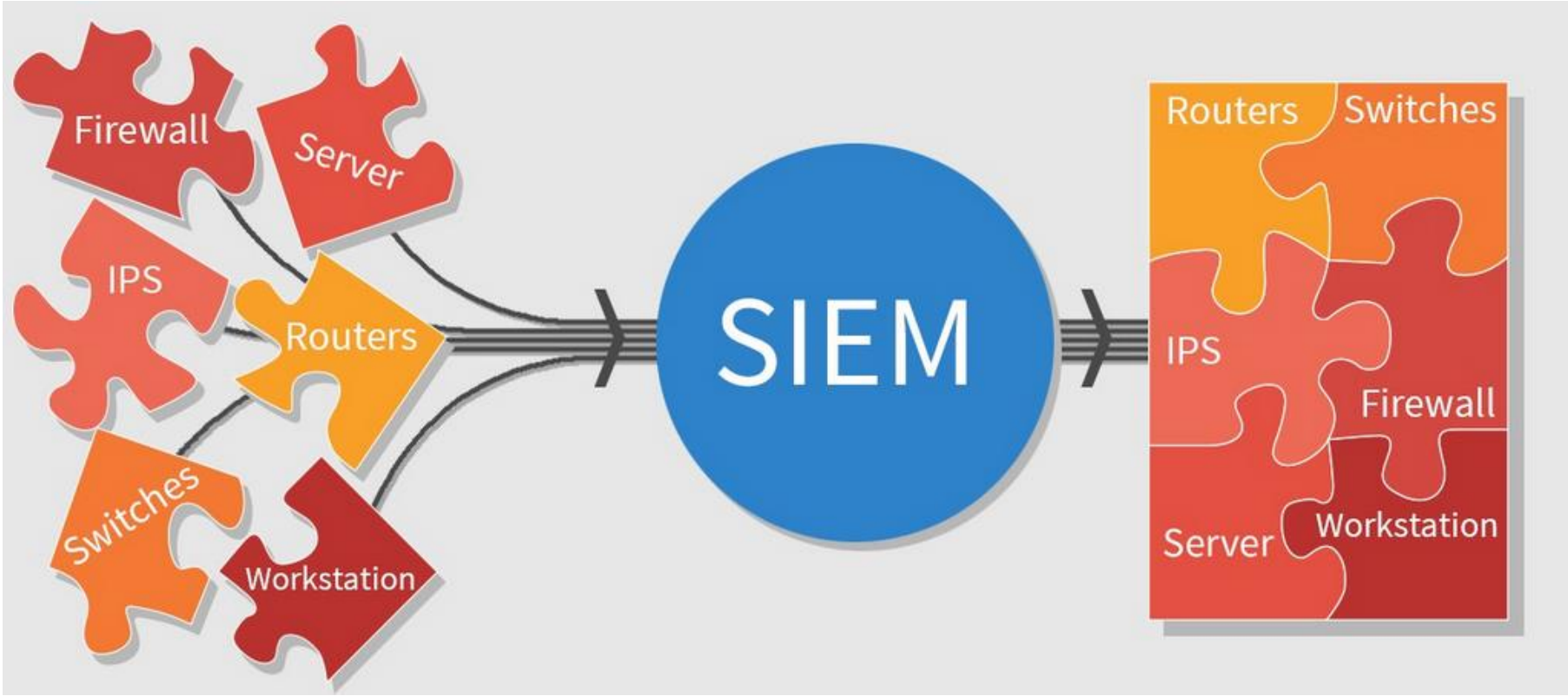
SIEM (Security Information and Event Management)



Offre un quadro completo e consolidato della sicurezza complessiva dell'infrastruttura digitale

BLUDIS
VALUE ADDED DISTRIBUTOR

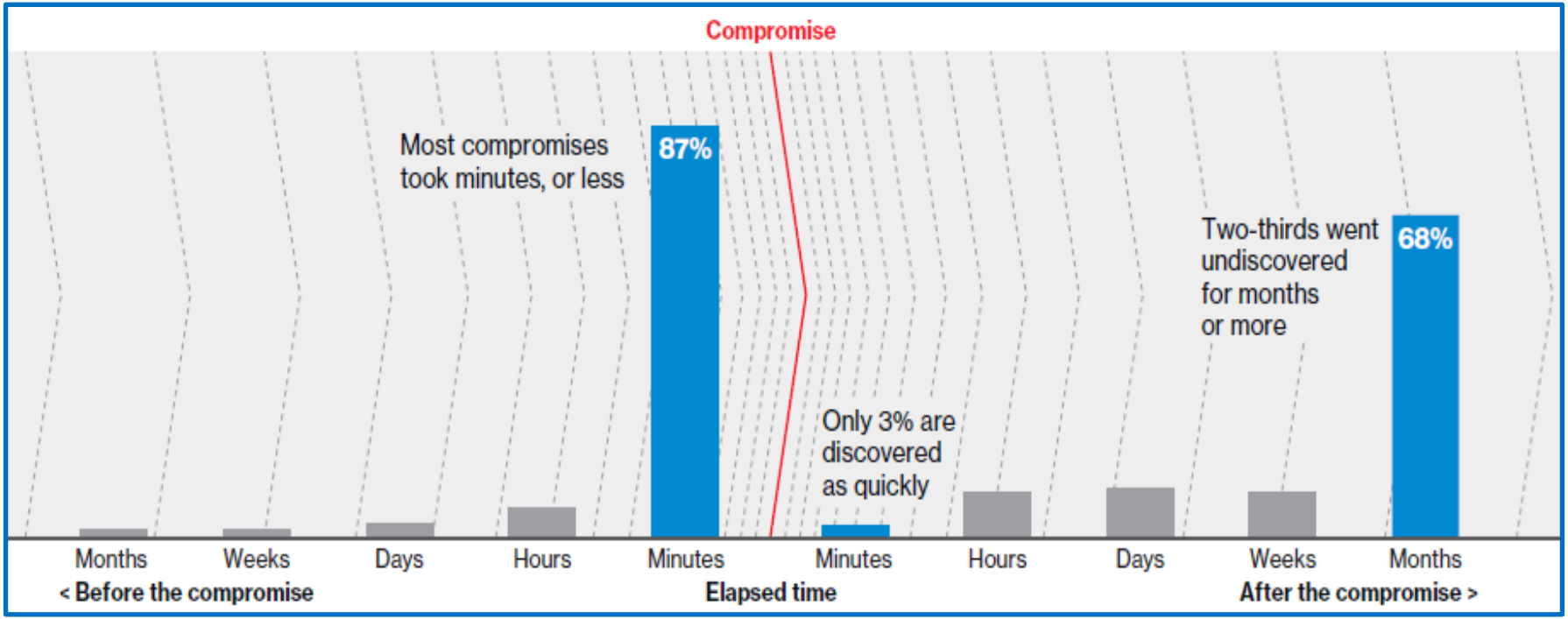
ManageEngine



Il SIEM è lo strumento che si occupa di raccogliere log prodotti da diverse fonti, interpretarli, normalizzarli e correlarli tra di loro

BLUDIS
VALUE ADDED DISTRIBUTOR

ManageEngine



Data Breach Investigations Report 2018 © Verizon

Il report del 2018 si basa su un'analisi dettagliata di oltre 53.000 incident di sicurezza, incluse 2.216 violazioni dei dati.

SIEM aiutano con la conformità

- NIST (National Institute of Standard and Technology)
- NIS (Network Information System)
- GDPR
- Framework Nazionale per la Cybersecurity
- PCI DSS
- Dora (Digital Operational Resilience ACT)
- ISO 27000

Provvedimento Log AdS Amministratori di Sistema

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - **27 novembre 2008.**

Ogni azienda quindi, dopo aver individuato i sistemi (dispositivi di rete, database, apparati di sicurezza e sistemi software complessi) che contengono i dati più critici ed averne nominato gli amministratori, dovrà dotarsi di un sistema di Log Management in grado di tracciare gli accessi degli operatori ai dispositivi ed alle applicazioni che gestiscono. Questo sistema dovrà conservare i dati in maniera sicura per un periodo minimo di sei mesi e dovrà essere consultabile dall'azienda e dalle autorità preposte alle attività di controllo.

Eventi generati da Infrastruttura IT azienda PMI

- 1500 Endpoint
- 2 Firewall
- Active Directory
- Antivirus
- IDS
- WAF

2 MILIARDI

DI EVENTI AL MESE COLLEZIONATI

BLUDIS
VALUE ADDED DISTRIBUTOR

ManageEngine

2 MILIARDI

DI EVENTI AL MESE COLLEZIONATI

900000

EVENTI SOSPETTI POST ANALISI DEI RAW DATA

25

DETECTION CONFERMATE

???

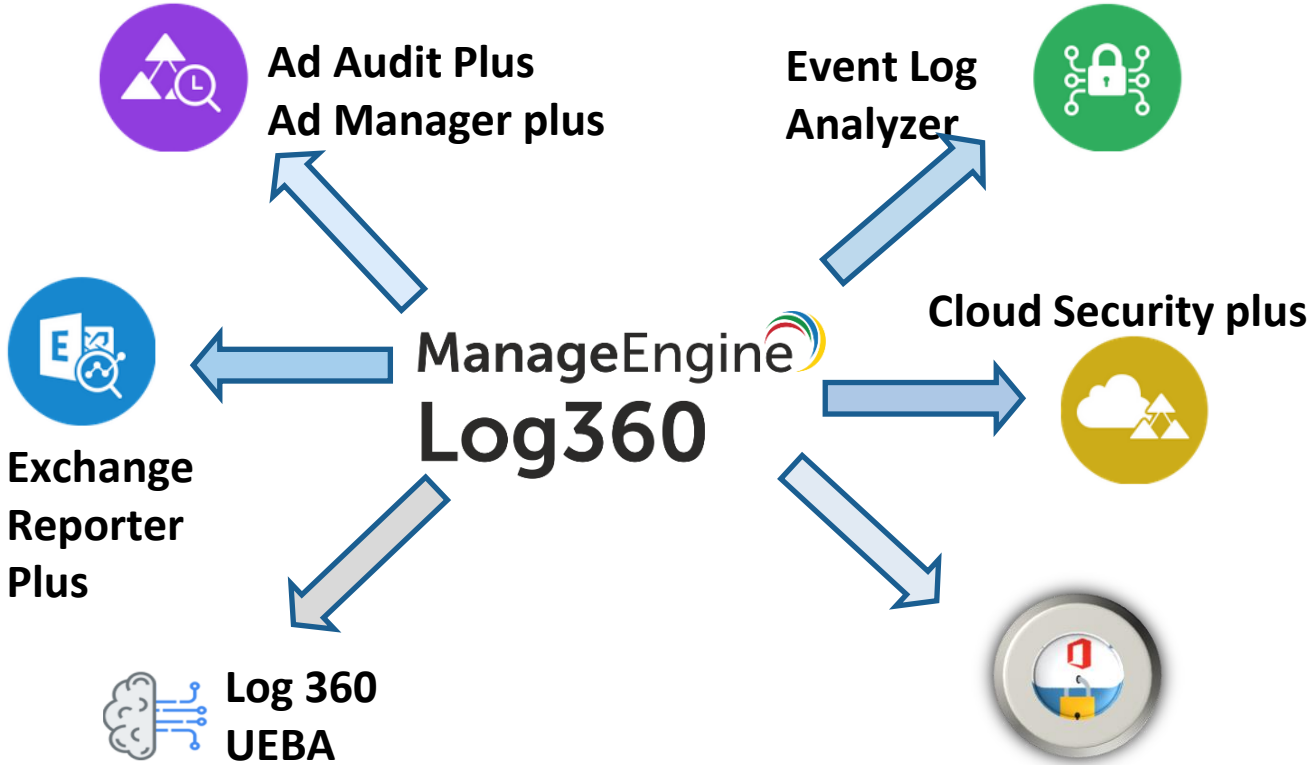
MINACCE REALI CONFERMATE

BLUDIS
VALUE ADDED DISTRIBUTOR

ManageEngine


A
D
W R O O T K I T
S A A
P R N V
C Y B E R S E C U R I T Y
W O R
T R O J A N M U
R W O R M S
E A
R
E

Quando il tuo assetto di sicurezza bada solo al rispetto della compliance...


Ad Audit Plus
Ad Manager plus
Event Log
Analyzer
Cloud Security plus
ManageEngine
Log360
Exchange
Reporter
Plus
Log 360
UEBA
Office 365
Manager Plus

ManageEngine
Log360

Why **Log360** is a complete **SIEM solution**

Integrated compliance management

Stay compliant with PCI DSS, GDPR, FISMA, HIPAA, SOX, GLBA with audit-ready report templates. Exclusive dashboard to view the compliance state of your network.

Lets you tweak existing report templates to meet internal security policies and also allows you to build your own compliance reports easily with reusable components.

Security analytics

Spots network intrusions and threats by analyzing events from network devices, servers, databases, web servers, Office 365 platforms, Exchange servers, and AD.

Intuitive dashboards and pre-built reports help you detect and respond to anomalies instantly.

Threat intelligence

Detects attacks at their early stages with its built-in global IP threat database and STIX/TAXII threat feed processor that identifies malicious entities interacting with your network.

The real-time alerting system is tied together with the incident management system allowing you to quickly detect security incidents and resolve them.

Cloud monitoring

Detects anomalous events by monitoring activities happening in PaaS and IaaS environments such as Azure, Amazon Web Services, and SaaS applications like Salesforce.

Spots activities such as unauthorized download of customer information from Salesforce with predefined reports and alerts.

User behavior analytics (UBA)

Spots anomalies without manual intervention using sophisticated machine learning techniques.

Detect unusual volume of logons, file activity, lockouts, and more with the intuitive dashboard and exhaustive reports.

Incident management

Includes built-in incident tracking system which allows you to automatically assign owners to security alerts, track the incident resolution process, and more.

Integrates with JIRA, ServiceNow, ServiceDesk Plus, Zendesk and other help desk tools for streamlined incident tracking and resolution.

Data security

Automatically discovers personal and sensitive data in Windows infrastructure with predefined confidential data detection policies. Protect these data with the extensive file integrity monitoring capability.

Monitors file and folder creation, deletion, modification, and permission changes in

Cosa rende UNICO ManageEngine Log360

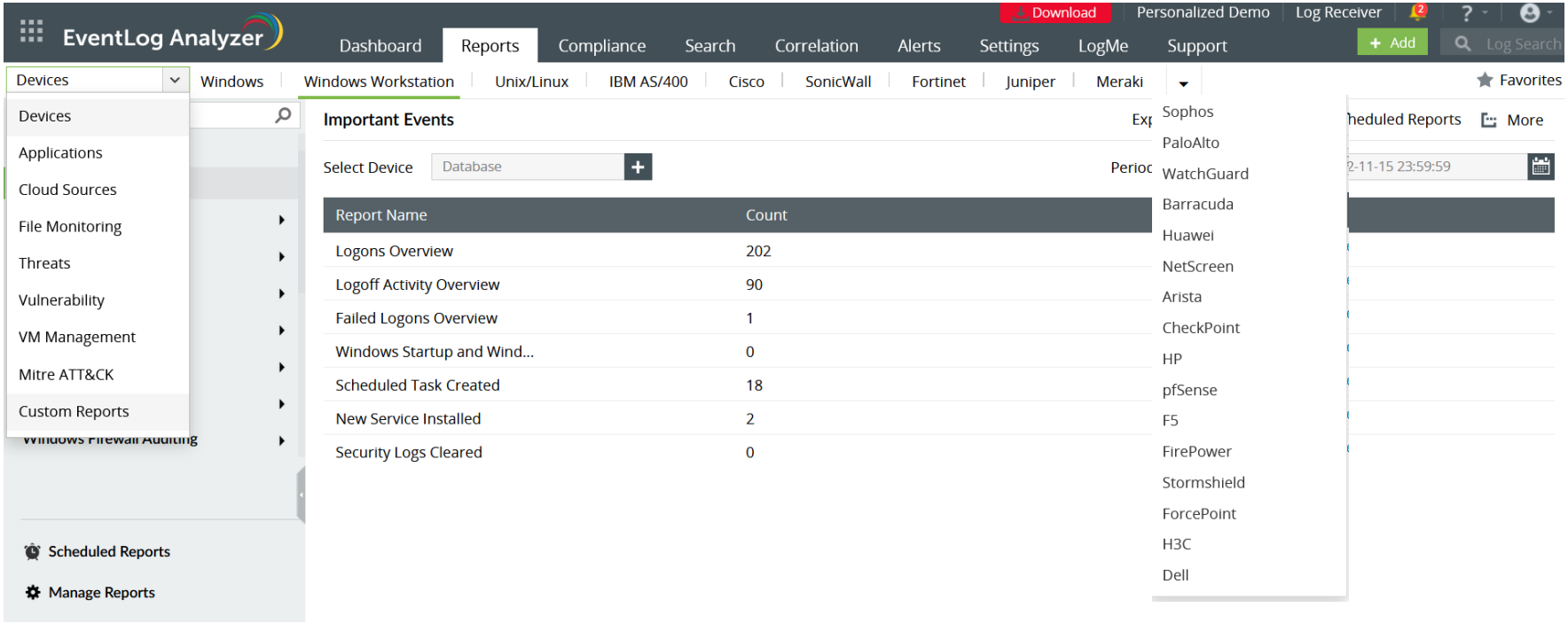
Report e alert predefiniti e custom per:

- Account Management
- Security Auditing
- User Activity Monitoring
- Threat Detection
- File Integrity Monitoring

BLUDIS
VALUE ADDED DISTRIBUTOR

ManageEngine

Centinaia di report predefiniti e specifici per tipologia di sistema

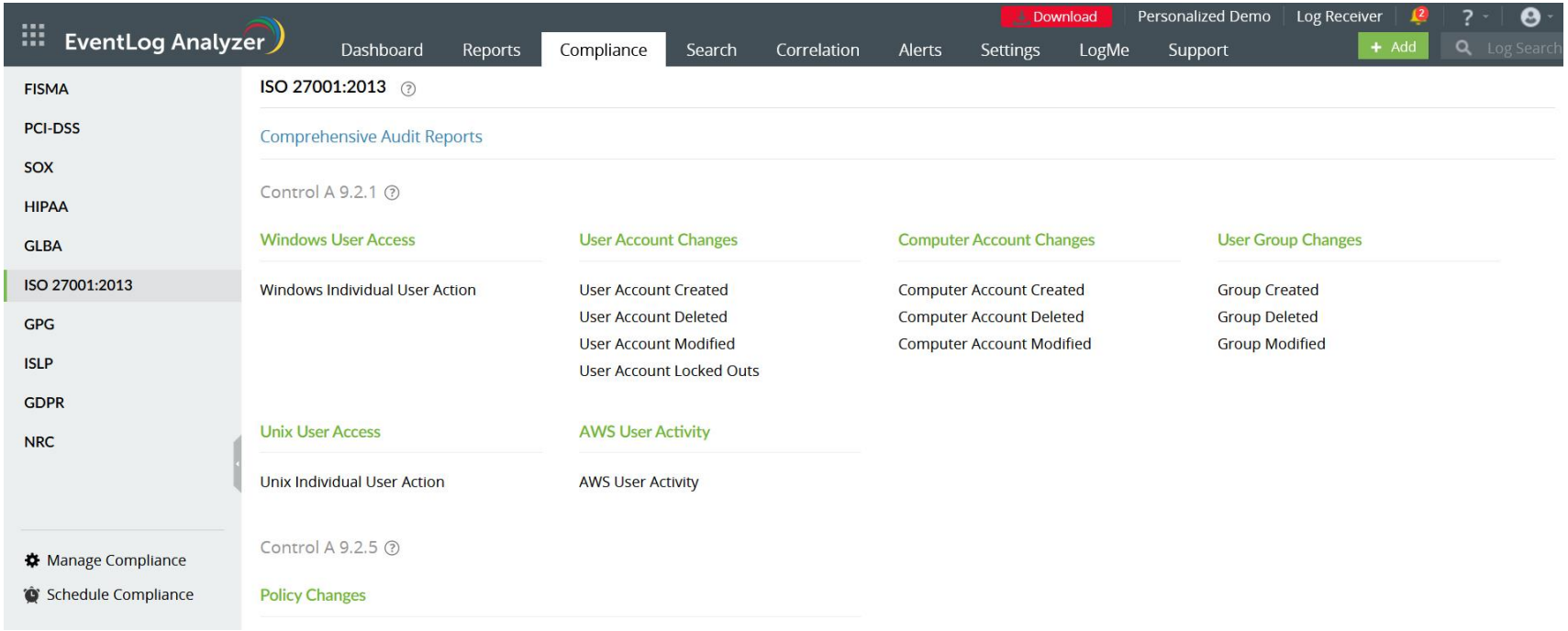


BLUDIS
VALUE ADDED DISTRIBUTOR

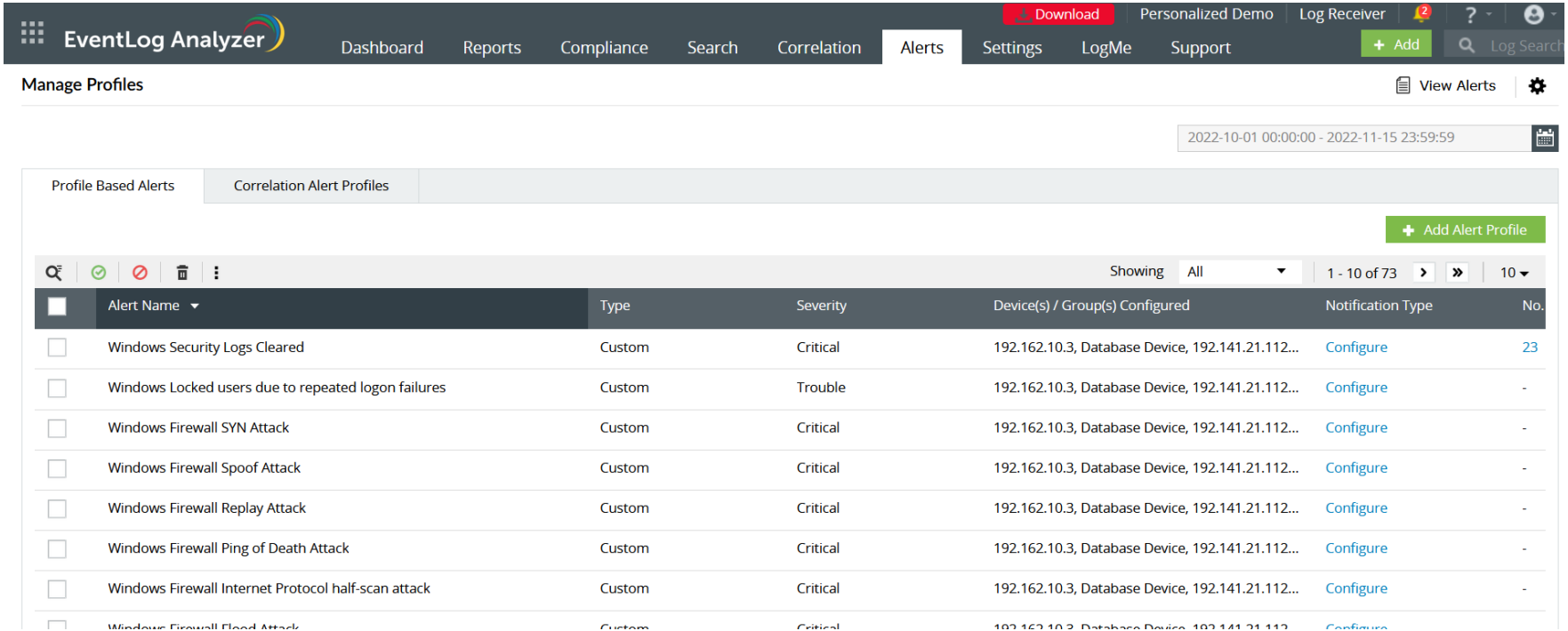
ManageEngine

Centinaia di report predefiniti e specifici per tipologia di sistema

Audit & Report Compliance: FISMA, PCI DSS, SOX, HIPAA, ISO 27001, GDPR, etc



Alert e sistema di notifica predefiniti e configurabili



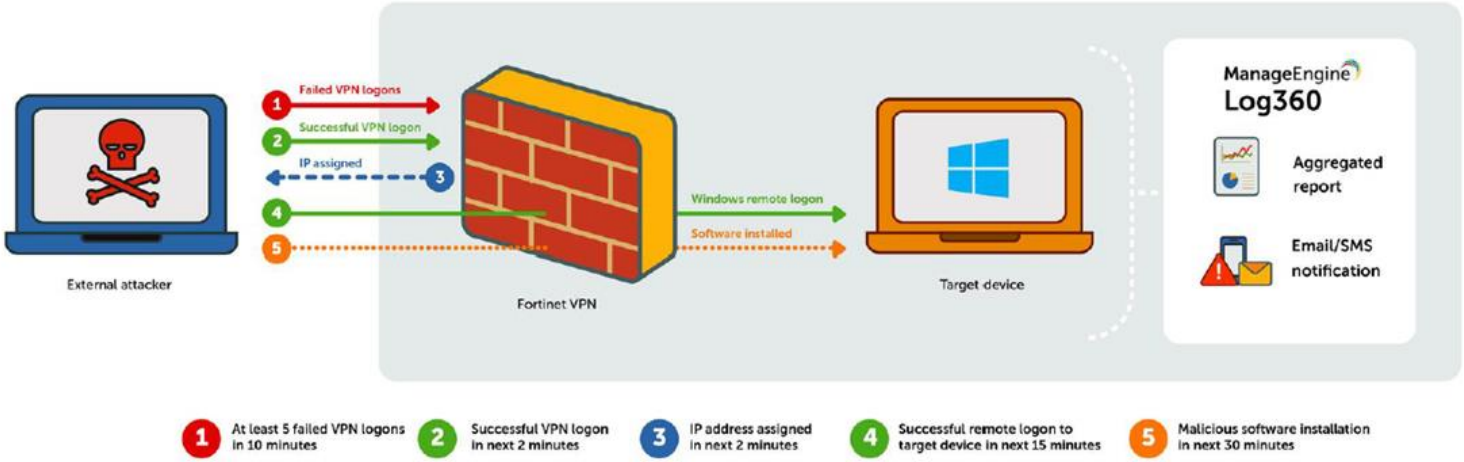
Security analytics

Correlazione avanzata degli eventi

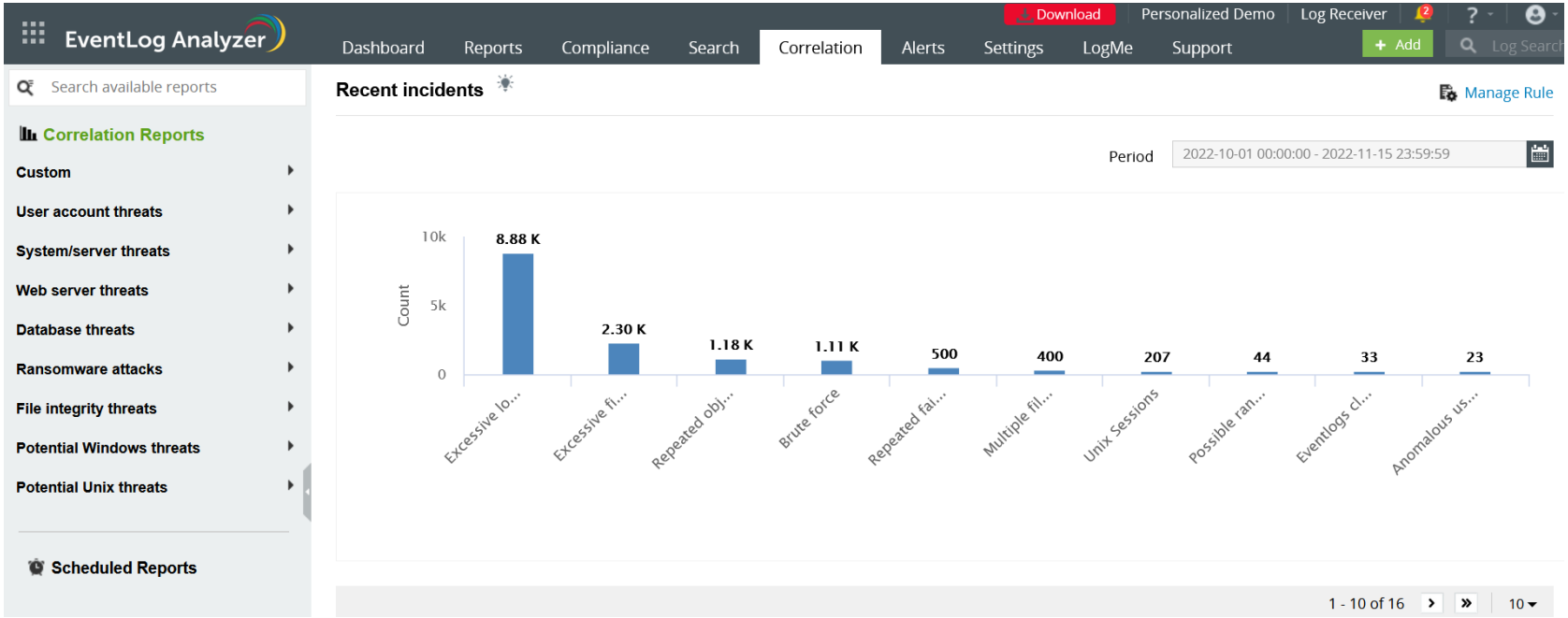
- Rilevamento degli incidenti pattern-based
- Oltre 30 regole predefinite: rileva software sospetti, cryptojacking, attività di worm e altro ancora
- Dashboard panoramica sugli incident
- Timeline dettagliate degli incident
- Generatore di regole di correlazione personalizzate con filtri avanzati

Rilevare l'installazione di software sospetti

Installazione di software sospetti



Task di correlazione eventi predefiniti e configurabili



BLUDIS
VALUE ADDED DISTRIBUTOR

ManageEngine

Log forense

- Engine di ricerca basato su Elasticsearch che aiuta a rilevare e analizzare gli incident complessi e scoprirne le cause in pochi minuti
- Ricerca di base e avanzata: utilizza opzioni flessibili per creare query di ricerca da zero o utilizza l'interfaccia avanzata del generatore di query
- Cerca nei log in formato annuncio non elaborato, inclusi gli archivi dei log
- Salva le ricerche come report o alert

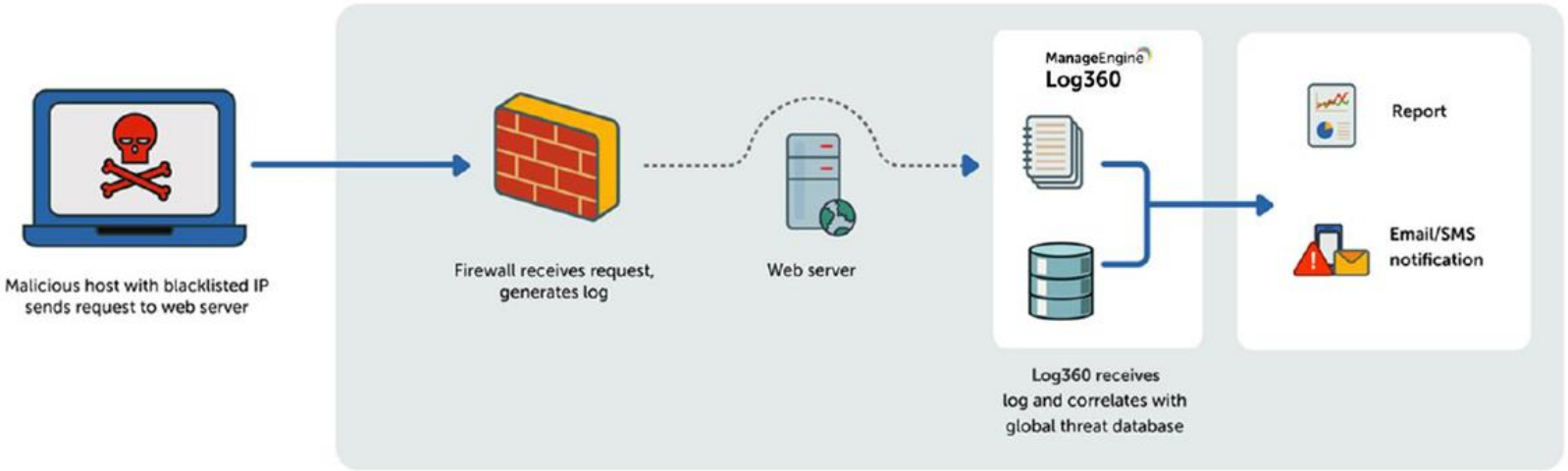
Threat intelligence

Threat intelligence

- Rileva le intrusioni nella rete grazie ai dati del feed minacce
- Avvisi in tempo reale per URL, IP e nomi di dominio dannosi
- Aggiungi feed di minacce STIX/TAXII personalizzati
- Nessuna configurazione necessaria
- Aggiornamenti dinamici e quotidiani

Rileva l'installazione di software sospetti

Inboud malicious IP

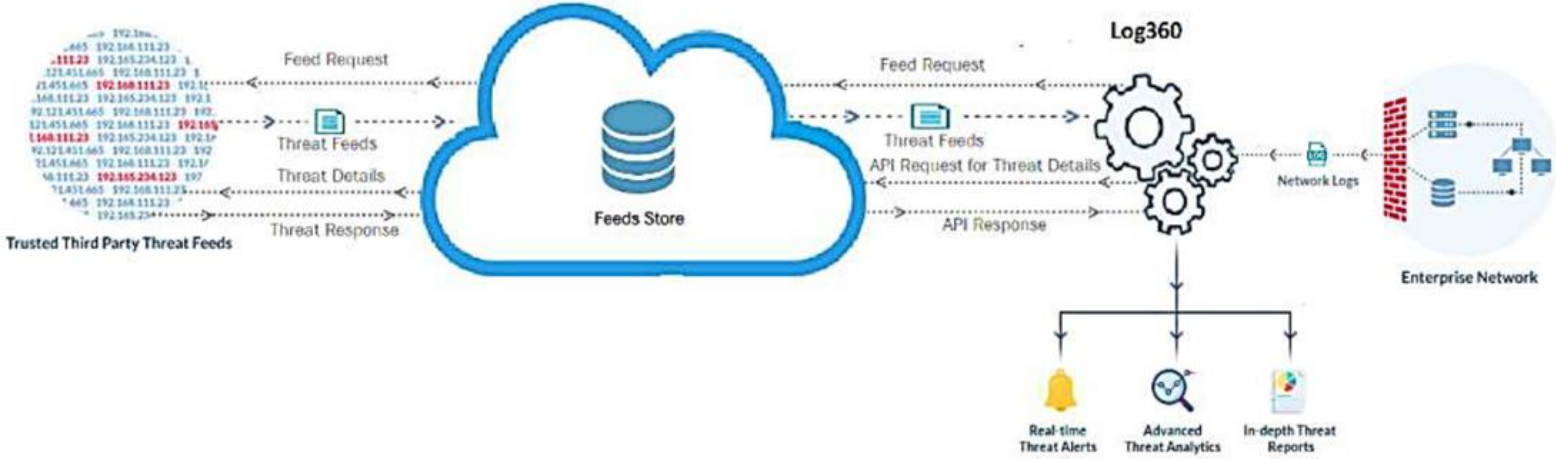



Advanced threat analytics

Analisi avanzata delle minacce

- Integrazione con provider affidabile di informazioni sulle minacce
- Informazioni più approfondite sulla minaccia segnalata
- Classificazione IP/URL
- Punteggio di Reputation

Feed minacce integrato



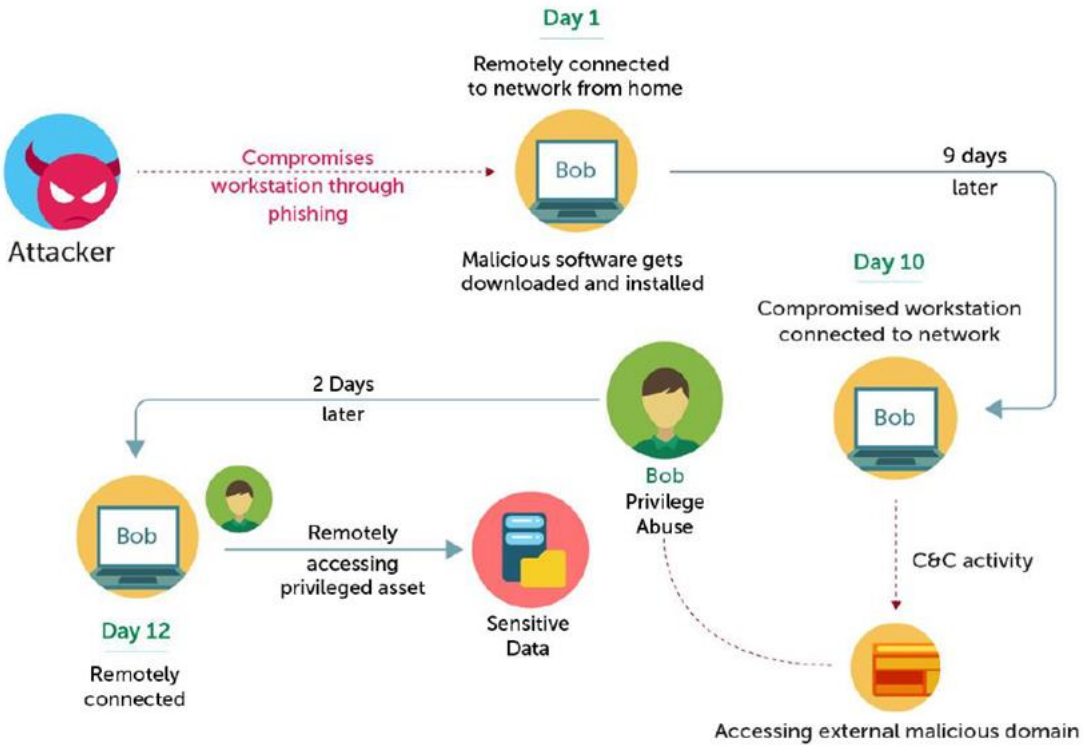
User and entity behavior analytics

Analisi del comportamento degli utenti e dei team

- Rilevamento delle anomalie dell'apprendimento automatico
- Rilevamento di comportamenti anomali: basato su tempo, modello o conteggio
- Prioritizzazione delle minacce basata sul punteggio di rischio: determinare il grado di rischio posto da una minaccia identificata
- Aggiungi utenti e team/aree ad alto rischio a una watchlist
- Conferma delle minacce: identificare l'indicatore delle minacce comuni (compromissione dell'account, esfiltrazione di dati e altro)

Use case

Workstation compromessa e tentativo di furto dei dati



Incident management

Gestione degli incident

Sistema di ticketing integrato

- Assegnazione automatica dei ticket relativi agli incident
- Track sullo stato degli incident
- Knowledge base degli incident risolti

Inoltrare informazioni sugli incident all'help desk software esterno

- Help desk software supportati: ServiceDesk Plus, ServiceNow, Jira Service Desk, ZenDesk, BMC Remedy, Kayako

Cloud monitoring

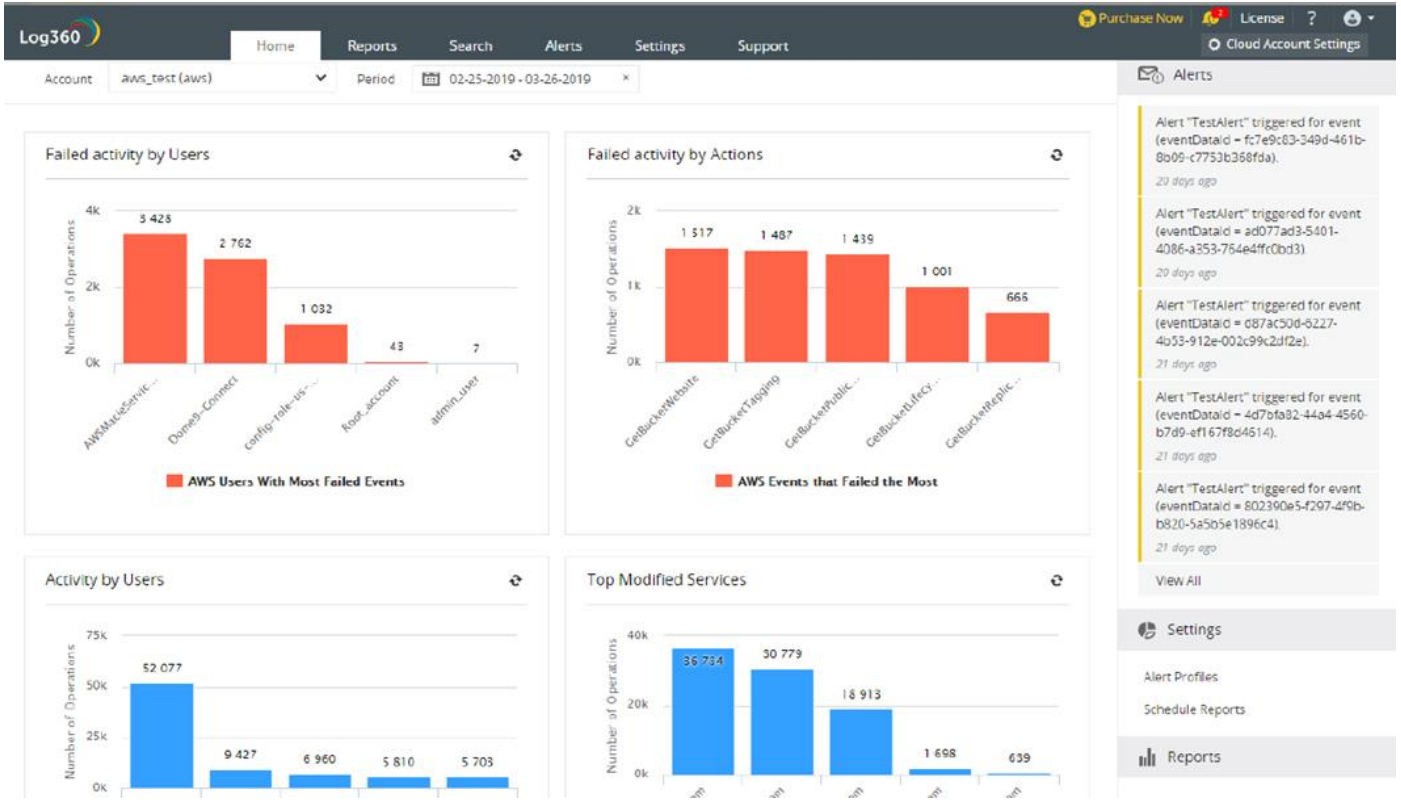
Ambienti cloud

Ottieni informazioni su

AWS: Amazon S3, Amazon EC2, Web Application Firewalls (WAF), Relational Database Service (RDS), and more

Microsoft Azure: User activity, changes made to network security groups, virtual networks, DNS zones, databases, and more

Salesforce: Login, report, content, and search activities


Log360
Home
Reports
Search
Alerts
Settings
Support
Purchase Now
License
Cloud Account Settings
Account
aws_test (aws)
Period
02-25-2019 - 03-26-2019
Failed activity by Users
Number of Operations
4k
2k
0k
3 428
2 762
1 032
43
7
AWSMarketServic...
Dome9_Connect
config-role-us-...
Root_account
admin_user
AWS Users With Most Failed Events
Failed activity by Actions
2k
1k
0k
1 517
1 487
1 439
1 001
665
GetBucketWebsite
GetBucketTagging
GetBucketPublic...
GetBucketLifecy...
GetBucketReplic...
AWS Events that Failed the Most
Activity by Users
75k
50k
25k
0k
52 077
9 427
6 960
5 810
5 703
Top Modified Services
40k
20k
0k
36 734
30 779
18 913
1 698
639
Alerts
Alert "TestAlert" triggered for event (eventDataId = fc7e9c83-349d-461b-8b09-c7753b358fda).
20 days ago
Alert "TestAlert" triggered for event (eventDataId = ad077ad3-5401-4086-a353-764e4ffc0bd3).
20 days ago
Alert "TestAlert" triggered for event (eventDataId = d87ac50d-6227-4b53-912e-002c99c2df2e).
21 days ago
Alert "TestAlert" triggered for event (eventDataId = 4d7bfa82-44a4-4560-b7d9-ef167f8d4614).
21 days ago
Alert "TestAlert" triggered for event (eventDataId = 802390e5-f297-4f9b-b820-5a5b5e1896c4).
21 days ago
View All
Settings
Alert Profiles
Schedule Reports
Reports

BLUDIS
VALUE ADDED DISTRIBUTOR

ManageEngine

Grazie mille

per la vostra attenzione!