IT Operations Analytics

Come il Log Management può essere di supporto alle certificazioni ISO 27001

Georg Kostner, Würth Phoenix

La difesa cibernetica diventa un *must*

- **General Data Protection Regulation** (**GDPR**) (Regolamento europeo 2016/679) valido a partire dal 25 Maggio 2018
- Gli hacker rubano i dati dei clienti (carte di credito, prezzi, dati personali, …)
- Spionaggio industriale
- Chi si sta connettendo alla mia infrastruttura? Quando e da dove? (dipendenti, fornitori)
- In caso di un attacco cibernetico: possiedo dati per il management, a fini dell'applicazione della legge o per la polizza contro il cyber risk?

Le sfide a livello pratico

I componenti di un ambiente IT, registrano eventi rilevanti per la sicurezza, fornendo un elevato quantitativo di dati.

I log hanno diversi formati a seconda del componente ed è quindi difficile mantenere una panoramica su milioni di dati registrati giornalmente.

Security Information e Event Management (SIEM)

Gartner definisce SIEM come:

*Security information and event management (SIEM) technology supports threat detection and security incident response through the **real-time collection** and **historical analysis** of **security events** from a wide variety of event and contextual data sources. It also supports compliance reporting and incident investigation through analysis of historical data from these sources.*

The core capabilities of SIEM technology are a broad scope of event collection and the ability to correlate and analyze events across disparate sources.

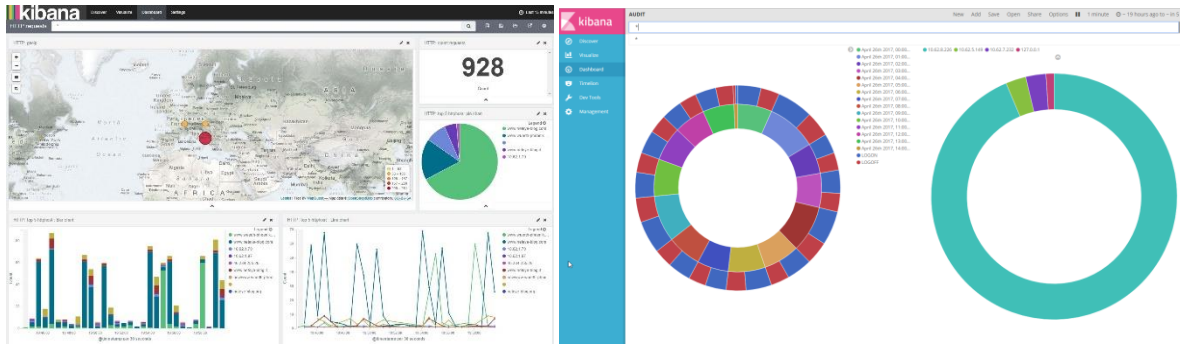
Security Information Management

- Central collection and long term storage of log files for trend analysis

Event Management

- Real-time monitoring, correlating events, alerts visualizations

La nostra soluzione



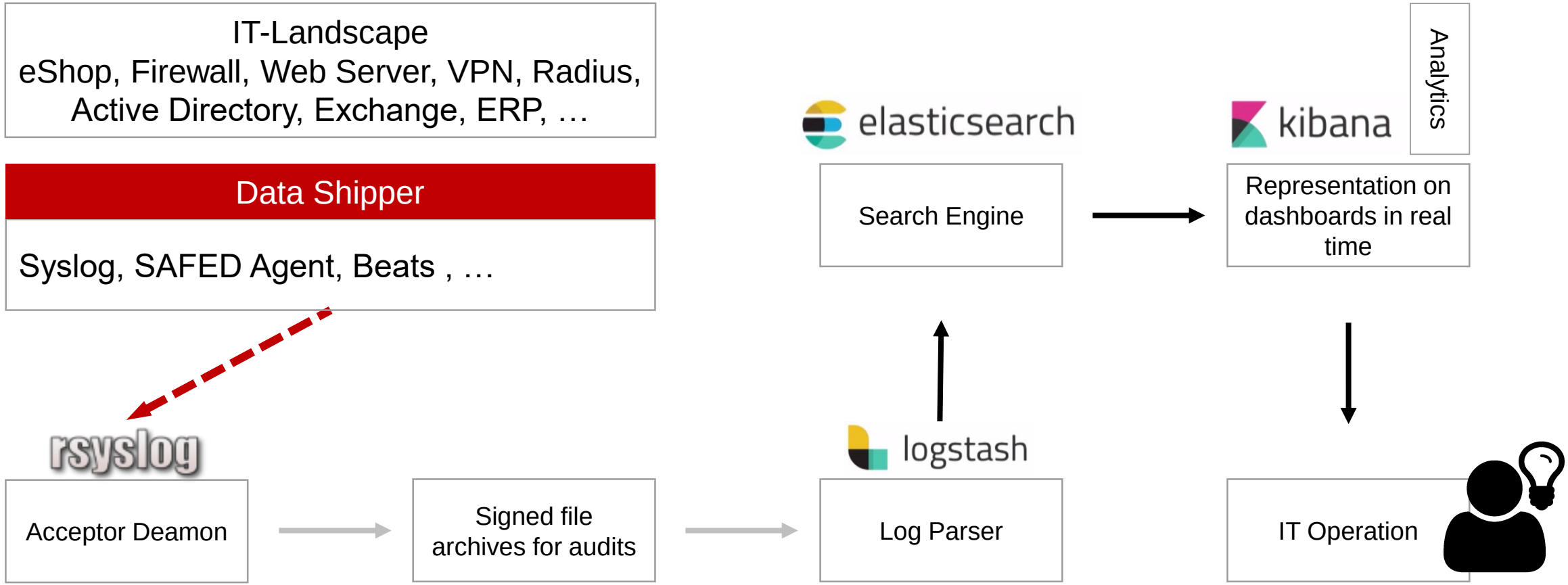
elasticsearch kibana logstash

WÜRTHPHOENIX NetEye

Una soluzione centralizzata per aggregare i log e analizzarli in tempo reale

Network | Security | Servers | Databases | Applications

NetEye Log Management: l'architettura



Le possibilità di NetEye per il SIEM in dettaglio

Data aggregation
aggregazione di dati da sorgenti diverse (network, security, servers, databases, applications)

Correlation
identificazione di attributi comuni per collegare gli eventi in modo significativo

Alarms
analisi automatizzate di eventi correlati e generazione di allarmi

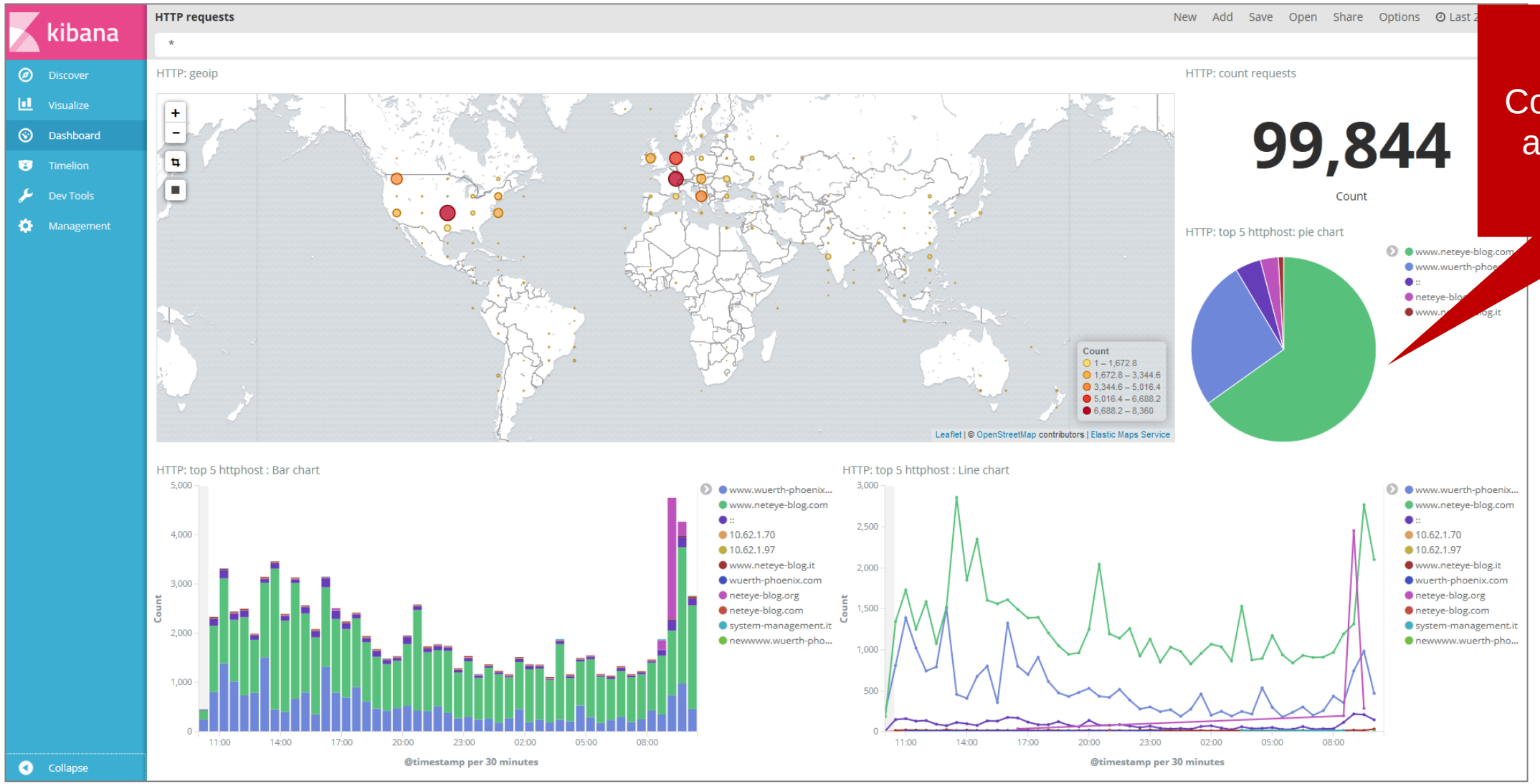
Dashboards
illustrazione grafica dei dati raccolti

Compliance
crazione di reports per scopi di Security, Governance e Auditing

Retention
archiviazione die dati a lungo termine

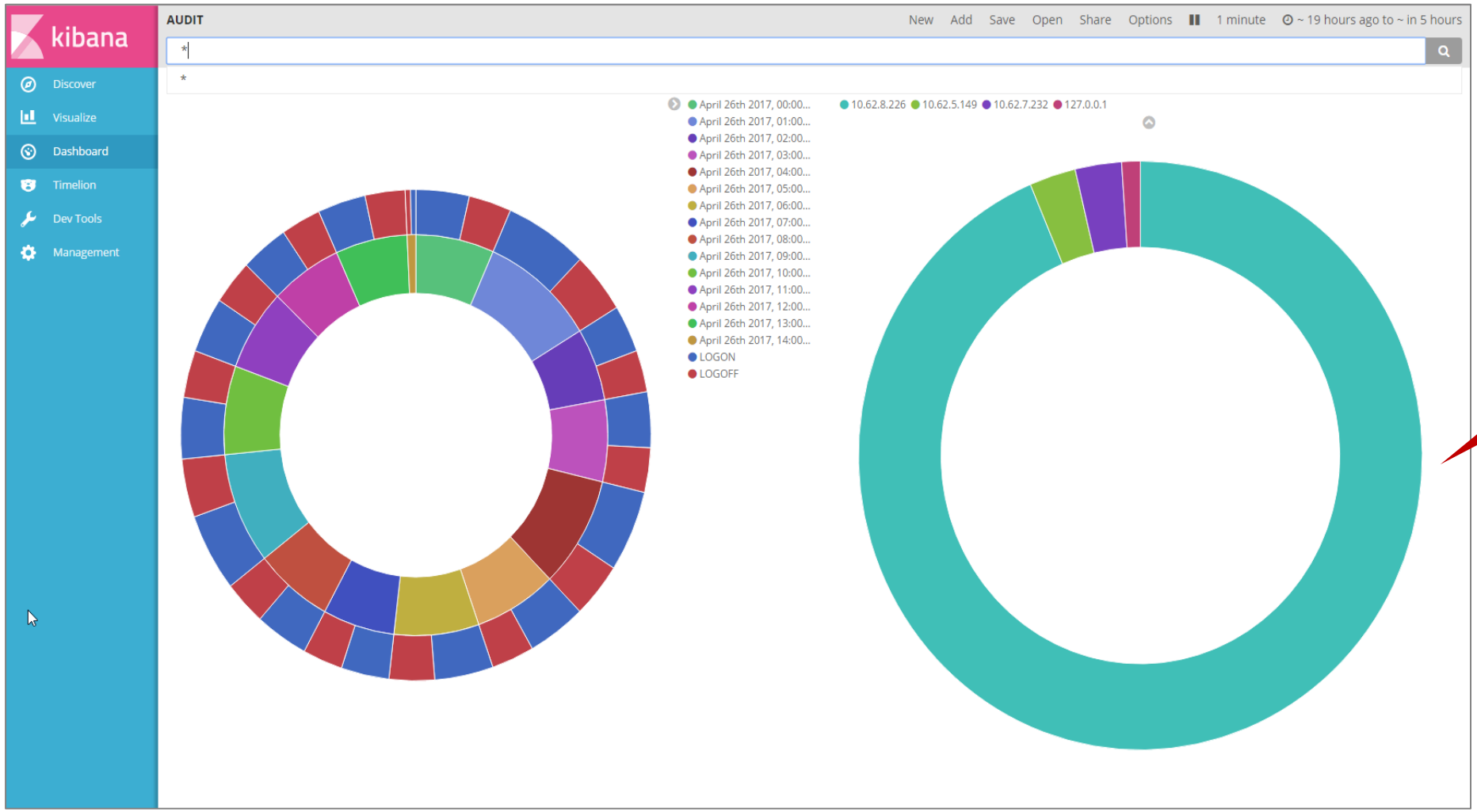
Forensic analysis
possibilità di ricerca sui log in base a vari criteri

NetEye Log Management: dashboard di esempio



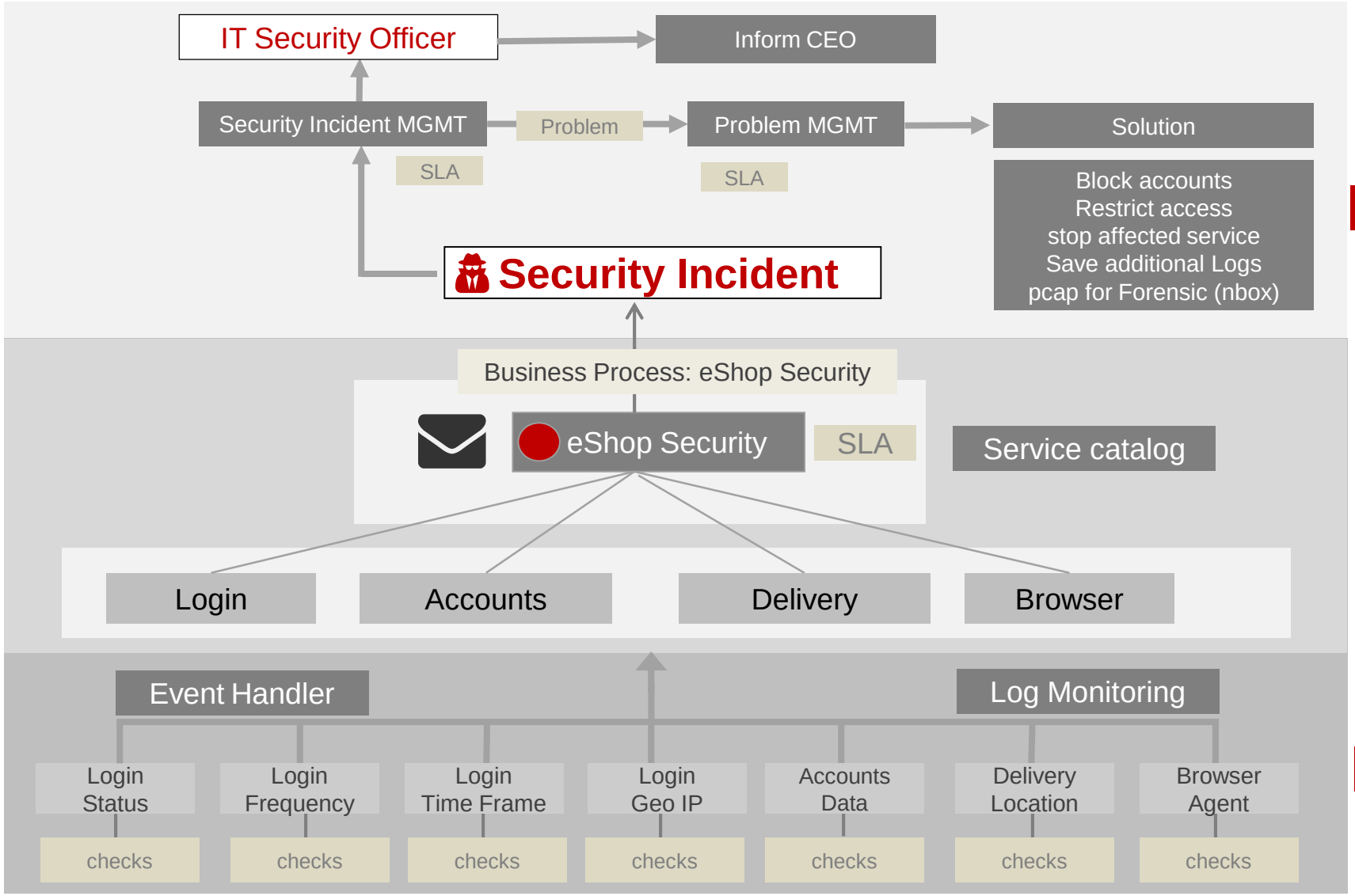
Correlazione sugli accessi via web

NetEye Log Management: dashboard di esempio



Audit sui login in base a fasce orarie

Relazioni legate al servizio: eShop come esempio



WÜRTHPHOENIX EriZone

WÜRTHPHOENIX NetEye

Information Security MGMT

Event MGMT

Event Management: come reagire agli eventi di log

ORIGINE

Configurazione dei componenti

TIPOLOGIA

Tipologia degli eventi

- LOG
- SMS
- E-Mail
- SNMP Trap
- …

REGOLE

Definizione e configurazione di regole per tipi di eventi diversi (informazioni sulla sicurezza e gestione eventi)

Rule Matching Engine

AZIONI

Possibili azioni da intraprendere:

- SNMP Trap
- Event Console
- SMS
- E-Mail
- Command
- Nagios
- Ignore
- …

I benefici ottenibili

Minor tempo per analisi migliori

Accesso centralizzato ai dati provenienti da diverse sorgenti

Generazione automatica delle dashboard

Analisi dei dati di log in tempo reale e rapida identificazione degli errori

Riconoscimento di errori generici e in base a processi

Misurazione della quantità degli errori e visualizzazione del loro sviluppo

Creazione delle dashboard senza necessità di possedere competenze tecniche

Supporto alle certificazioni ISO 27001

ISO 27001 in cosa consiste?

Lo standard **ISO/IEC 27001**

(*Tecnologia delle informazioni - Tecniche di sicurezza - Sistemi di gestione della sicurezza delle informazioni - Requisiti*)

è una **norma** internazionale che definisce i requisiti per impostare e gestire un sistema di **gestione della sicurezza delle informazioni** (SGSI o ISMS, dall'inglese *Information Security Management System*), ed include aspetti relativi alla sicurezza logica, fisica ed organizzativa.

Sorgente: Wikipedia

L’adozione di un Information Security Management System

WÜRTHPHOENIX EriZone

WÜRTHPHOENIX NetEye

ISMS

È un approccio olistico per la gestione della sicurezza delle informzioni.

Confidenzialità

Integrità

Disponibilità

Dati e Informazioni

La procedura da seguire

1. Identificazione delle informazioni e dei requisiti di sicurezza
2. Analisi e valutazione dei rischi di sicurezza
3. Selezione degli obiettivi di controllo e attività di controllo per la gestione dei rischi
4. Monitoraggio, gestione e miglioramento dell’efficacia dei controlli

I controlli ISO 27001

Rif.	Descrizione
A5	Information security policies
A6	Information Security Policy
A7	Human resource security
A8	Asset Management
A9	Access Control
A10	Cryptography
A11	Physical and environmental security
A12	Operations security
A13	Communications security
A14	System acquisition, development and maintenance
A15	Supplier relationships
A16	Information security incident management
A17	IS aspects of business continuity management
A18	Compliance

NetEye & EriZone vi supportano

Rif.	Descrizione	Aree supportate	Soluzione
A8	Asset Management	☑ Information classification ☑ Media Handling	NetEye
A9	Access Control	☑ User access management ☑ System and application access control	EriZone
A12	Operations security	☑ Logging and monitoring ☑ Control of operational software ☑ Technical vulnerability management ☑ Information systems audit considerations	NetEye
A13	Communications security	☑ Network security management	NetEye
A14	System acquisition, development and maintenance	☑ Security requirements of information systems ☑ Security in development and support processes ☑ Test data	NetEye EriZone NetEye
A15	Supplier relationships	☑ Information security in supplier relationships ☑ Supplier service delivery management	EriZone EriZone
A16	Information security incident management	☑ Management of information security incidents and improvements	NetEye
A17	IS aspects of business continuity management	☑ Information security continuity	

GRAZIE!