SOC و نقش آن در امنیت سازمانی

(بخش اول)

جلسه گروه کاربران گنو/لینوکس تهران

خرداد 96

بهین راهکار

MOST LIKELY NETWORK SECURITY CHALLENGE IN NEXT 12 MONTHS

16% EMPLOYEE MISTAKES

17% DATA LEAKAGE

13% INCIDENTS FROM EMPLOYEE-OWNED DEVICES

5% EXTERNAL HACKING

7% CYBER ATTACKS

11% CLOUD COMPUTING

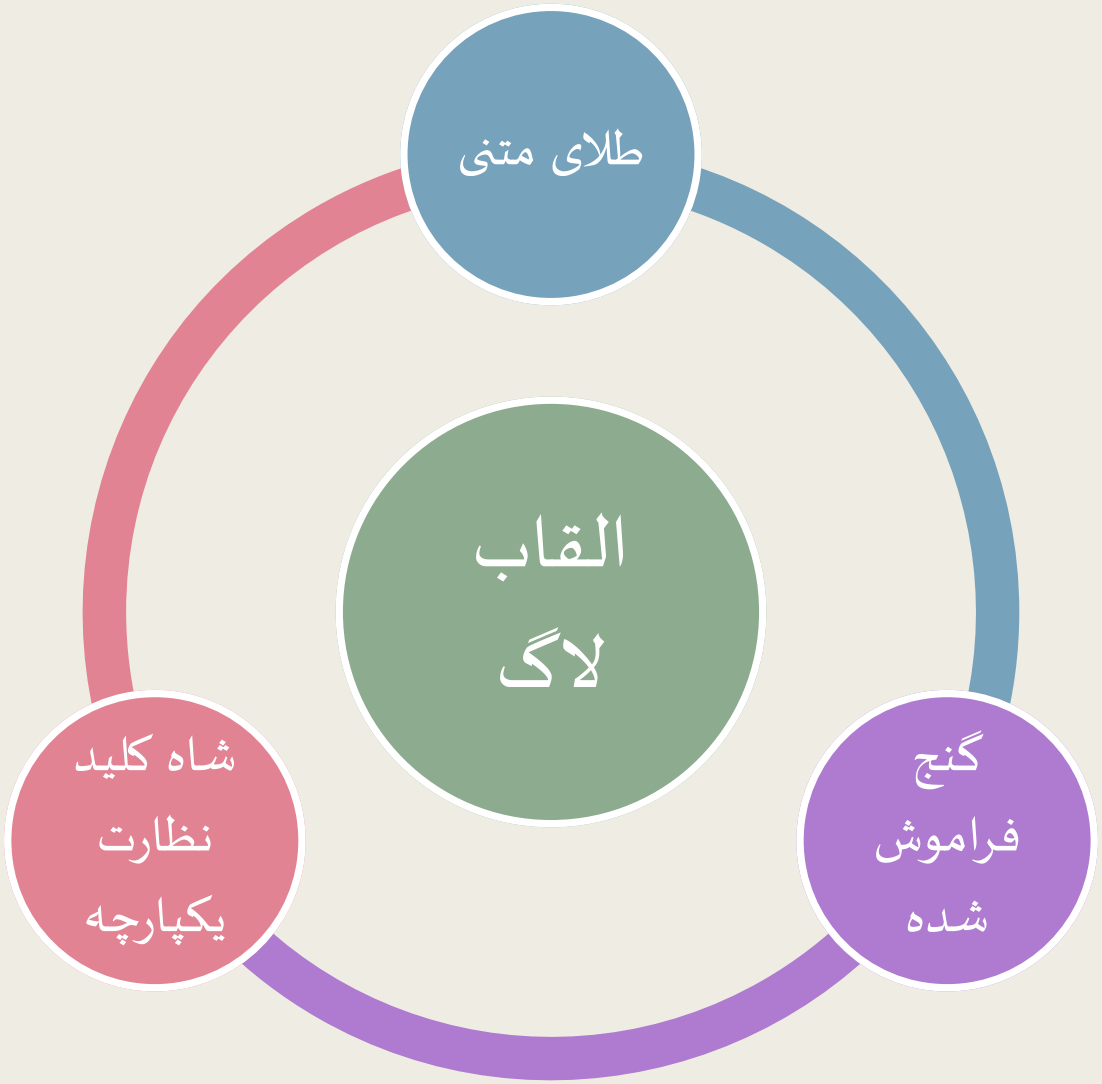
5% DISGRUNTLED EMPLOYEE

19% ALL OF THE ABOVE

8% NONE OF THE ABOVE

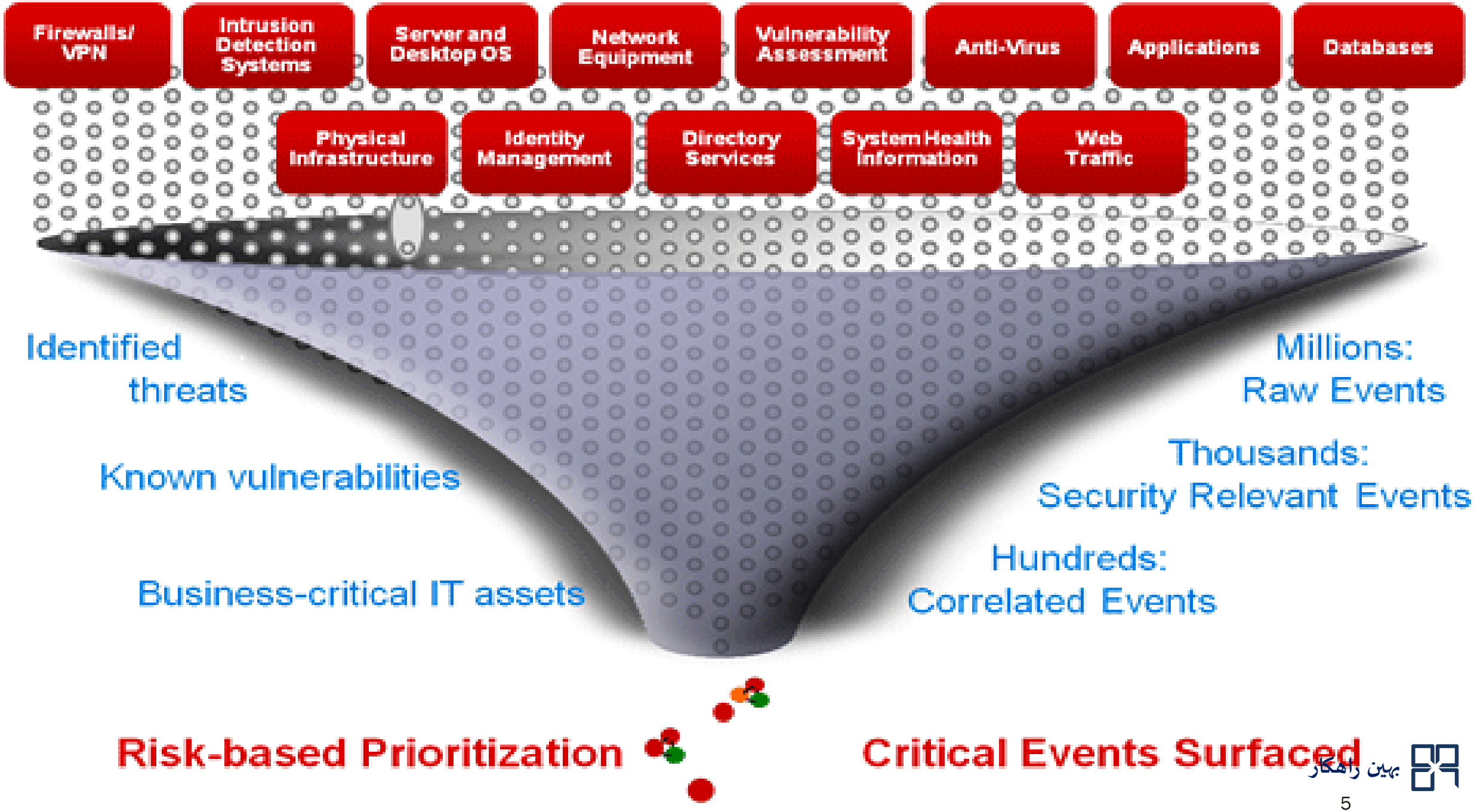
ISACA

Log راهکار حل مساله



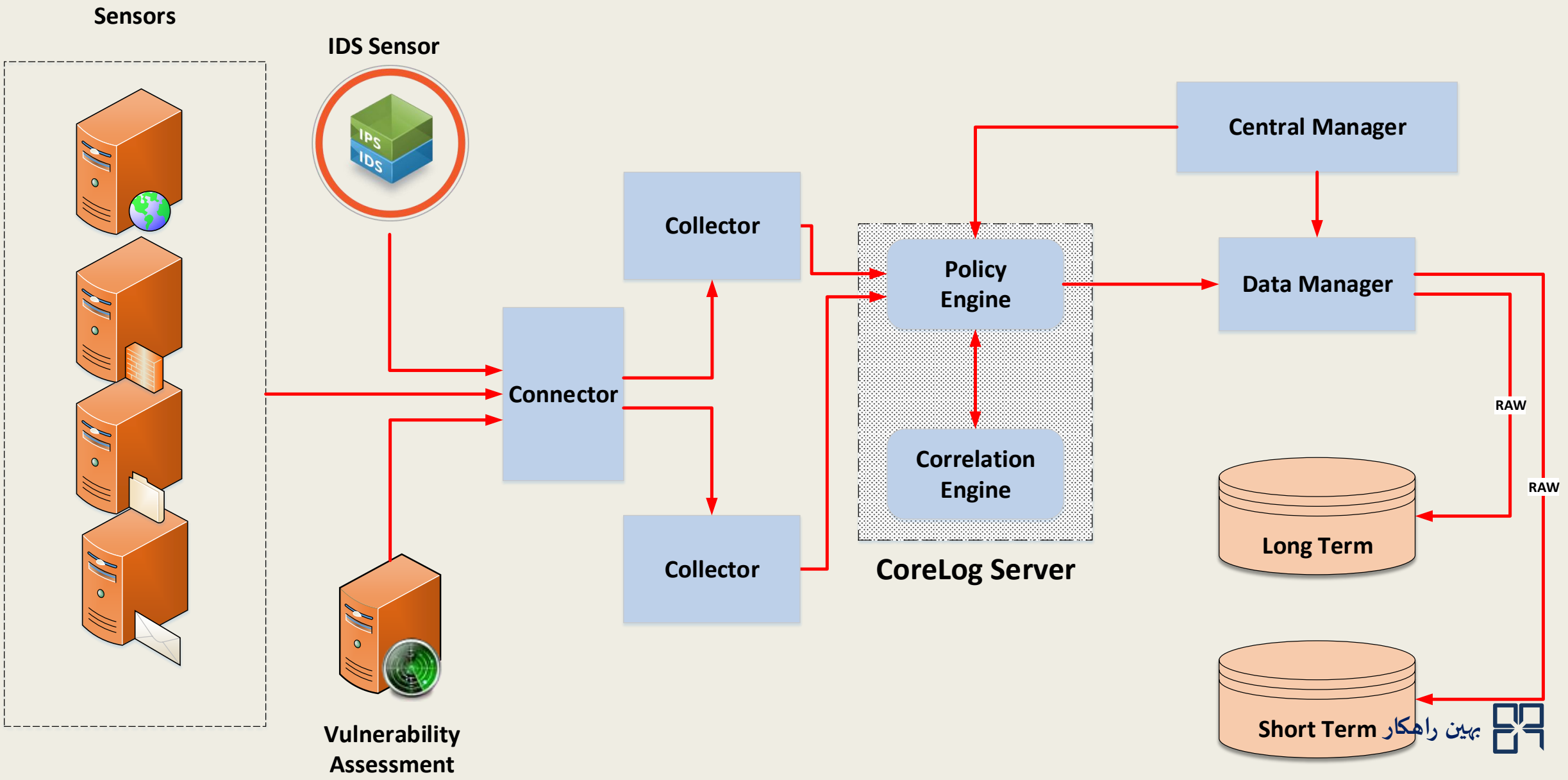
Log بیانگر هر آن چیزی است که در سازمان رخ می دهد و در صورتی که بدرستی استفاده شود، مقادیر با ارزشی برای سازمان محسوب می شود.

S	• Security
I	• Information
E	• Event
M	• Management

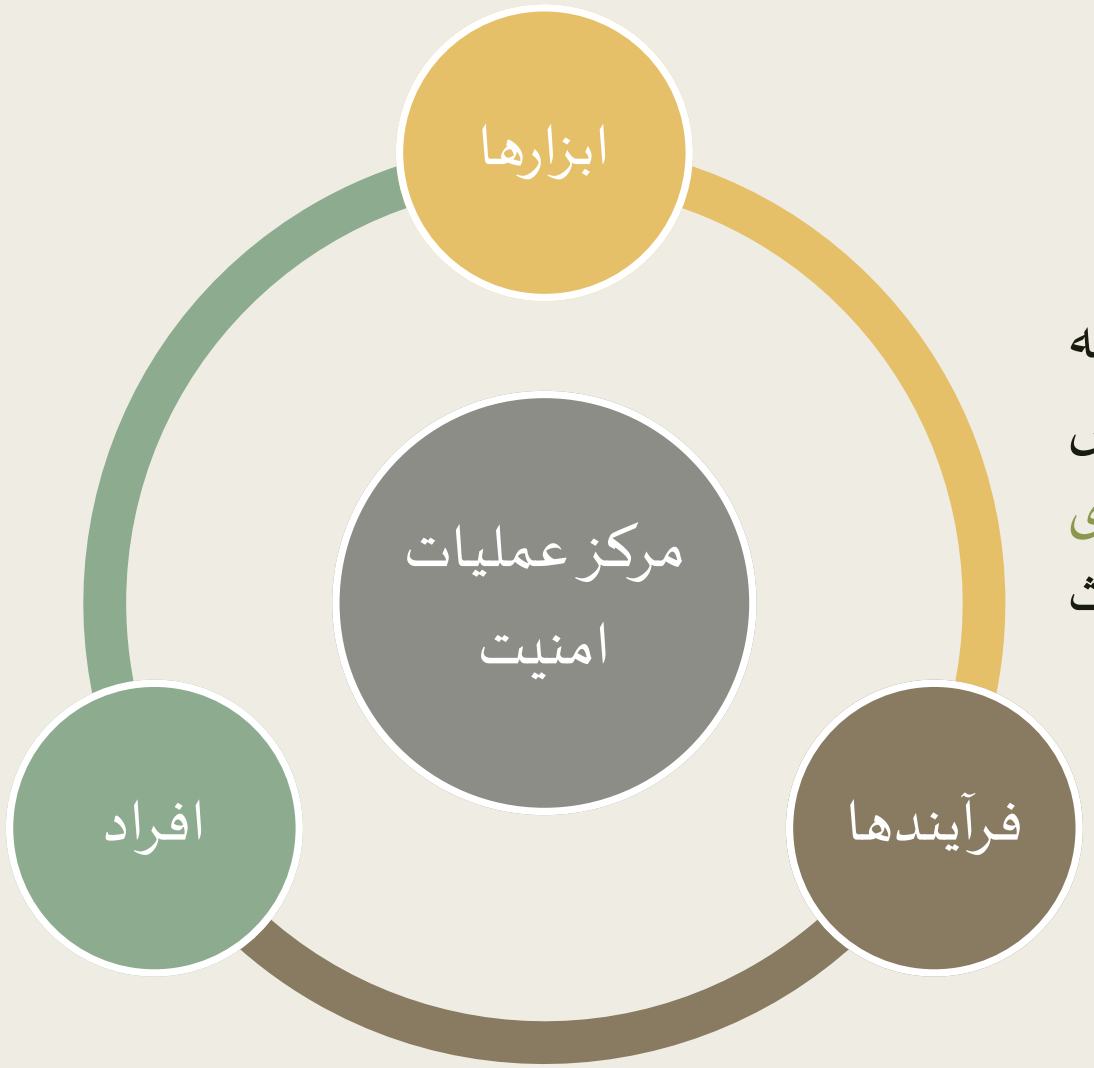

Firewalls/ VPN
Intrusion Detection Systems
Server and Desktop OS
Network Equipment
Vulnerability Assessment
Anti-Virus
Applications
Databases
Physical Infrastructure
Identity Management
Directory Services
System Health Information
Web Traffic
Identified threats
Known vulnerabilities
Business-critical IT assets
Millions: Raw Events
Thousands: Security Relevant Events
Hundreds: Correlated Events
Risk-based Prioritization
Critical Events Surfaced

وظایف اصلی SIEM

معماری سامانه کورلاگ

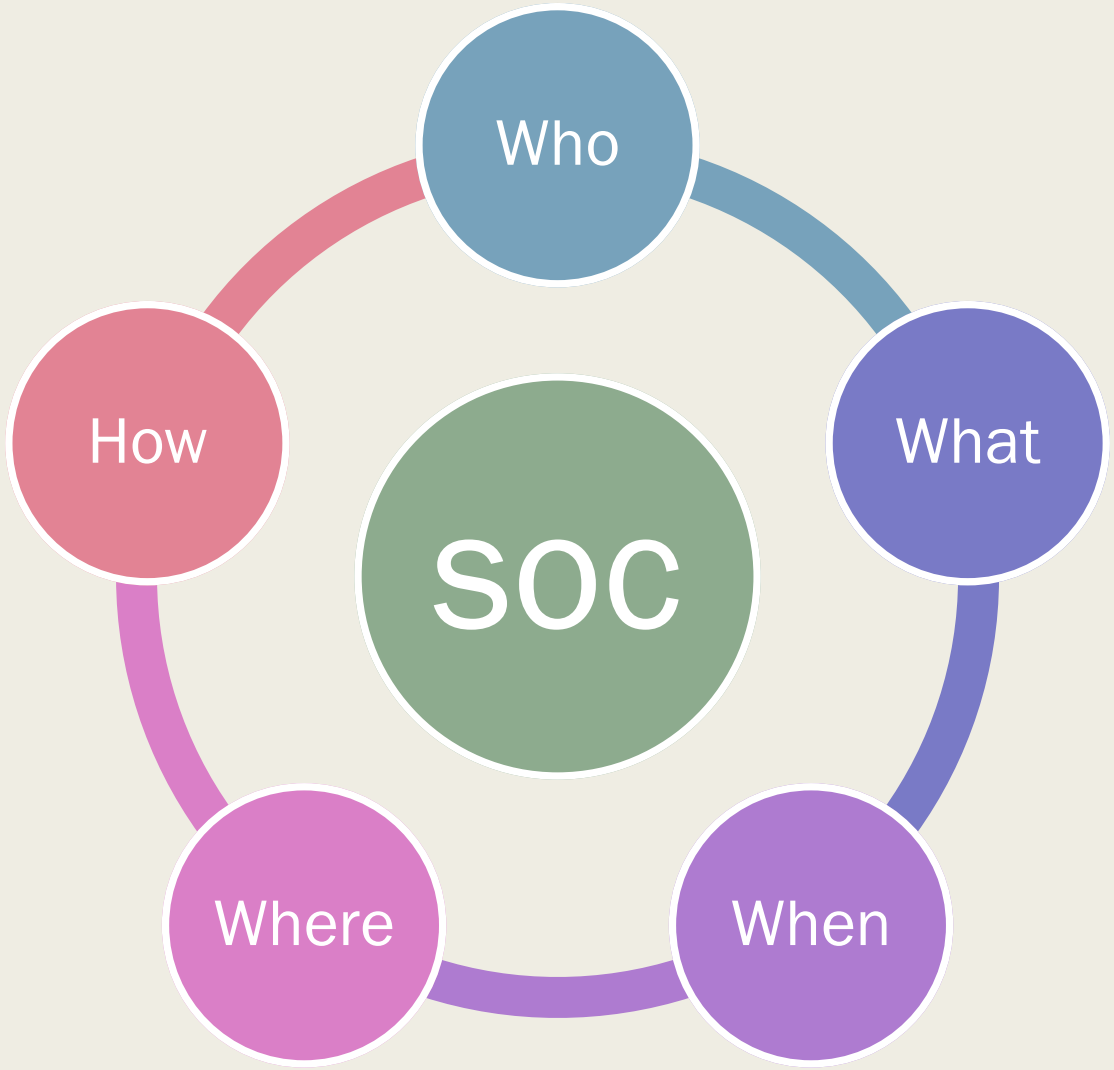


مرکز عملیات امنیت



- مجموعه تیم کارشناسان و تحلیل گران امنیتی که طبق یک مجموعه روال های مشخص به پایش رویدادهای موجود در سازمان توسط تکنولوژی های مجتمع و یکپارچه اقدام می نمایند تا حوادث امنیتی را شناسایی نموده و به آنها پاسخ دهند.

حادثه امنیتی



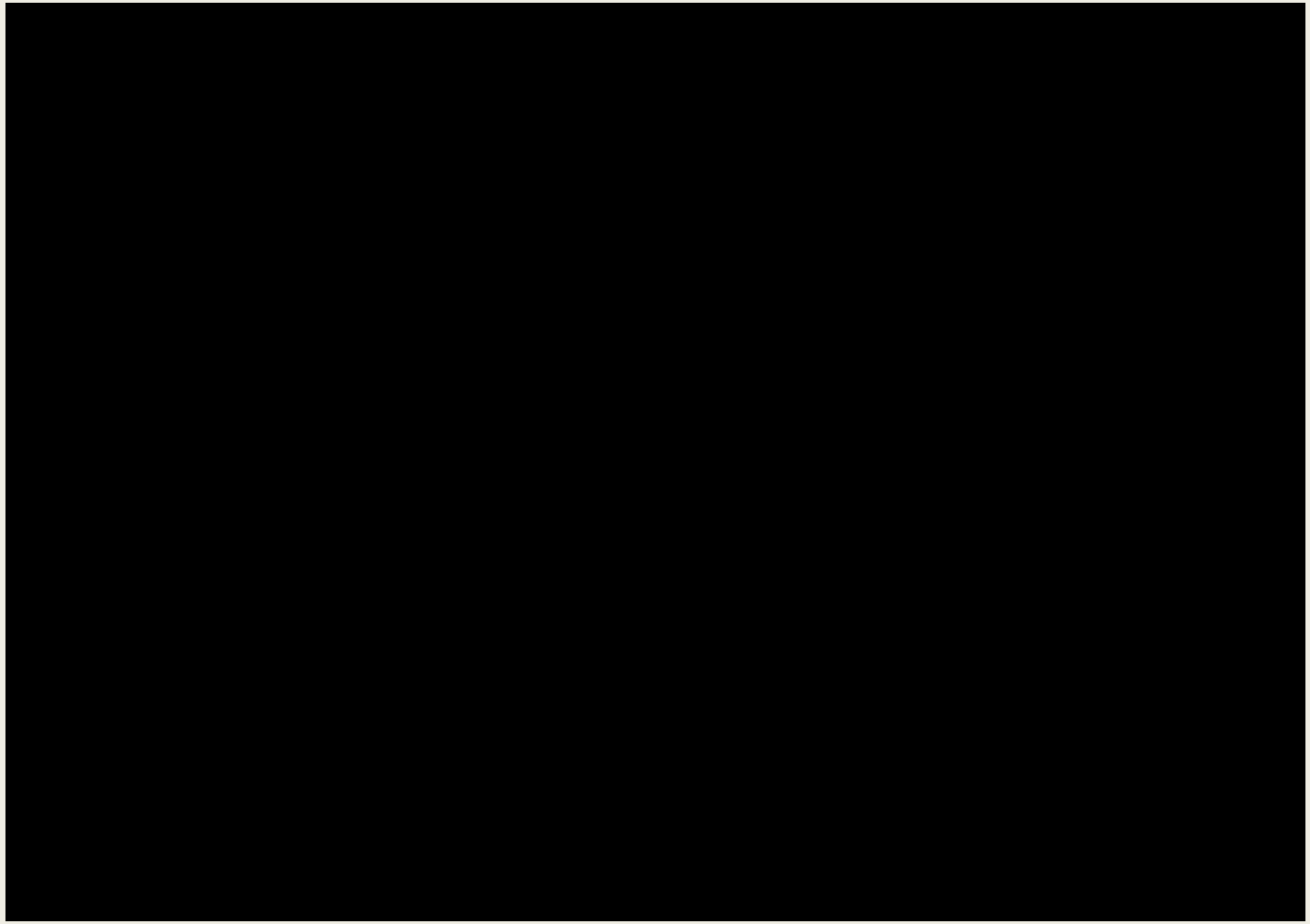
ارتباطات مرکز عملیات امنیت

ویژگی های فنی سامانه کورلاگ

سیستم عامل	• لینوکس سفارشی سازی شده
زبان برنامه نویسی	• C++، Java، C#
پایگاه داده	• Postgre، Oracle، noSQL
Agentاختصاصی	• مدیریت بلادرنگ رخدادهای ویندوزی با قابلیت فیلترینگ پیشرفته
پایگاه دانش گسترده	• پشتیبانی از 100 سنسور و 143000 نوع رخداد
کارایی بالا	• جمع آوری 30000 رخداد در ثانیه

بهین راهکار

شهپاد در رسانه ها



شهپاد در PressTV

دعوت به همکاری

Job@BehinRahkar.com

www.BehinRahkar.com

با سپاس