OSSIM – Monitorando ameaças tecnológicas em tempo real

Alexandro Silva
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

Prevenção

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

Managing cyber risks in an interconnected world

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

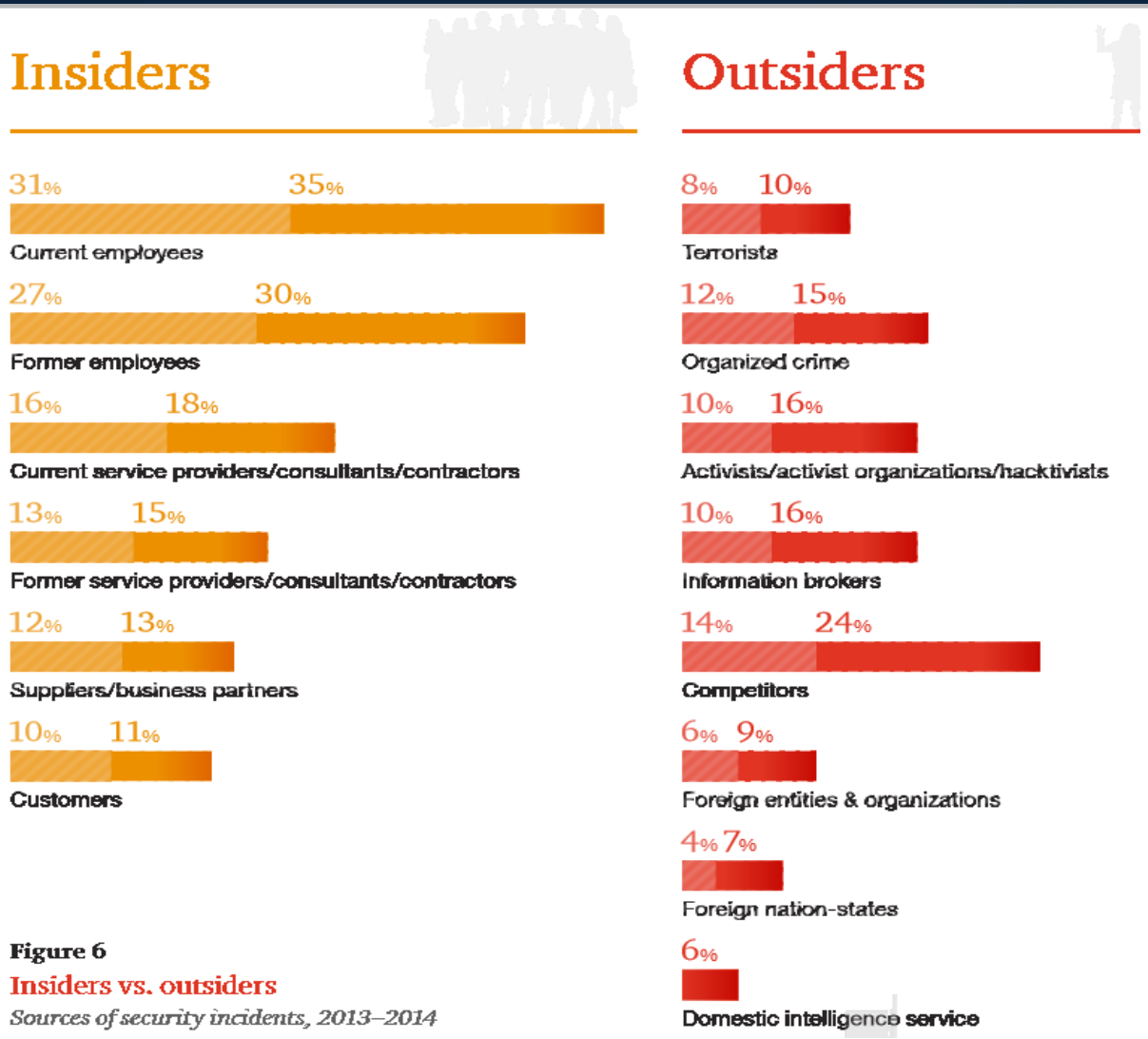
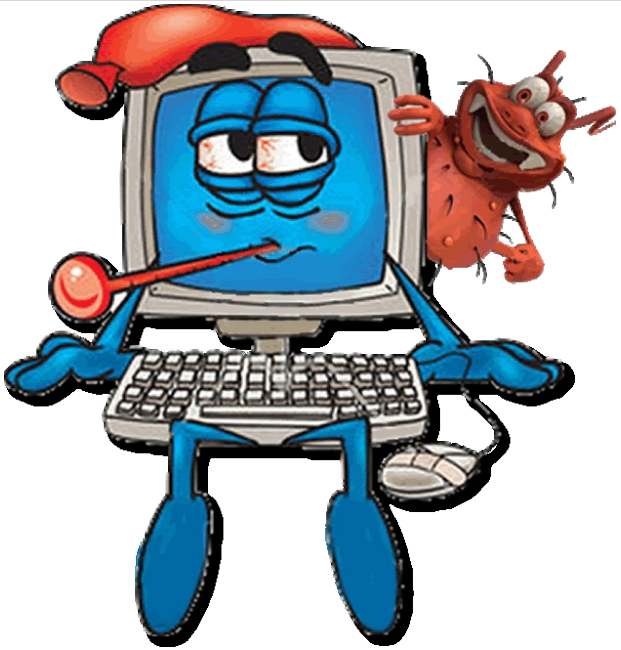


Figure 6
Insiders vs. outsiders
Sources of security incidents, 2013–2014

Ameaças

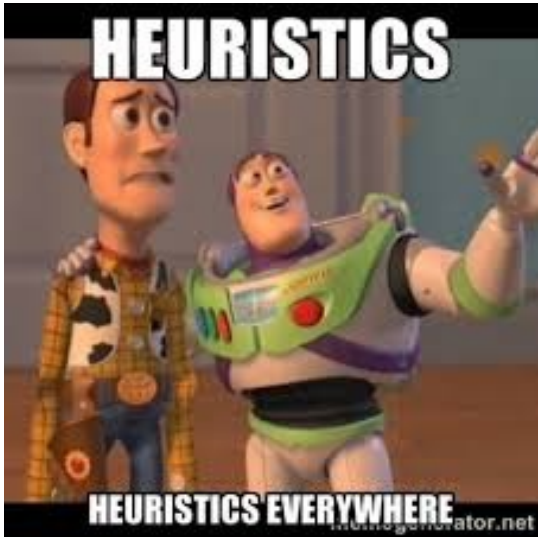
Como vocês se previnem hoje?

Prevenção



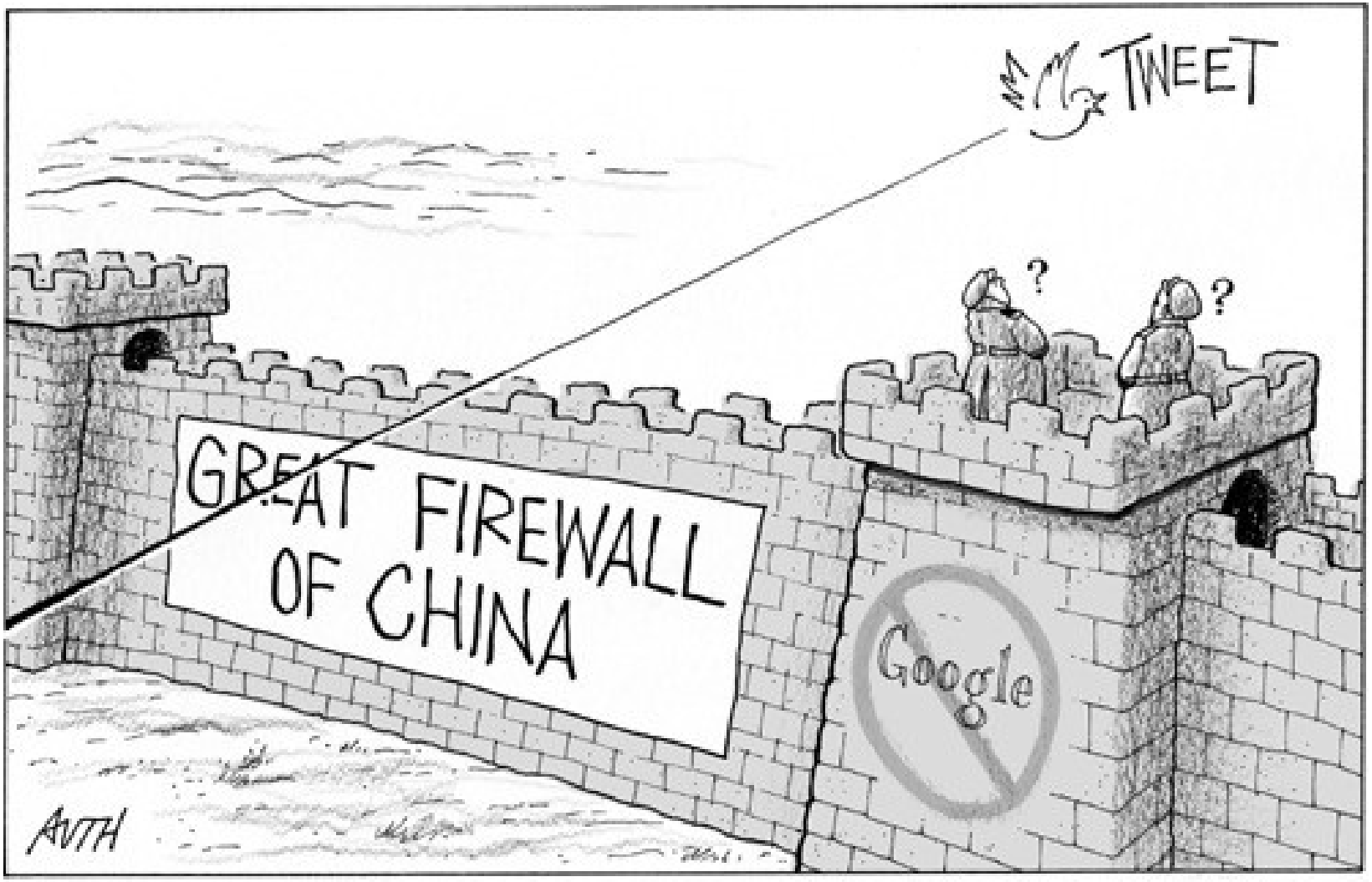

pattern
MATCHING


UPDATE


HEURISTICS
HEURISTICS EVERYWHERE

Prevenção

Prevenção



Prevenção

Como se previnir?

Prevenção

Usando processos e procedimentos

O processo

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

Prevenção

- Auditar
  - Ativos
  - Aplicações
  - Sistemas
  - Pessoas
- Gerencimento 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

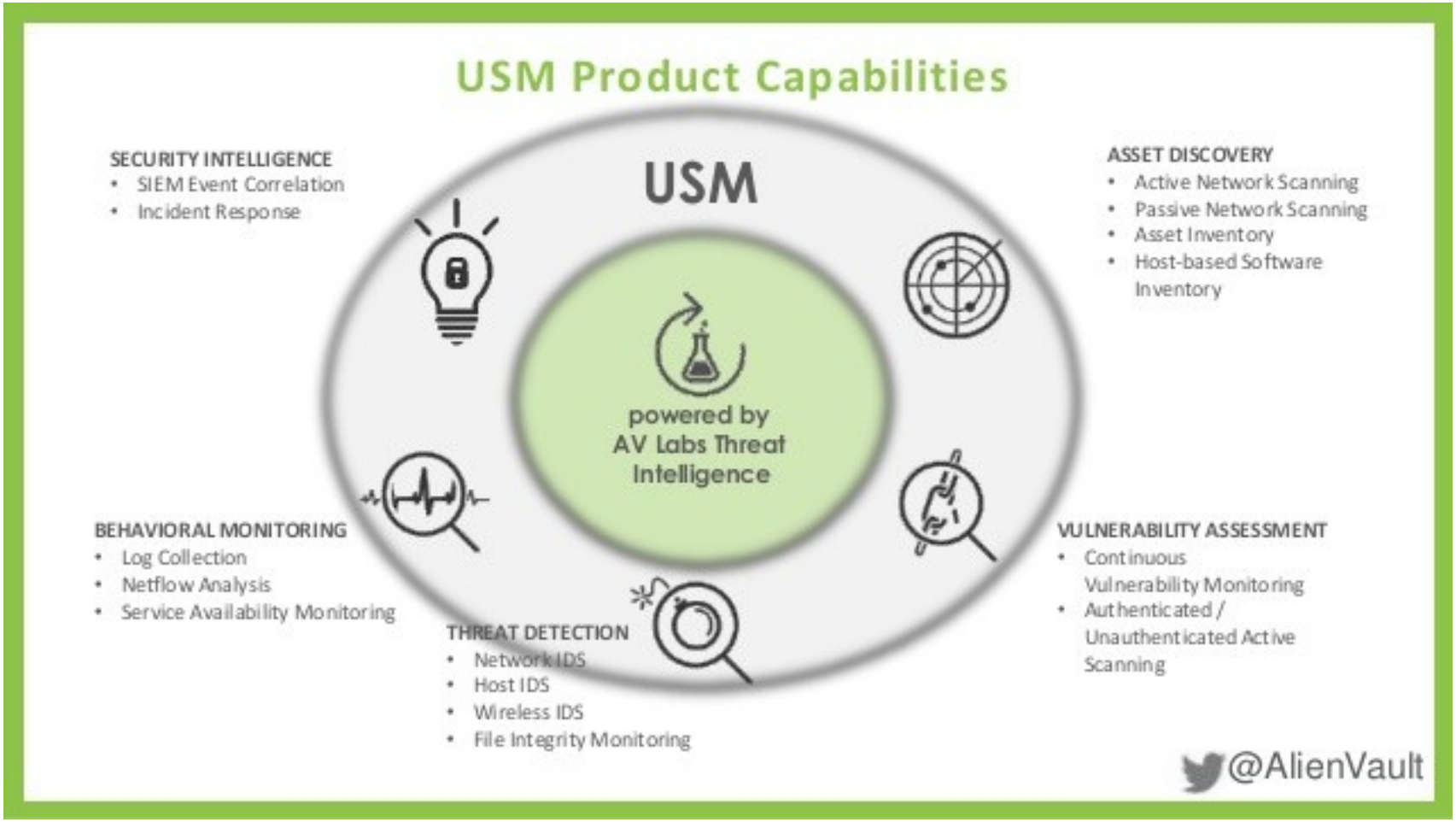
Security Information and Event Management (SIEM)

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)

Security Information and Event Management (SIEM)



Alienvault OSSIM

Arquitetura

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

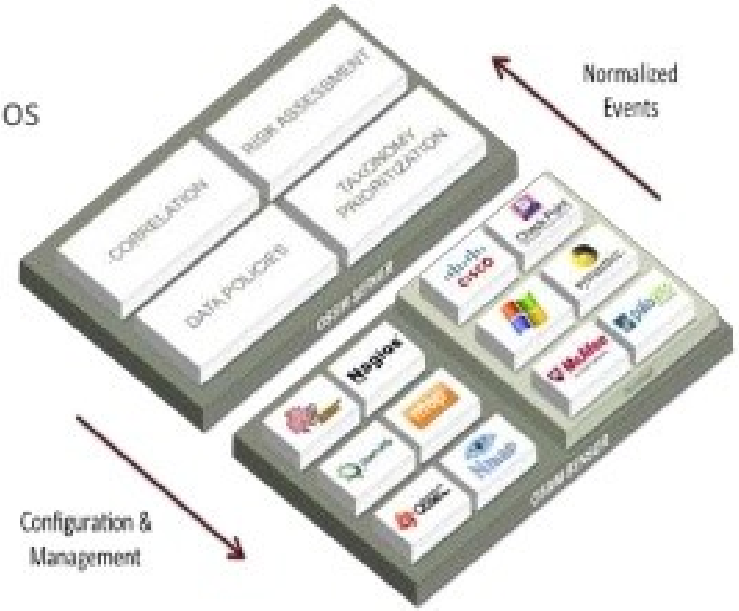
ALIENVAULT USM ARCHITECTURE

Embedded tools:

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

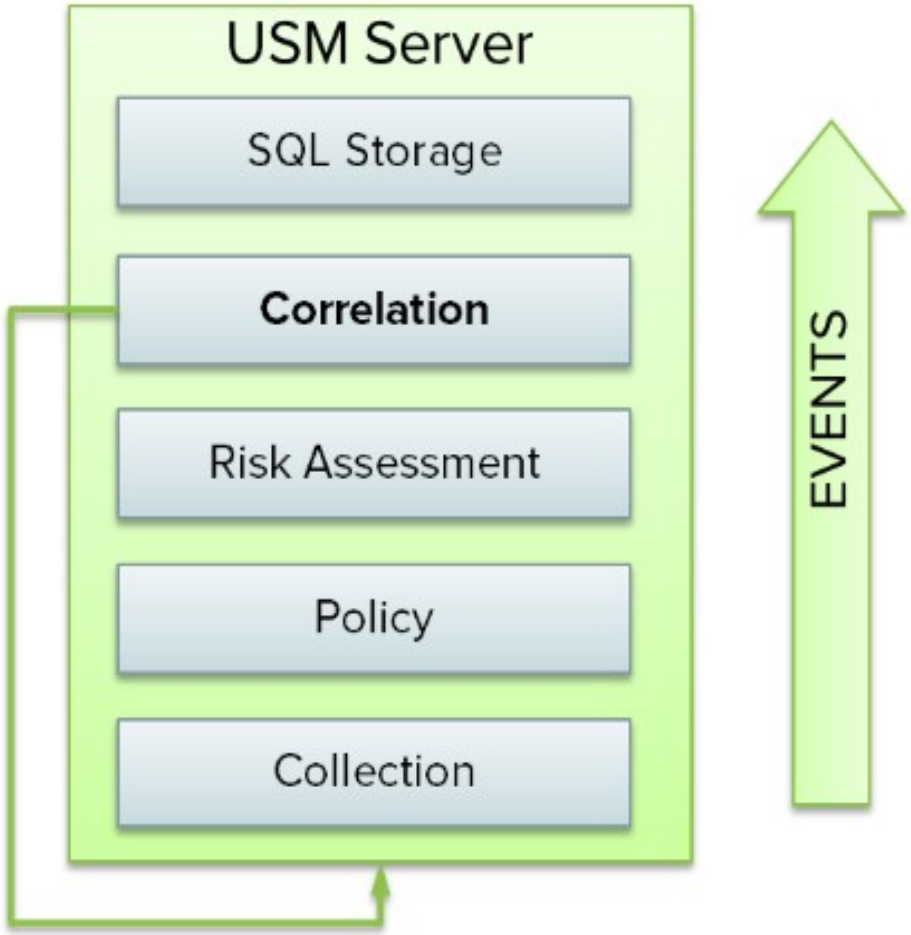
External collectors:

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



https://www.alienvault.com/doc-repo/usm/security-intelligence/AlienVault_Correlation_Reference_Guide.pdf

Alienvault OSSIM
Correlação de Eventos

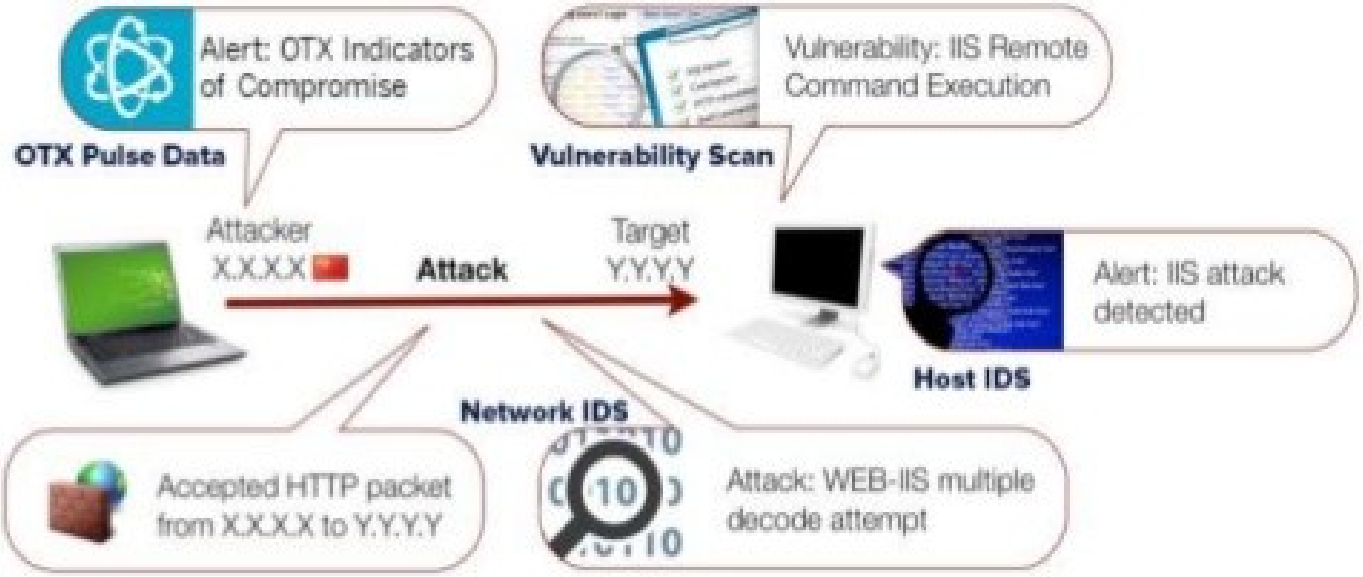


https://www.alienvault.com/doc-repo/usm/security-intelligence/AlienVault_Correlation_Reference_Guide.pdf

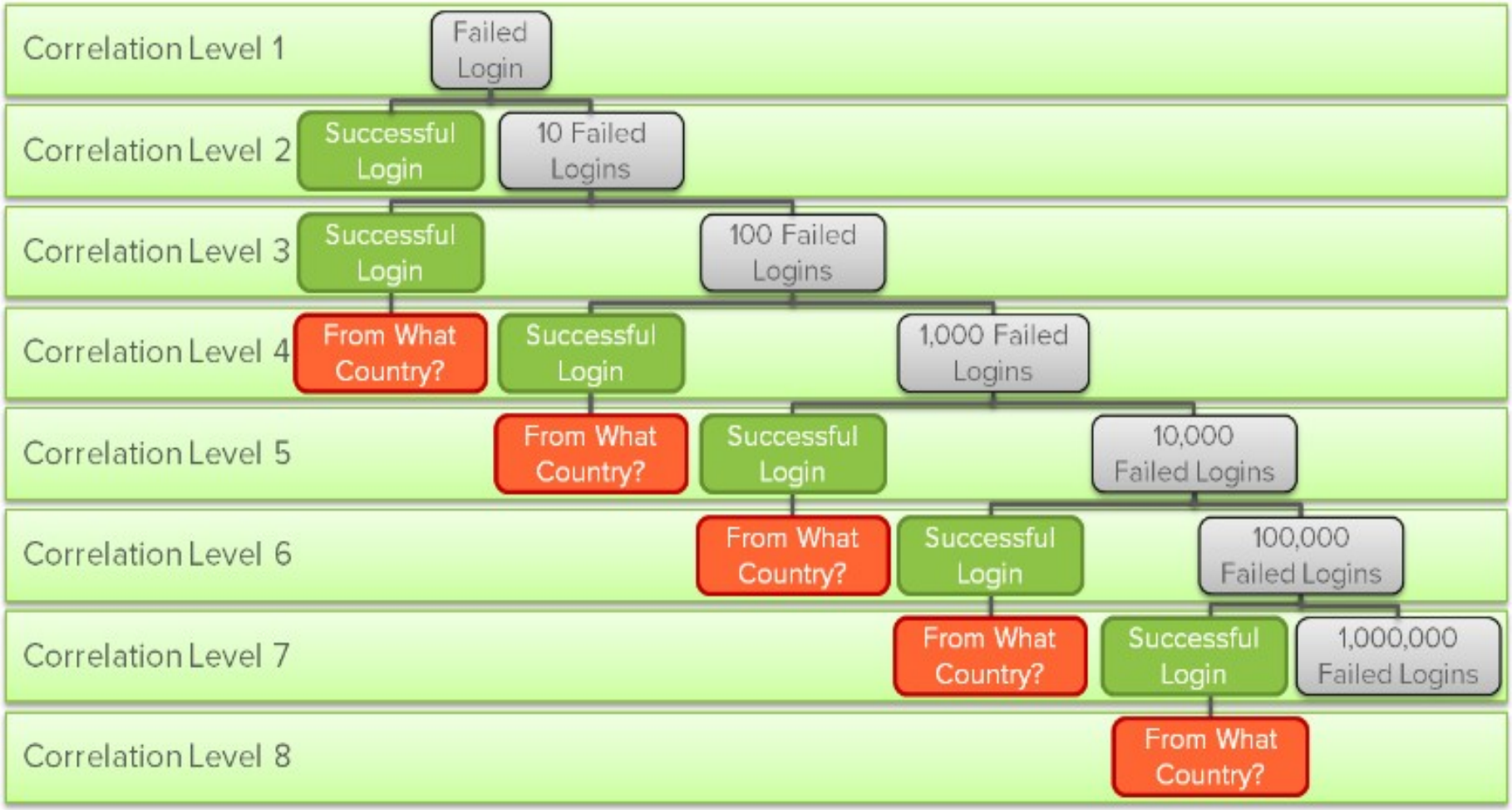
Alienvault OSSIM
Correlação de Eventos

AlienVault Event Correlation

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

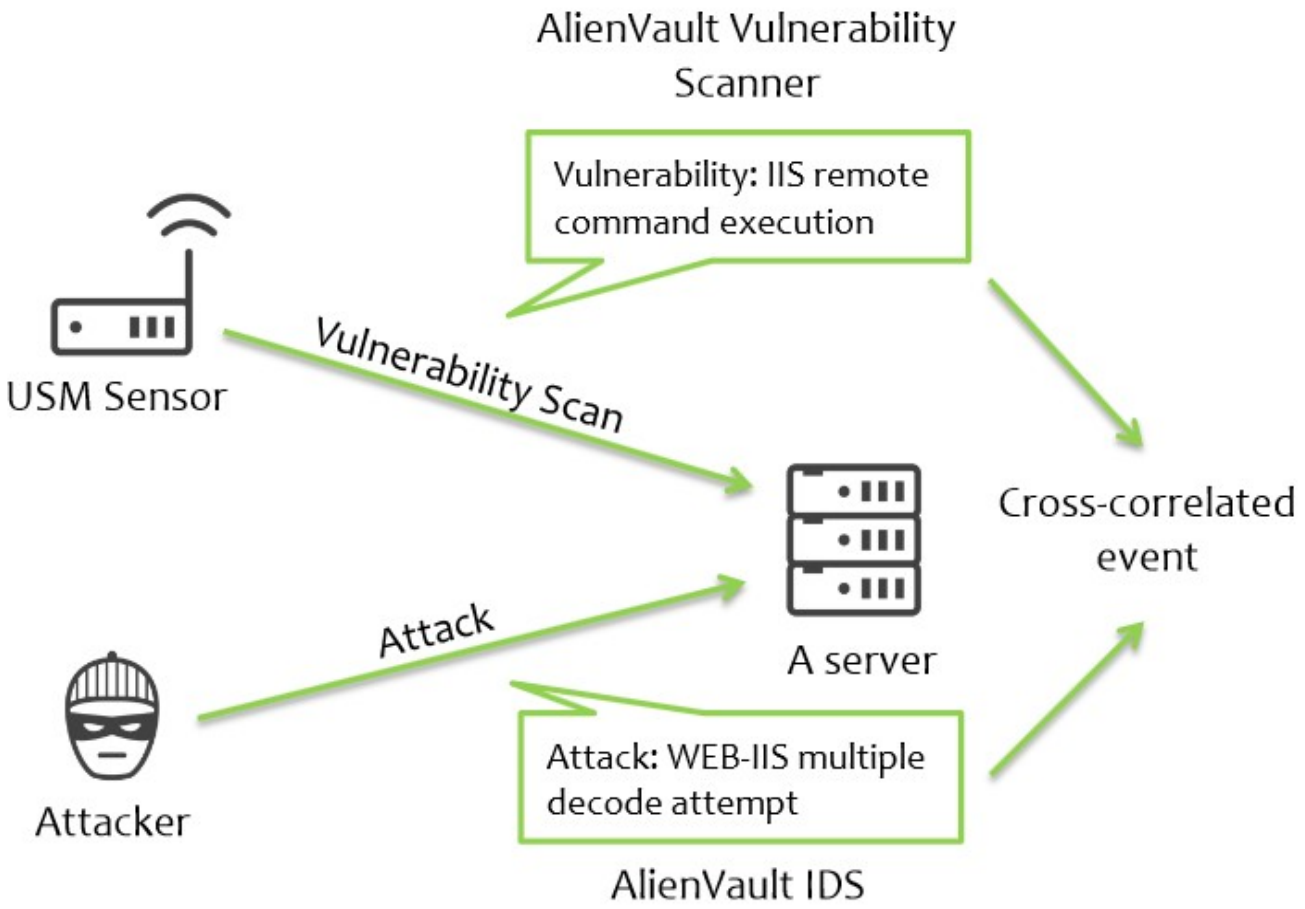


Alienvault OSSIM
Brute force



https://www.alienvault.com/doc-repo/usm/security-intelligence/AlienVault_Correlation_Reference_Guide.pdf

Alienvault OSSIM
Cross-correlação



https://www.alienvault.com/doc-repo/usm/security-intelligence/AlienVault_Correlation_Reference_Guide.pdf

Alienvault OSSIM

Casos

Alienvault OSSIM

Fraudes

Alienvault OSSIM

Infraestrutura

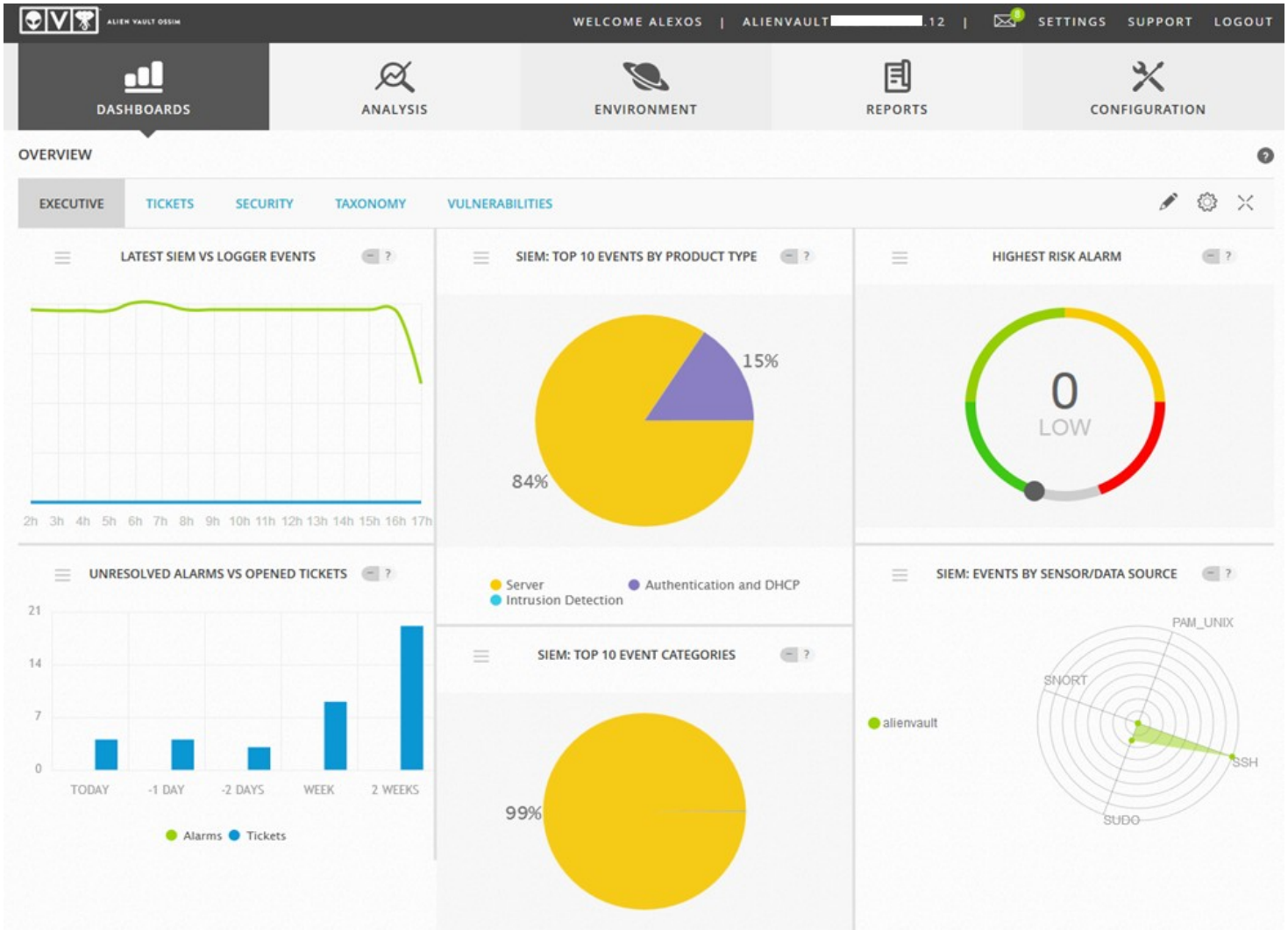
Alienvault OSSIM

Segurança

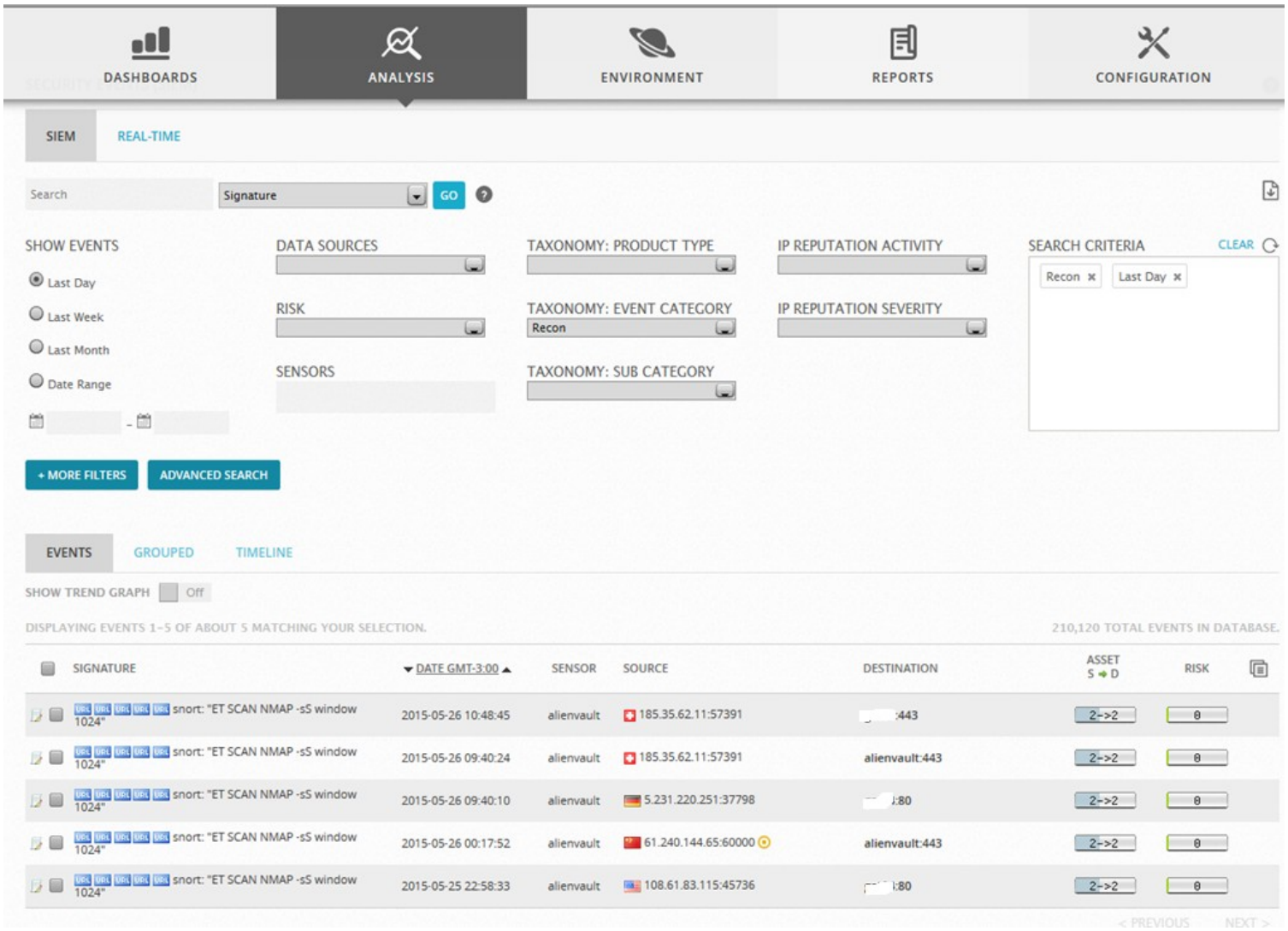
Alienvault OSSIM

Hands On

Ferramenta
SIEM



Ferramenta
SIEM




THANK
YOU
GRACIAS
ARIGATO
SHUKURIA
BOLZÏN
MERCI
BÏYAN
SHUKRIA
TINGKI
DANKSCHEEN
SPASSIBO
NUHUN
SNACHALHUYA
CHALTU
YAQHANYELAY
TASHAKKUR ATU
YUSPAGARÀTAM
WABEEJA
MAITEKA
HUI
SUKSAMA
EKHMET
GUI
HÀTUR
EKOJU
SIKOMO
MAKETAI
MINMONCHAR
DHANYABAAD
ANHIA
ATTO
MERSI
SPASIBO
DENKAUJA
NENACHALHYA
UNALCHÉESH
MAAKE
GRAZIE
MEHRBANI
PALDIES
LAH
SAINCO
MERASTAWHY
GAEJTHO
KOMAPSUMNIDA
TAVTAPUCH
MEDAWAGSE
GOZAIMASHITA
EFCHARISTO
AGUYJE
FAKAAUE
BAIKA
JUSPAXAR

iBLISS
SEGURANÇA & INTELIGÊNCIA

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
alexos@ibliss.com.br