



# OSSIM – Monitorando ameaças tecnológicas em tempo real

Alexandro Silva  
[alexos@ibliss.com.br](mailto:alexos@ibliss.com.br)  
<http://www.ibliss.com.br>

# Quem é esse “cabra”?



- Gerente de Operações na iBLISS Segurança e Inteligência
- Professor
- Co-fundador da Nullbyte Security Conference





Ferramentas de proteção  
estão preparadas para  
acompanhar a evolução  
das ameaças?

# Ameaças



Malicious Gaming App Infects More than 1 Million

Android Users

📅 Sunday, July 12, 2015 👤 Swati Khandelwal

Apple Mac OS X Vulnerability Allows Attackers to Hack your Computer

📅 Wednesday, July 22, 2015 👤 Mohit Kumar

600TB MongoDB Database 'accidentally' exposed on the

Internet

📅 Wednesday, July 22, 2015 👤 Swati Khandelwal

Java Zero-day vulnerability exploited in the Wild

📅 Tuesday, July 14, 2015 👤 Mohit Kumar

Oops! Adult Dating Website Ashley Madison Hacked; 37

Million Accounts Affected

📅 Tuesday, July 21, 2015 👤 Swati Khandelwal

Oh Gosh! Four Zero Day Vulnerabilities Disclosed in Internet Explorer

📅 Friday, July 24, 2015 👤 Swati Khandelwal

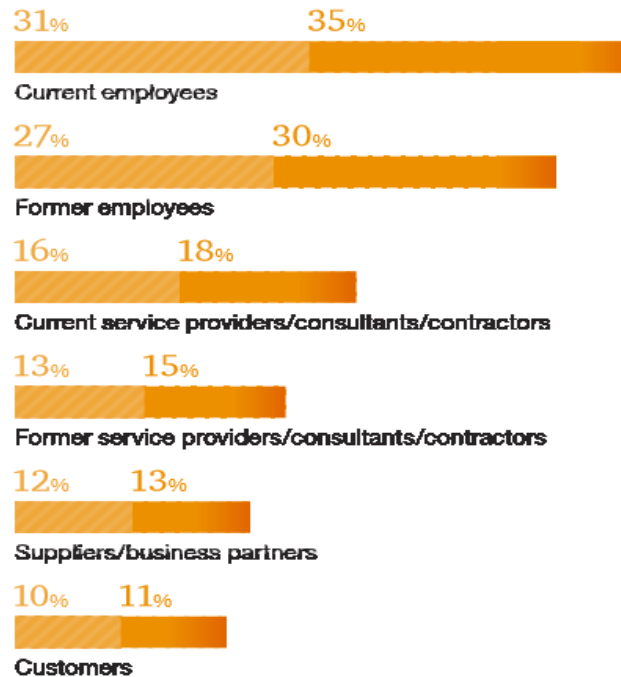
'Hacking Team' Gets Hacked! 500GB of Data Dumped Over the Internet

📅 Sunday, July 05, 2015 👤 Swati Khandelwal

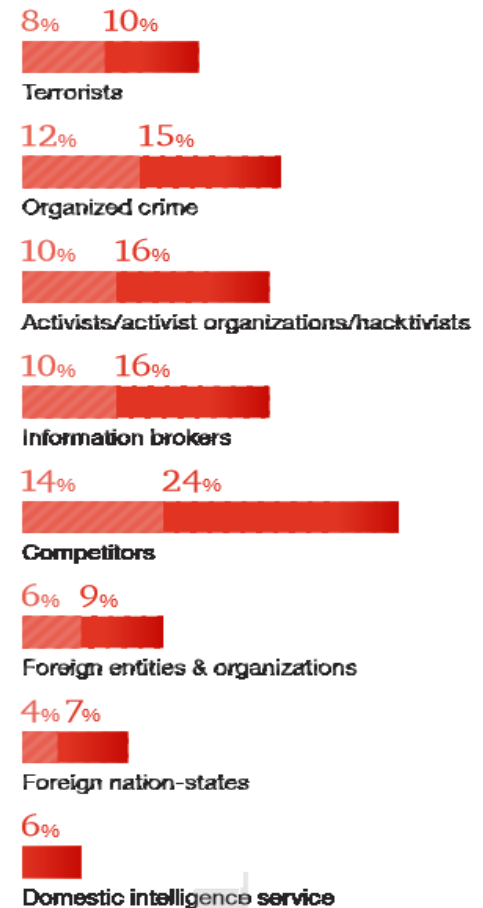
# Ameaças Externas vs Ameaças Internas



## Insiders



## Outsiders



**Figure 6**  
**Insiders vs. outsiders**  
*Sources of security incidents, 2013–2014*

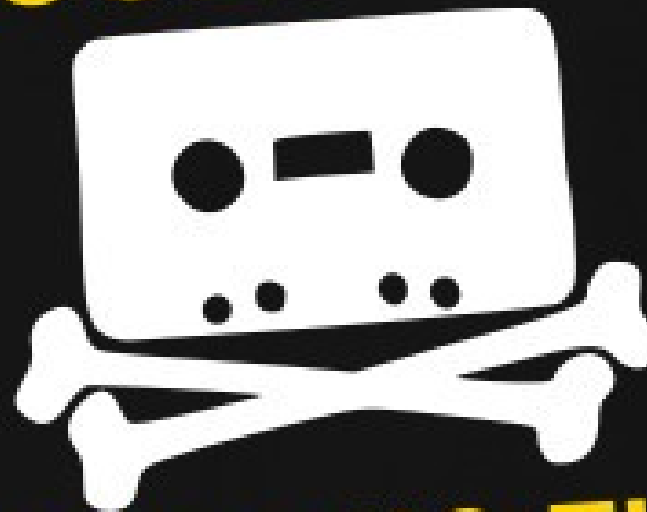
Managing cyber risks in an interconnected world

<http://www.dol.gov/ebsa/pdf/erisaadvisorycouncil2015security3.pdf>

# Ameaças



**RESPONSIBLE  
DISCLOSURE**

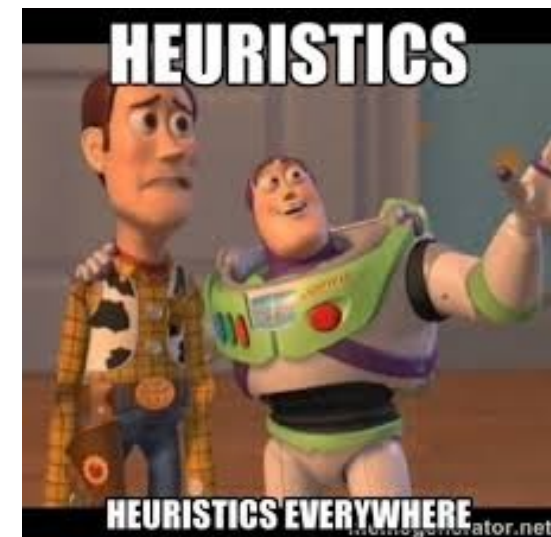
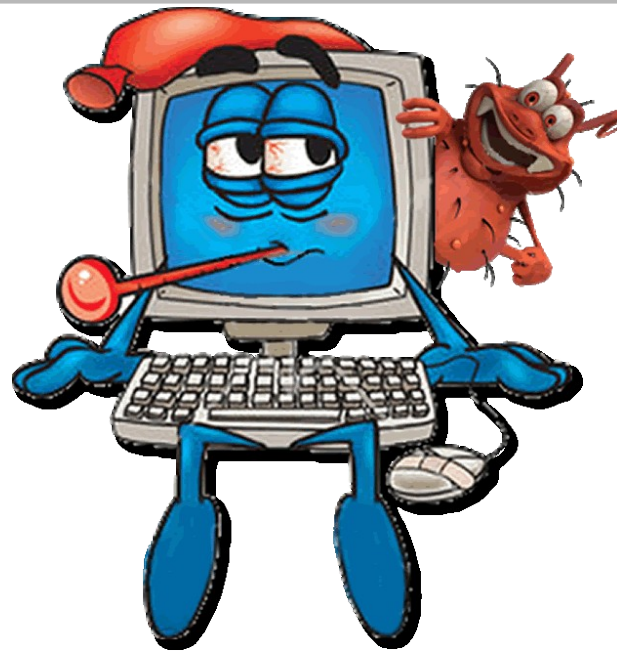


**IS KILLING THE  
0-DAY INDUSTRY**



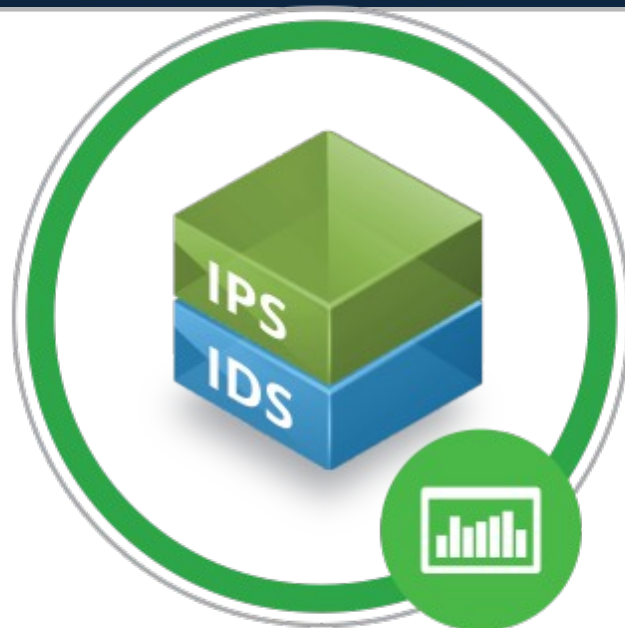
Como vocês se  
previnem hoje?

# Prevenção

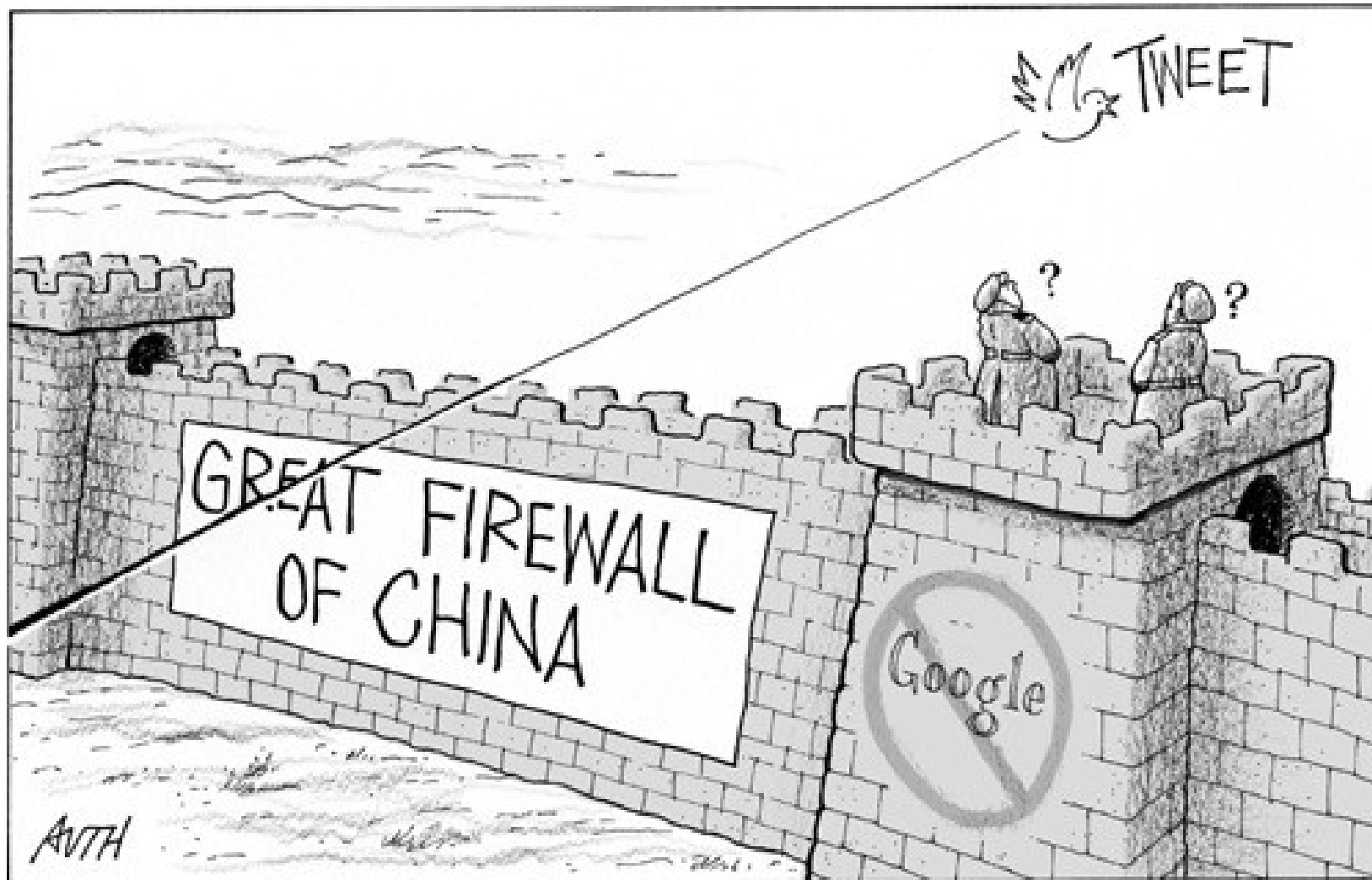




# Prevenção



# Prevenção



3-25-10 THE PHILADELPHIA INQUIRER. ILLUSTRATION BY AVTH



Como se prevenir?



## Usando processos e procedimentos

# O processo



- ✓ Planejar
- ✓ Auditar
- ✓ Corrigir
- ✓ Monitorar

# Prevenção



- Auditar
  - Ativos
  - Aplicações
  - Sistemas
  - Pessoas
- Gerenciamento de ameaças tecnológicas
- TDI
- Monitoração continuada

# Cenário



Foi possível identificar que em certos horários do dia, ocorre um grande fluxo de pacotes saindo da rede interna para Internet deixando a rede lenta.

Após horas de análise Severino, o Sysadmin, identificou o servidor comprometido e localizou os seguintes arquivos dentro do diretório /tmp :

- Jonh the ripper
- Shadows e Passwd
- Um arquivo contendo senhas “crackeadas”



# Monitoração Contínua de Ameaças



# Security Information and Event Management (SIEM)



Coleta, normaliza e relaciona informações enviada de diversas origens:

- ✓ Firewalls
- ✓ Servidores
- ✓ IDS/IPS
- ✓ Aplicações

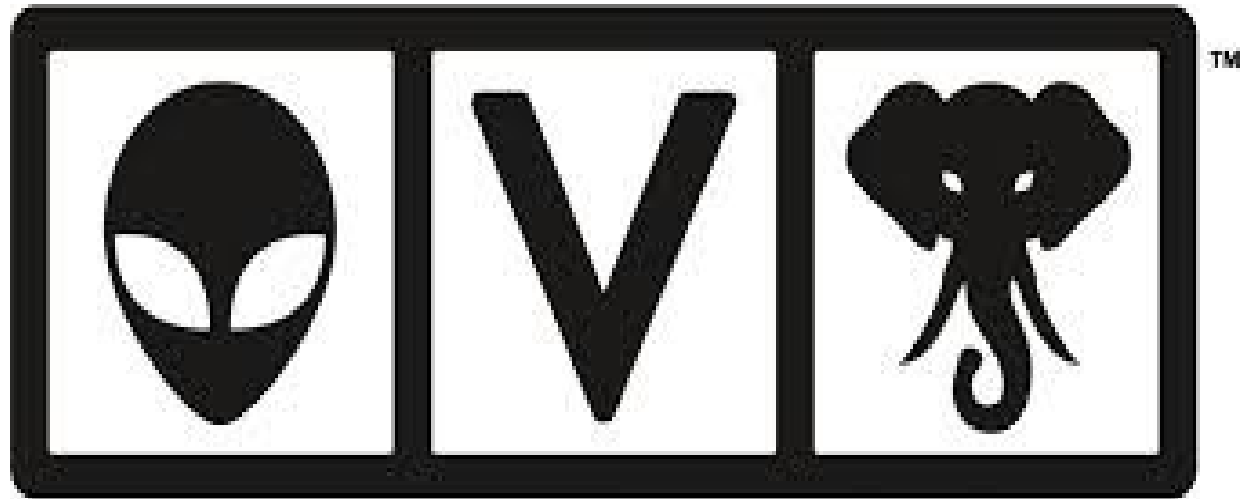
# Security Information and Event Management (SIEM)



A partir da correlação desses eventos é possível gerar várias ações:

- ✓ Alertas (email, SMS, etc)
- ✓ Bloqueios
- ✓ Abertura de tickets
- ✓ Relatórios

# Security Information and Event Management (SIEM)



**ALIEN VAULT OSSIM**

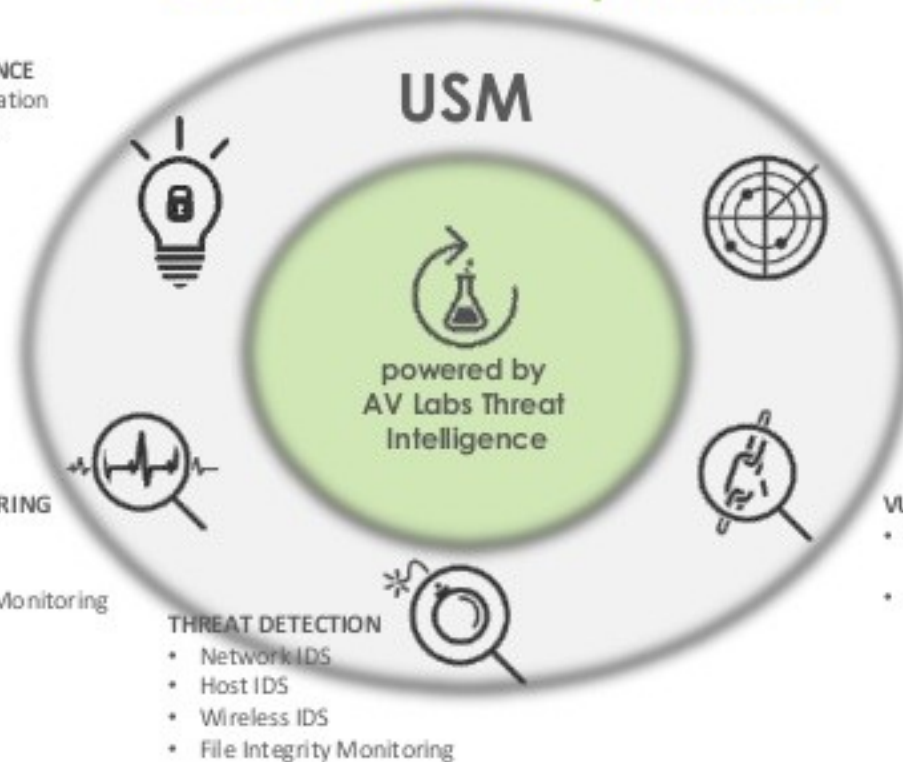
# Security Information and Event Management (SIEM)



## USM Product Capabilities

### SECURITY INTELLIGENCE

- SIEM Event Correlation
- Incident Response



### ASSET DISCOVERY

- Active Network Scanning
- Passive Network Scanning
- Asset Inventory
- Host-based Software Inventory

### BEHAVIORAL MONITORING

- Log Collection
- Netflow Analysis
- Service Availability Monitoring

### THREAT DETECTION

- Network IDS
- Host IDS
- Wireless IDS
- File Integrity Monitoring

### VULNERABILITY ASSESSMENT

- Continuous Vulnerability Monitoring
- Authenticated / Unauthenticated Active Scanning



## Arquitectura

# Alienvault OSSIM



- ✓ PRADS - Identifica hosts e serviços passivamente.
- ✓ OpenVAS - Análise de vulnerabilidade e correlação cruzada com alertas de IDS
- ✓ Snort - Detecção de intrusão também usado para correlação com Nessus.
- ✓ Suricata - Sistema de detecção de intrusão padrão do OSSIM

# Alienvault OSSIM



- ✓ Tcptrack – Obtém informações sobre sessão para correlação de ataques.
- ✓ Nagios - Monitoramento de ativos
- ✓ OSSEC - Sistema de detecção de intrusão para hosts
- ✓ Munin - Análise de tráfego de rede .
- ✓ NFSen/NFDump - Coleta e analisa informações de NetFlow.
- ✓ FProbe, gera o NetFlow de dados capturados.

# Alienvault OSSIM



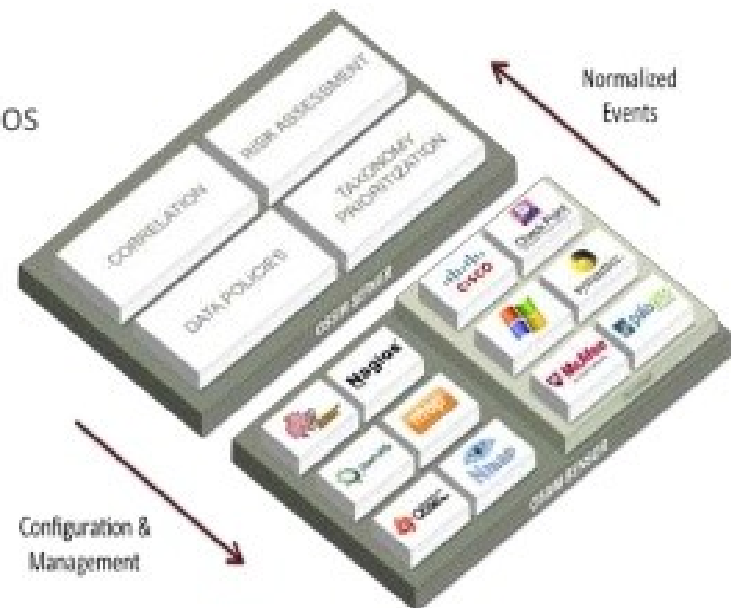
## ALIENVAULT USM ARCHITECTURE

Embedded tools:

- Asset discovery: Nmap, Prads
- Behavioral monitoring: Netflow, Ntop, Nagios
- Threat detection: Snort, Suricata, OSSEC
- Vulnerability assessment: Openvas

External collectors:

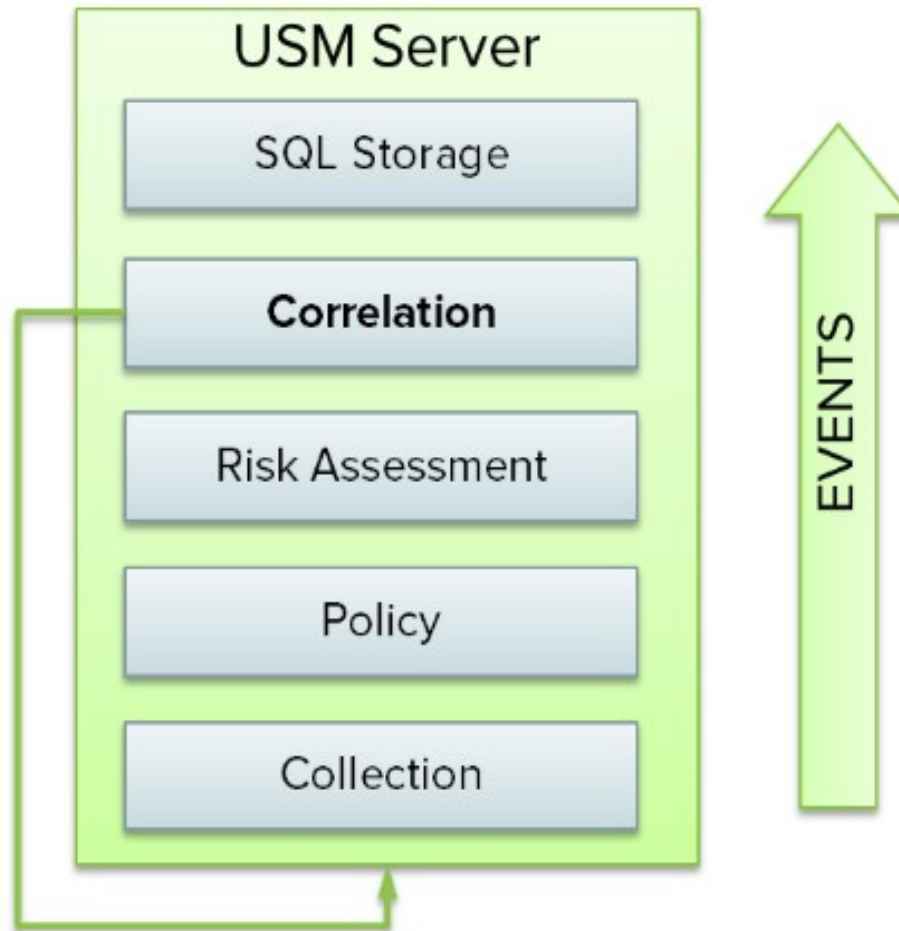
- Syslog, FTP, SCP, NFS
- Samba, SNMP, WMI, LEA
- SDEE, SQL, Unix Socket





# Alienvault OSSIM

## Correlação de Eventos



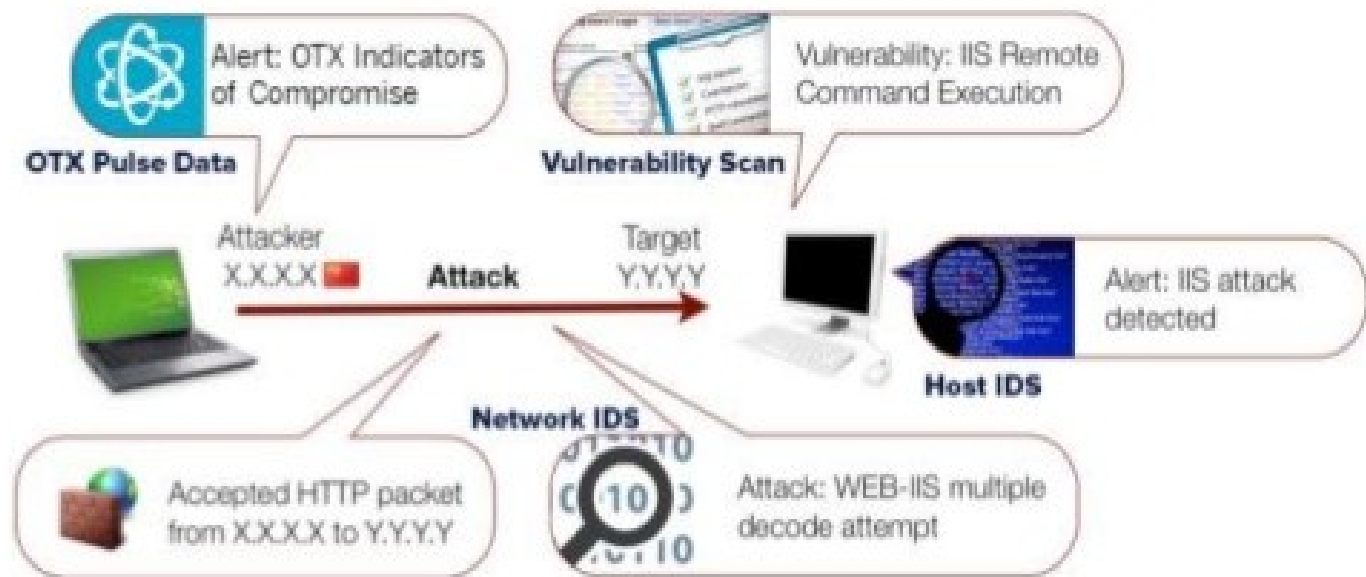
# Alienvault OSSIM

## Correlação de Eventos



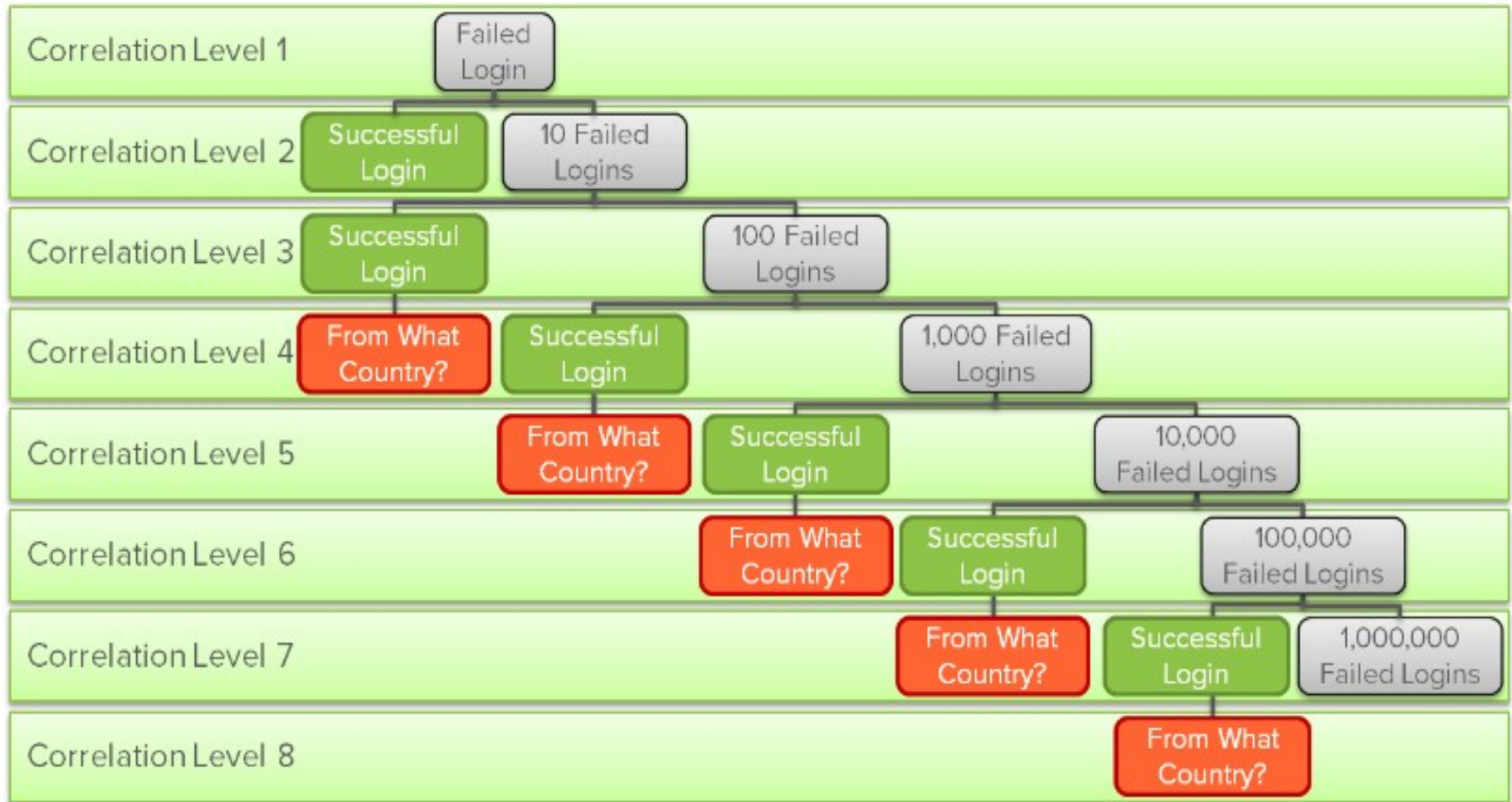
### AlienVault Event Correlation

- AlienVault USM correlates events from multiple sources, crossing HIDS alerts with information collected from embedded detectors and external sources.

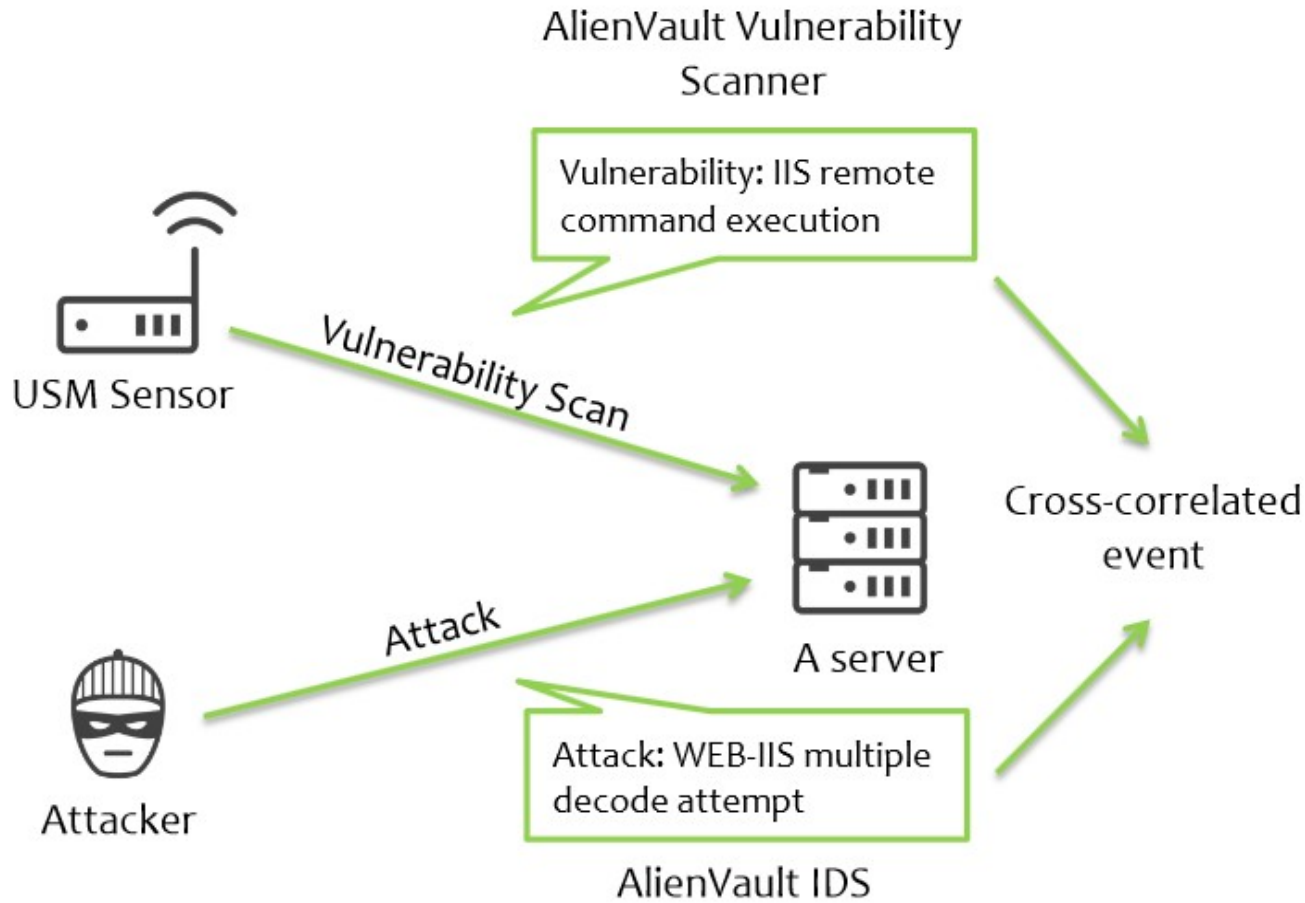


# Alienvault OSSIM

## Brute force



# Alienvault OSSIM Cross-correlação





## Casos



# Fraudes



## Infraestructura



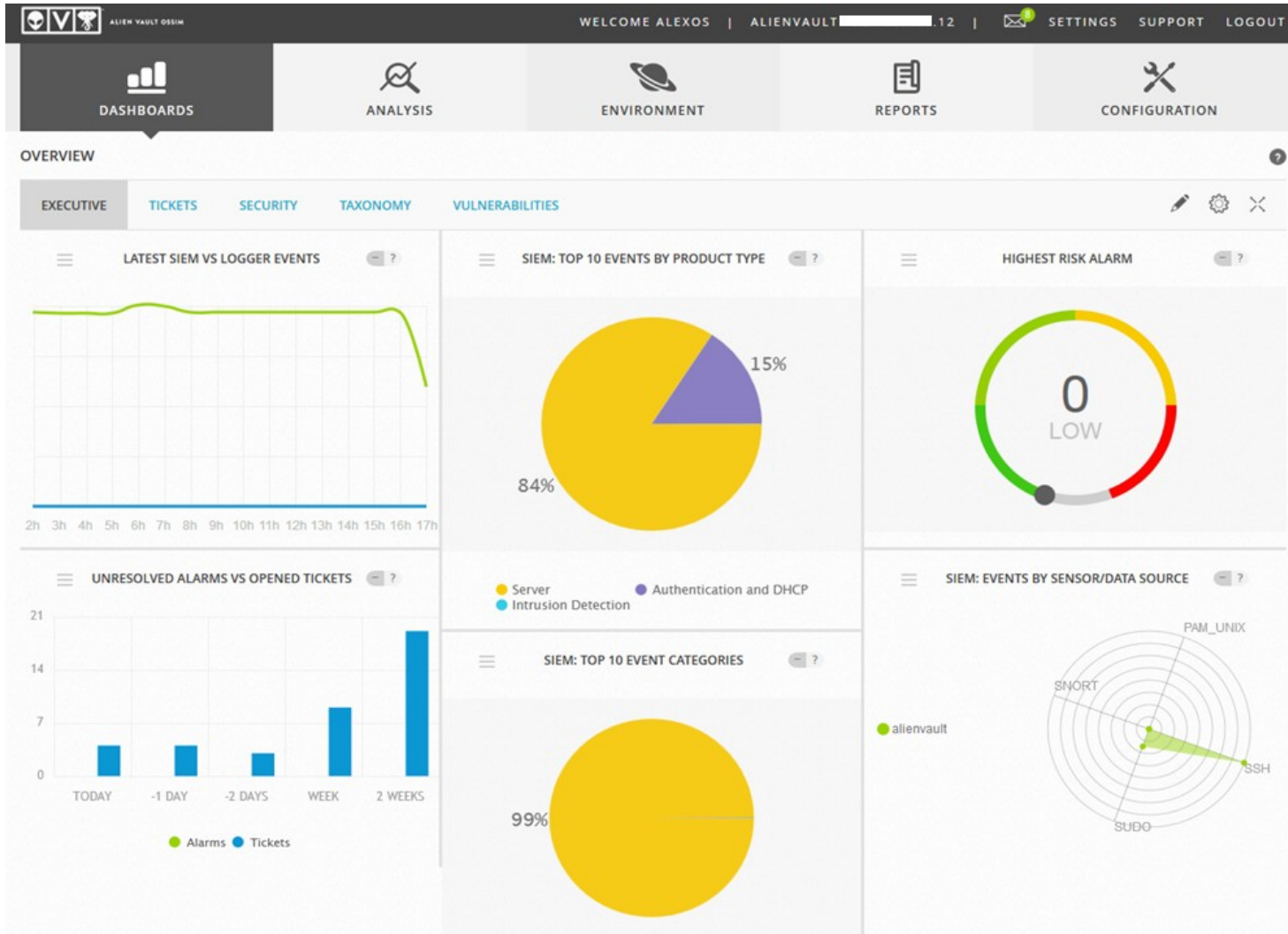
## Segurança





# Hands On

# Ferramenta SIEM



# Ferramenta SIEM



DASHBOARDS

ANALYSIS

ENVIRONMENT

REPORTS

CONFIGURATION

SIEM
REAL-TIME

Signature
GO
?

SHOW EVENTS

- Last Day
- Last Week
- Last Month
- Date Range

-

DATA SOURCES

RISK

SENSORS

TAXONOMY: PRODUCT TYPE

TAXONOMY: EVENT CATEGORY

Recon

TAXONOMY: SUB CATEGORY

IP REPUTATION ACTIVITY

IP REPUTATION SEVERITY

SEARCH CRITERIA CLEAR

Recon x
Last Day x

+ MORE FILTERS

ADVANCED SEARCH

EVENTS
GROUPED
TIMELINE

SHOW TREND GRAPH  Off

DISPLAYING EVENTS 1-5 OF ABOUT 5 MATCHING YOUR SELECTION. 210,120 TOTAL EVENTS IN DATABASE.

SIGNATURE	DATE GMT-3:00	SENSOR	SOURCE	DESTINATION	ASSET S + D	RISK
snort: "ET SCAN NMAP -sS window 1024"	2015-05-26 10:48:45	alienvault	185.35.62.11:57391	:443	2->2	<div style="width: 100px; height: 10px; background-color: #ccc; border: 1px solid #ccc; position: relative;"> <div style="width: 0%; height: 100%; background-color: #0070c0; position: absolute; left: 0;"></div> </div> 0
snort: "ET SCAN NMAP -sS window 1024"	2015-05-26 09:40:24	alienvault	185.35.62.11:57391	alienvault:443	2->2	<div style="width: 100px; height: 10px; background-color: #ccc; border: 1px solid #ccc; position: relative;"> <div style="width: 0%; height: 100%; background-color: #0070c0; position: absolute; left: 0;"></div> </div> 0
snort: "ET SCAN NMAP -sS window 1024"	2015-05-26 09:40:10	alienvault	5.231.220.251:37798	:80	2->2	<div style="width: 100px; height: 10px; background-color: #ccc; border: 1px solid #ccc; position: relative;"> <div style="width: 0%; height: 100%; background-color: #0070c0; position: absolute; left: 0;"></div> </div> 0
snort: "ET SCAN NMAP -sS window 1024"	2015-05-26 00:17:52	alienvault	61.240.144.65:60000	alienvault:443	2->2	<div style="width: 100px; height: 10px; background-color: #ccc; border: 1px solid #ccc; position: relative;"> <div style="width: 0%; height: 100%; background-color: #0070c0; position: absolute; left: 0;"></div> </div> 0
snort: "ET SCAN NMAP -sS window 1024"	2015-05-25 22:58:33	alienvault	108.61.83.115:45736	:80	2->2	<div style="width: 100px; height: 10px; background-color: #ccc; border: 1px solid #ccc; position: relative;"> <div style="width: 0%; height: 100%; background-color: #0070c0; position: absolute; left: 0;"></div> </div> 0

< PREVIOUS
NEXT >



**THANK YOU**

**GRACIAS**

**ARIGATO**

**SHUKURIA**

**JUSPAXAR**

**DANKSCHEEN**

**BIYAN SHUKRIA**

**TASHAKKUR ATU**

**YAQHANYELAY**

**SUKSAMA**

**GRAZIE**

**MEHRBANI**

**PALDIES**

**BOLZIN**

**MERCI**

**TINGKI**

**GOZAIMASHITA**

**EFCHARISTO**

**KOMAPSUMNIDA**

**MAAKE**

**LAH**

**SPASIBO**

**SNACHALHUYA**

**NUHUN**

**CHALTU**

**WABEEJA**

**MAITEKA**

**HUI**

**YUSPAGARATAM**

**DIHANYABAAD**

**ANIRIA**

**ATTO**

**EKHMET**

**MERSI**

**SPASIBO**

**DENKAUJA**

**UNALCHEESH**

**HATUR GU**

**EROUJU**

**SIKOMO**

**HAKETAI**

**MIMMONCHAR**

**TAVTAPUCHI**

**MEDAWAGSE**

**BAIRKA**

**MERASTAWHY**

**GAEJTIO**

**AGUYJE**

**FAKAAUE**

**UNALCHALHYA**



# GAT

**Gerenciamento de Ameaças Tecnológicas**

Alexandro Silva

Rua Nestor Pestana, 30 cj 156

São Paulo-SP

+55 11 3255-3926 Tel

[www.ibliss.com.br](http://www.ibliss.com.br)

[alexos@ibliss.com.br](mailto:alexos@ibliss.com.br)