TÓPICOS ESPECIAIS EM DEFESA CIBERNÉTICA

Professor Me. Vladimir Geraseev Junior

Fatec Centro Paula Souza Governo de São Paulo

Curso: TECNOLOGIA EM DEFESA CIBERNÉTICA

Disciplina: Tópicos Especiais em Defesa Cibernética

Sejam Bem Vindos!

Prof. Vladimir Geraseev Junior

PROF VLADIMIR GERASEEV JUNIOR

- **GRADUAÇÃO EM CIÊNCIAS DA COMPUTAÇÃO**
- **MESTRADO EM ENGENHARIA - UNITAU**

- EXPERIÊNCIA PROFISSIONAL:

- COMPANHIA DE INFORMÁTICA DE JUNDIAÍ – ARQUITETO DE REDES
- EMBRAER – GRUPO DE ENGENHARIA
- INSTITUTO NACIONAL DE PESQUISAS ESPACIAIS – INPE – ANALISTA DE REDES E SEGURANÇA
- IMPLEMENTAÇÃO DOS REQUISITOS DE SEGURANÇA CIBERNÉTICA PARA EQUIPAMENTOS PARA TELECOMUNICAÇÕES (ATO 77) – ANATEL
- CONSULTORIA EM CONDUÇÂO DE PENTESTS

PROF VLADIMIR GERASEEV JUNIOR

- EXPERIÊNCIA PROFISSIONAL ACADÊMICA.

- PROFESSOR NA FATEC TAUBATÉ
- PROFESSOR NA ETEC JACAREÍ
- PROFESSOR EM UNIVERSIDADES PARTICULARES (UNIP, UNIVAP, FAPI)

RESPOSTA A INCIDENTES DE SEGURANÇA COM FERRAMENTAS SIEM

Agenda

- **MODELOS DE SEGURANÇA.**
- Desafios atuais da segurança.
- *Intelligence Driven Security.*
- SIEM: definições e exemplos
- SIEM: arquitetura e casos de uso.
- Benefícios da Resposta a Incidentes com o uso de ferramentas SIEM.
- Conclusão.

- Segurança Física (Mainframes) – 60 – Hoje
  - Os perímetros de segurança eram claros.
  - As informações residiam em computadores e centros de processamento com acessos restritos.
  - A grande maioria dos usuários somente conseguiam visualizar as informações em seus terminais, que não as armazenavam.

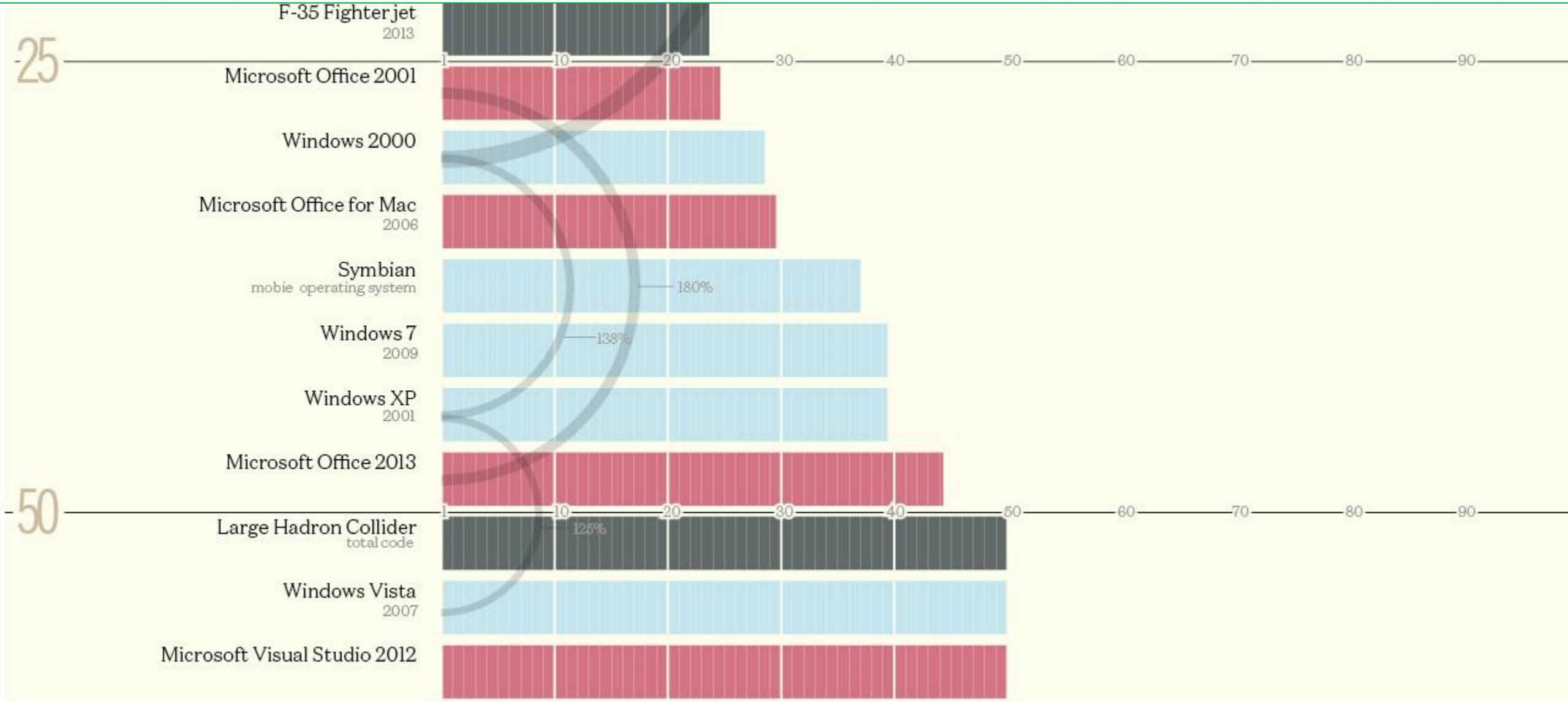
- Segurança de Redes (Sistemas Distribuídos) – 90 – Hoje
  - Com a ampliação das redes de computadores surgiram sistemas cliente-servidor aonde os dados trafegavam via rede entre um servidor e os computadores dos usuários.
  - Ameaças surgiram em relação ao tráfego de dados, como:
    - Interceptação;
    - Interrupção;
    - Modificação; e
    - Fabricação.

- Segurança na Internet (Sistemas Web) – 2000 – Hoje
  - Aplicações web cresceram e hoje fazem parte de praticamente toda empresa.
  - Os sistemas agora estão expostos ao mundo e com uma superfície de ataque muito maior: Internet e Extranets ampliam consideravelmente os antigos perímetros de proteção.

- Segurança Onipresente – Hoje!
  - Internet das Coisas, Big Data, Cloud, BYOD, Mobile...
    - Hoje o perímetro de segurança é muito difícil de se mapear.
    - Afinal, aonde estão as informações que precisam ser protegidas?

  - Os sistemas hoje apresentam três características que dificultam muito a sua segurança:
    - **Interconectividade**: com os sistemas acessíveis através da Internet, extranets e intranets a tarefa de projetar a segurança do software se tornou árdua, devido a ameaças distintas de cada um desses ambientes.
    - **Extensibilidade**: os sistemas de hoje precisam receber atualizações, funcionar com códigos externos (*plugins* e *add-ons),* interagir com os sistemas legados; tudo em nome da flexibilidade.
    - **Complexidade**: O aumento de funcionalidades e compatibilidades agrega valor ao sistema, mas em termos de segurança muitas vezes o torna difícil de gerenciar devido a sobreposições de pacotes de software, integrações e customizações de cada ambiente.

Fonte: https://freedom-to-tinker.com/blog/gem/software-security-trinity-trouble/



Fonte: http://www.informationisbeautiful.net/visualizations/million-lines-of-code/

- O mundo da segurança é marcado pela evolução contínua, no qual novos ataques têm como resposta novas formas de proteção, que levam ao desenvolvimento de novas técnicas de ataques, de maneira que um ciclo é formado.
- Isso ocorre porque o arsenal de defesa usado pela organização pode funcionar contra determinados tipos de ataques; porém, pode ser falho contra novas técnicas desenvolvidas para driblar esse arsenal de defesa.
- Deve se ter em mente que a segurança deve ser contínua e evolutiva!

Fonte: Segurança de Redes em Ambientes Cooperativos - Nakamura e Geus

- Os intrusos são mais espertos que você.

DESAFIOS ATUAIS

Fonte: http://taosecurity.blogspot.com.br/2006/02/bears-teach-network-security.html

- Os intrusos são imprevisíveis.

DESAFIOS ATUAIS

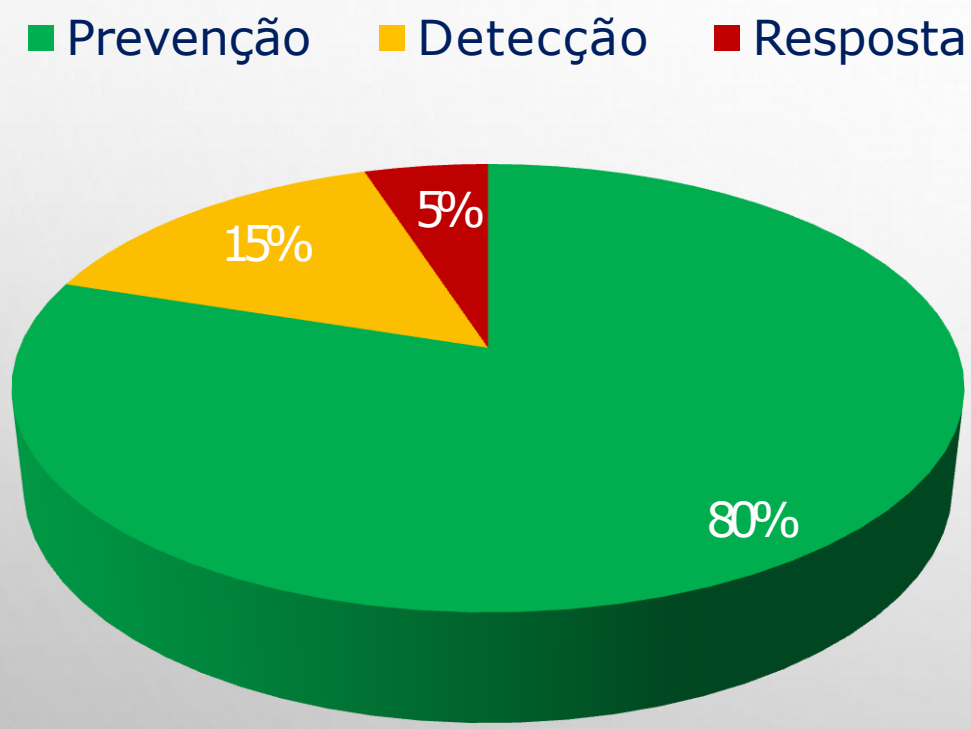
Fonte: http://taosecurity.blogspot.com.br/2006/02/bears-teach-network-security.html

- A prevenção eventualmente falha.

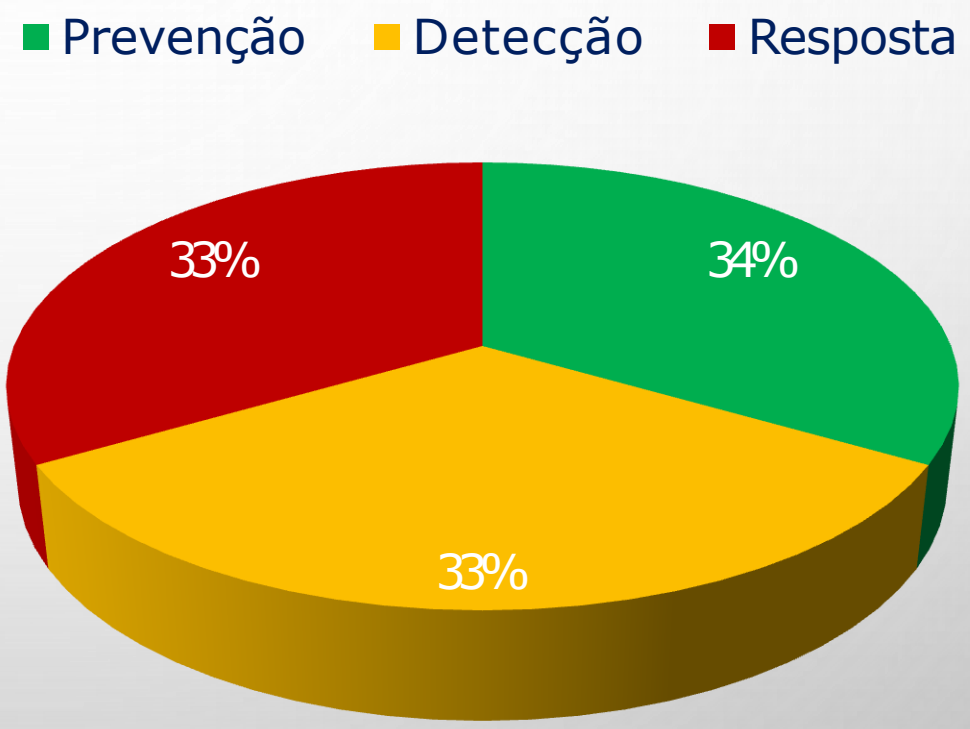
Fonte: http://taosecurity.blogspot.com.br/2006/02/bears-teach-network-security.html

INTELLIGENCE DRIVEN SECURITY

- Etapas da Segurança (Prevenção / Detecção / Resposta).



Hoje



Proposta RSA

- Principais diferencias: Visibilidade, Análise, Ação.

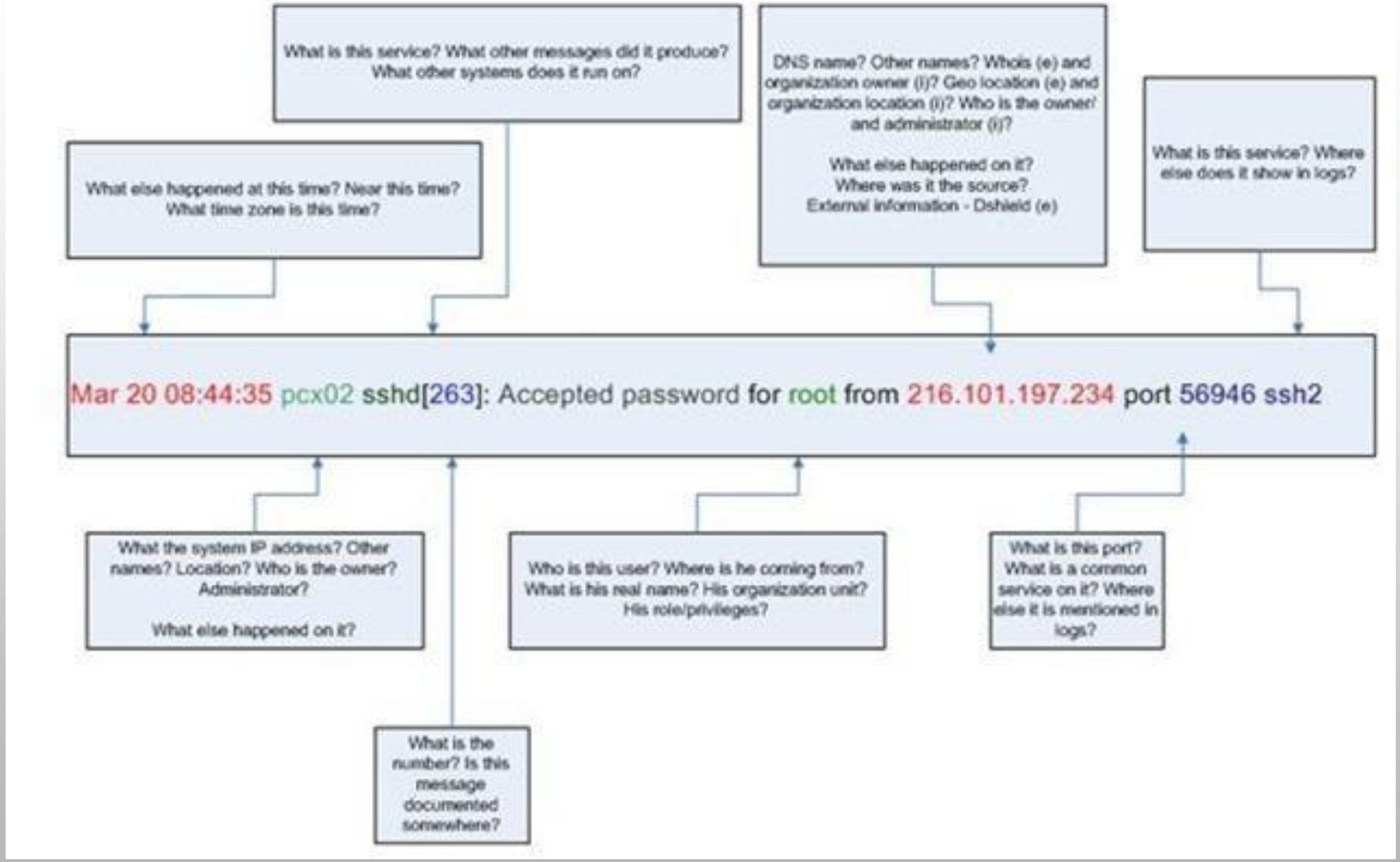
SIEM - DEFINIÇÕES

- **Evento**
  - Qualquer atividade de um sistema passível de registro.
- **Log**
  - É o registro do eventos em algum formato estruturado.
- **Alertas**
  - Visualização de certos eventos com a aplicação de um filtro.
- **Incidentes**
  - Eventos que geram ou tem grande potencial de gerar um dano ou prejuízo.
- **Correlação de eventos**
  - Estabelecer relacionamentos dos registros de eventos de acordo com regras e padrões definidos de forma a gerar informações que sejam relevantes para o seu proprietário.
- **SIEM (Security Information Event Management)**
  - É o sistema que faz a correlação de eventos relacionados a segurança da informação (eventos relativos à confidencialidade, integridade e disponibilidade das informações e ambientes de processamento de dados.)

SIEM – EXEMPLOS DE EVENTOS DE TI

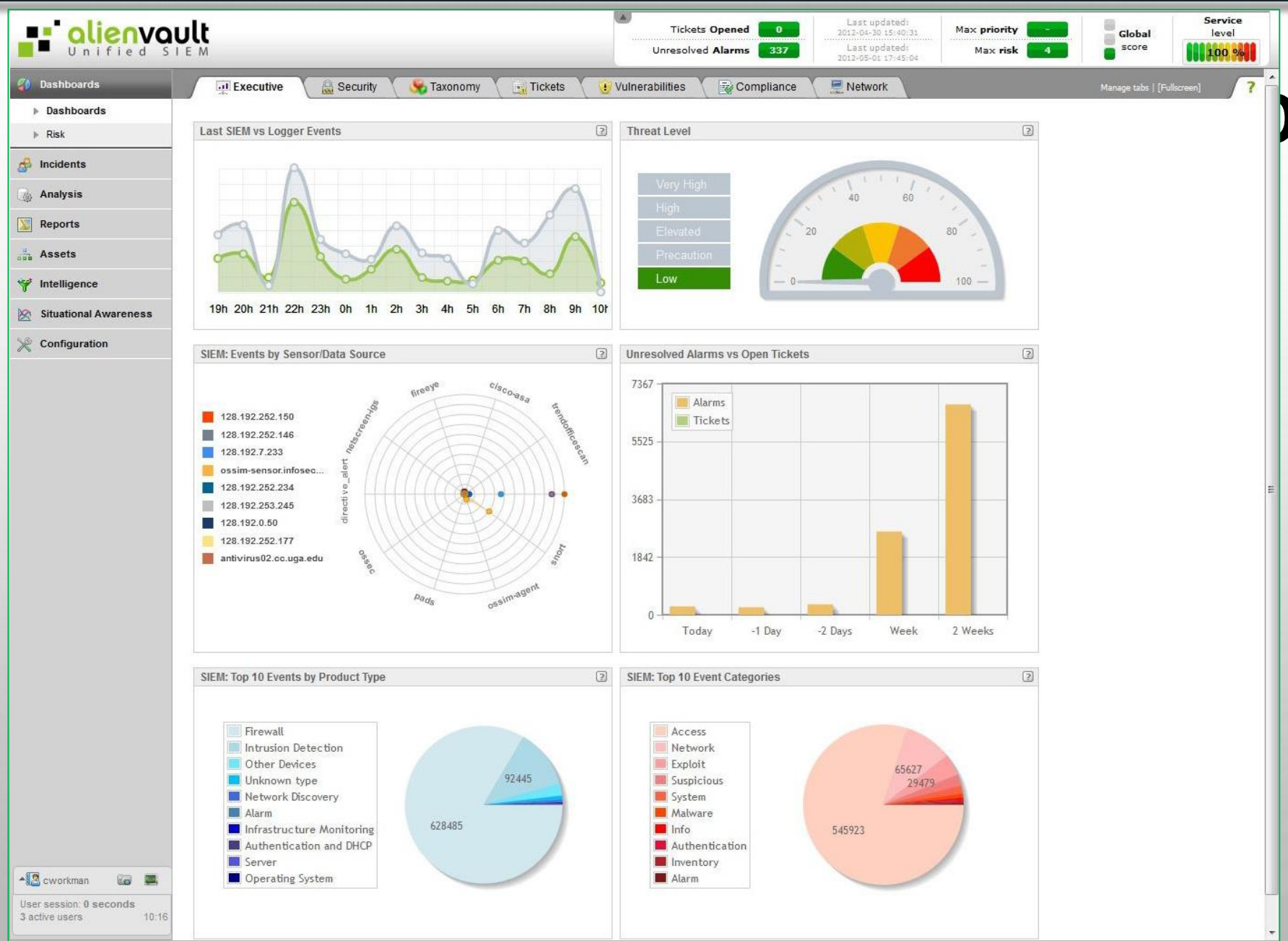
- Sistemas operacionais registram as atividades de suas aplicações e eventos de segurança.
- Servidores de autenticação registram os acessos feitos a pastas, arquivos e aos computadores e dispositivos da rede.
- Bancos de dados armazenam os registros de modificações nos dados, como inserções, deleções, alterações e consultas.
- Aplicações registram transações, erros, alertas e falhas.
- Sistemas de firewall e proxy registram o tráfego de internet e de rede.
- Roteadores e demais dispositivos de rede registram o tráfego entre os segmentos internos de rede.

SIEM – EXEMPLO DE LOG: AUTENTICAÇÃO SSH



SIEM – EXEMPLOS DE CORRELAÇÃO DE EVENTOS

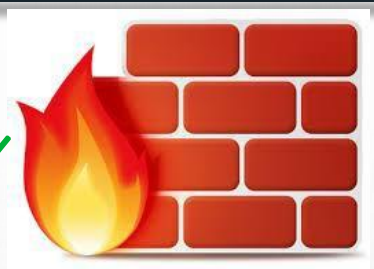
- Dezenas de falhas de autenticação de um usuário em um sistema exposto à Internet.
- Acessos a determinadas pastas e arquivos em horários fora do expediente de trabalho através de acessos remotos.
- Requisições feitas a partir de computador da rede interna para links com reputação maliciosa na Internet.
  - Ex: http://www.phishtank.com
- Comandos SQL submetidos para uma aplicação através de interface web.
- Tráfego de rede em portas de serviço TCP ou UDP anômalas e não registradas para serviços conhecidos.


alienvault Unified SIEM
Tickets Opened 0
Unresolved Alarms 337
Last updated: 2012-04-30 15:40:31
Last updated: 2012-05-01 17:45:04
Max priority -
Max risk 4
Global score
Service level 100 %
Dashboards
Dashboards
Risk
Incidents
Analysis
Reports
Assets
Intelligence
Situational Awareness
Configuration
Executive
Security
Taxonomy
Tickets
Vulnerabilities
Compliance
Network
Manage tabs | [Fullscreen]
Last SIEM vs Logger Events
19h 20h 21h 22h 23h 0h 1h 2h 3h 4h 5h 6h 7h 8h 9h 10h
Threat Level
Very High
High
Elevated
Precaution
Low
0 20 40 60 80 100
SIEM: Events by Sensor/Data Source
128.192.252.150
128.192.252.146
128.192.7.233
ossim-sensor.infosec...
128.192.252.234
128.192.253.245
128.192.0.50
128.192.252.177
antivirus02.cc.uga.edu
fireeye
cisco-asa
trendofficescan
snort
ossim-agent
pads
ossec
directive_alert
netscreen-igs
Unresolved Alarms vs Open Tickets
7367
5525
3683
1842
0
Alarms
Tickets
Today
-1 Day
-2 Days
Week
2 Weeks
SIEM: Top 10 Events by Product Type
Firewall
Intrusion Detection
Other Devices
Unknown type
Network Discovery
Alarm
Infrastructure Monitoring
Authentication and DHCP
Server
Operating System
92445
628485
SIEM: Top 10 Event Categories
Access
Network
Exploit
Suspicious
System
Malware
Info
Authentication
Inventory
Alarm
65627
29479
545923
cworkman
User session: 0 seconds
3 active users
10:16

SIEM - ARQUITETURA

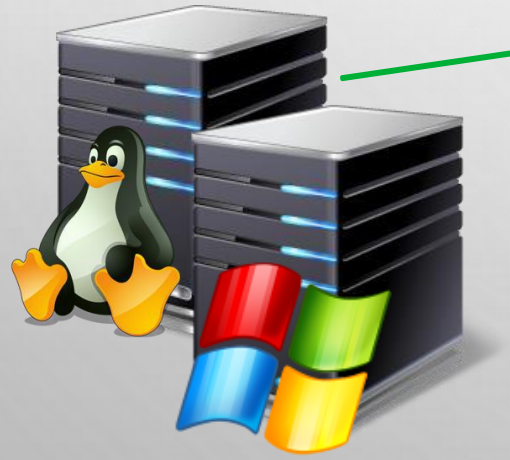
Antivírus

Aplicações



Firewall / Proxy de Internet

SIEM



Servidores

Bases de Dados

Mainframe

SIEM – Casos de uso

- **UMA FERRAMENTA SIEM PODE SER** para diversas áreas e demandas das empresas, como:
  - INVESTIGAÇÃO DE FRAUDES.
  - SUPORTE ÀS OPERAÇÕES DE TI.
  - CONFORMIDADE COM AS NORMATIVAS DE SEGURANÇA E PADRÕES EXTERNOS COMO SOX E PCI-DSS.
  - IDENTIFICAÇÃO DE VULNERABILIDADES E AMEAÇAS AOS SISTEMAS.
  - RESPOSTA A INCIDENTES DE SEGURANÇA.

SIEM – BENEFÍCIOS PARA A RESPOSTA A INCIDENTES

- O monitoramento em tempo real dos eventos de segurança, coletando e agregando os dados.
- Uma análise histórica dos eventos de segurança, para análises de padrões e comportamentos, extraídos a partir de certos parâmetros de pesquisa.
- O estabelecimento regras para alertar a equipe de monitoração caso ocorram certos eventos ou conjunto de eventos no ambiente de TI que sejam relevantes conforme as diretrizes da área de segurança.

- Ferramentas SIEM não fazem mágica!
- Elas apenas mostram ao usuário o que é pedido. Se não houver uma coleta eficiente dos logs e não forem feitas as "perguntas" certas, o que teremos será apenas TB de registros de atividades dos sistemas!
- Uma abordagem que vem dando certo é a criação de uma área de inteligência de regras e a automatização de ações de acordo com a detecção de certos padrões.
- O essencial é ver quais tipos de registros temos na infraestrutura de TI e estudar como podemos utilizá-los de acordo com as estratégias de segurança e gestão de riscos da empresa.

- As ferramentas de SIEM possuem diversas funcionalidades que podem colaborar e aumentar significativamente os processos e atividades de segurança, agilizando as atividades de detecção e resposta a incidentes de segurança.
- Entretanto, seu valor é alto e seu uso adequado depende fortemente das pessoas e processos das empresas, além de uma grande estruturação das áreas de TI, Segurança e Resposta a Incidentes, podendo ter seu desempenho seriamente afetado por ineficiências e obstáculos existentes nestas áreas.