



# Module 26: Avaliando alertas



CyberOps Associate v1.0

Prof. Clemilson Oliveira

[clemilson.oliveira@edu.sc.senai.br](mailto:clemilson.oliveira@edu.sc.senai.br)



# Module Objectives

**Module Title:** Avaliando alertas

**Module Objective:** Explique o processo de avaliação de alertas

Topic Title	Topic Objective
Source of Alerts	Identifique a estrutura dos alertas.
Overview of Alert Evaluation	Explique como os alertas são confidenciais.

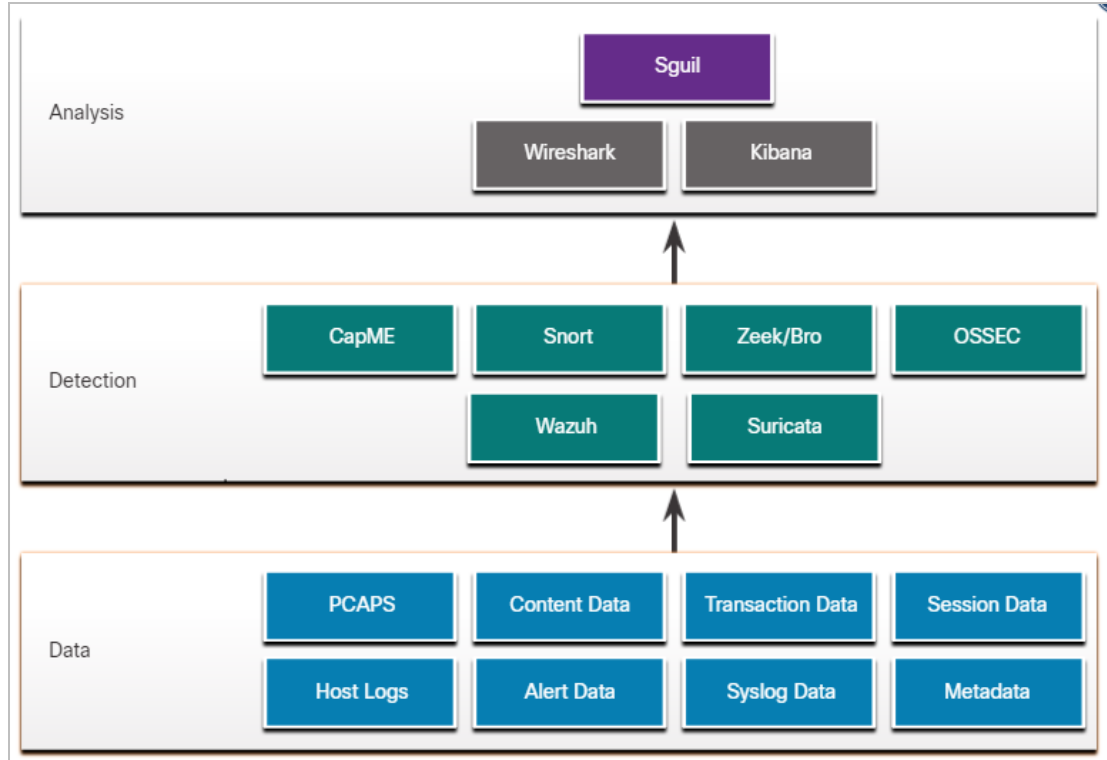
# 26.1 Sources of Alerts

# Security Onion

- Security Onion é um conjunto de ferramentas nSM (Network Security Monitoring, monitoramento de segurança de rede) de código aberto que são executadas em uma distribuição Ubuntu Linux.
- As ferramentas Security Onion fornecem três funções principais para o analista de segurança cibernética, como captura completa de pacotes e tipos de dados, sistemas de detecção de intrusão baseados em rede e host e alerta ferramentas de analista.
- Segurança A cebola pode ser instalada como uma instalação autônoma ou como uma plataforma de sensor e servidor.
- Alguns componentes da Security Onion são de propriedade e mantidos por corporações, como Cisco e Riverbend Technologies, mas são disponibilizados como código aberto.

# Detection Tools for Collecting Alert Data

- A Cebola de Segurança contém muitos componentes. Trata-se de um ambiente integrado que foi projetado para simplificar a implantação de uma solução NSM abrangente.
- A figura ilustra a forma como os componentes da Cebola de Segurança trabalham juntos.
- 



## A Security Onion Architecture

# Detection Tools for Collecting Alert Data (Contd.)

A tabela a seguir lista as ferramentas de detecção da Cebola de Segurança:

Components	Description
CapME	Este é um aplicativo web que permite a visualização de transcrições pcap renderizadas com as ferramentas tcpflow ou Zeek.
Snort	Este é um Sistema de Detecção de Intrusão de Rede (NIDS). É uma importante fonte de dados de alerta que é indexada na ferramenta de análise Sguil.
Zeek	Anteriormente conhecido como Mano. Este é um NIDS que usa mais de uma abordagem baseada em comportamento para detecção de intrusões.
OSSEC	Este é um sistema de detecção de intrusão baseado em host (HIDS) que é integrado à Cebola de Segurança.
Wazuh	É uma solução completa que fornece um amplo espectro de mecanismos de proteção de ponto final, incluindo análise de arquivo de registro de host, monitoramento de integridade de arquivos, detecção de vulnerabilidades, avaliação de configuração e resposta a incidentes.
Suricata	Este é um NIDS que usa uma abordagem baseada em assinatura. Também pode ser usado para prevenção de intrusões inline.

## Evaluating Alerts

# Analysis Tools

O Security Onion integra esses vários tipos de registros do Sistema de Detecção de Dados e Intrusões (IDS) em uma única plataforma através das seguintes ferramentas:

Este fornece um console de alto nível para investigar alertas de segurança de uma grande variedade de fontes. Sguil serve como ponto de partida na investigação de alertas de segurança. Muitas fontes de dados estão disponíveis pivotando diretamente do Sguil para outras ferramentas.

**Kibana:** É uma interface interativa de painel para dados da Elasticsearch. Permite a consulta de dados NSM e fornece visualizações flexíveis desses dados. É possível pivotar de Sguil diretamente para Kibana para ver displays contextualizados.

**Wireshark:** É um aplicativo de captura de pacotes que é integrado ao traje de cebola de segurança. Ele pode ser aberto diretamente de outras ferramentas e exibir capturas completas de pacotes relevantes para uma análise.

**Zeek:** Este é um analisador de tráfego de rede que serve como um monitor de segurança. Fiscaliza todo o tráfego em um segmento de rede e permite uma análise aprofundada desses dados. Pivotar de Sguil no Zeek fornece acesso a logs de transações muito precisos, conteúdo de arquivo e saída personalizada.

# Alert Generation

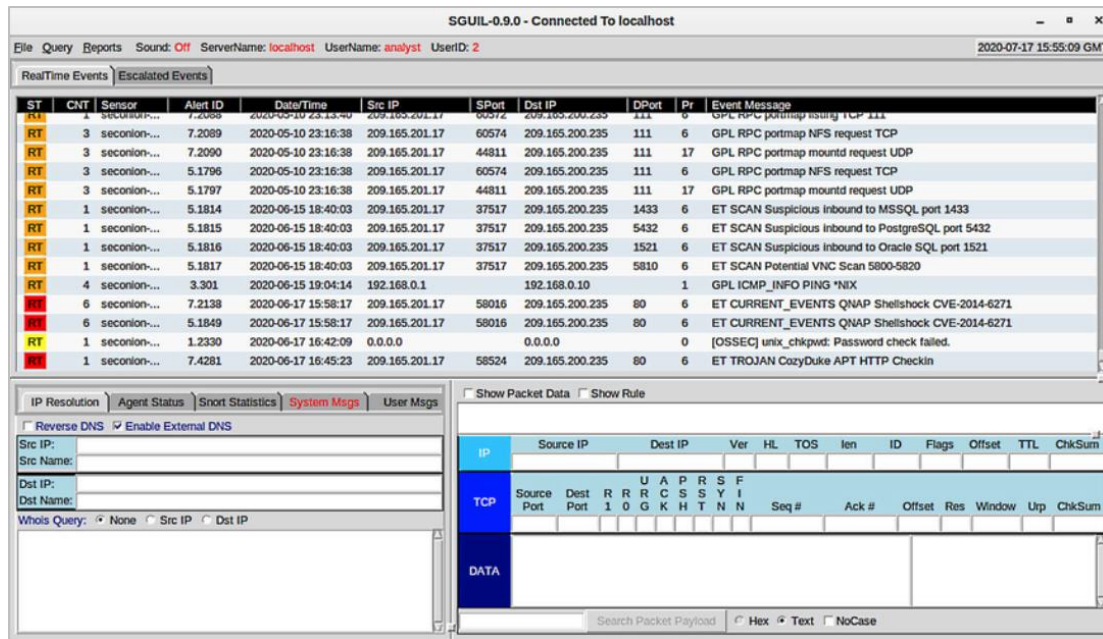
- Alertas de segurança são mensagens de notificação geradas por ferramentas, sistemas e dispositivos de segurança NSM. Os alertas podem vir de muitas formas dependendo da fonte.
- Em Security Onion, o Sguil fornece um console que integra alertas de várias fontes em uma fila cronometrada.
- Um analista de segurança cibernética trabalha através da fila de segurança investigando, classificando, aumentando ou aposentando alertas.
- Os alertas geralmente incluem informações de cinco tuplas, bem como timestamps e informações que identificam qual dispositivo ou sistema gerou o alerta.
- **SrcIP** - o endereço IP de origem para o evento.
  - **SPort** - a porta de origem (local) Camada 4 para o evento.
  - **DstIP** - o IP de destino para o evento.
  - **DPort** - o destino Porta camada 4 para o evento.
  - **Pr** - o número do protocolo IP para o evento.



# Alert Generation (Contd.)

A figura mostra a janela do aplicativo Sguil com a fila de alertas que estão esperando para serem investigados na parte superior da interface. Os campos disponíveis para os eventos em tempo real são os seguintes:

- **ST** - Este é o status do evento. O evento é codificado por cores por prioridade com base na categoria do alerta. Há quatro níveis de prioridade: muito baixo, baixo, médio e alto e as cores variam de amarelo claro a vermelho à medida que a prioridade aumenta.
- **CNT** - Esta é a contagem para o número de vezes que este evento foi detectado para o mesmo endereço IP de origem e destino. O sistema determinou que este conjunto de eventos está correlacionado.
- **Sensor** - Este é o agente relatando o evento. Os sensores disponíveis e seus números de identificação podem ser encontrados na guia Status do agente do painel que aparece abaixo da janela de eventos à esquerda.



Sguil Window

# Evaluating Alerts

## Alert Generation (Contd.)

- **Alert ID** - Este número de duas partes representa o sensor que relatou o problema e o número de evento para esse sensor.
- **Date/Time** - Este é o horário do evento. No caso de eventos correlacionados, é o timestamp para o primeiro evento.
- **Event Message** - Este é o texto de identificação para o evento. sua está configurada na regra que acionou o alerta. A regra associada pode ser visualizada no painel direito, logo acima dos dados do pacote. Para exibir a regra, a caixa de seleção Mostrar regra deve ser selecionada.

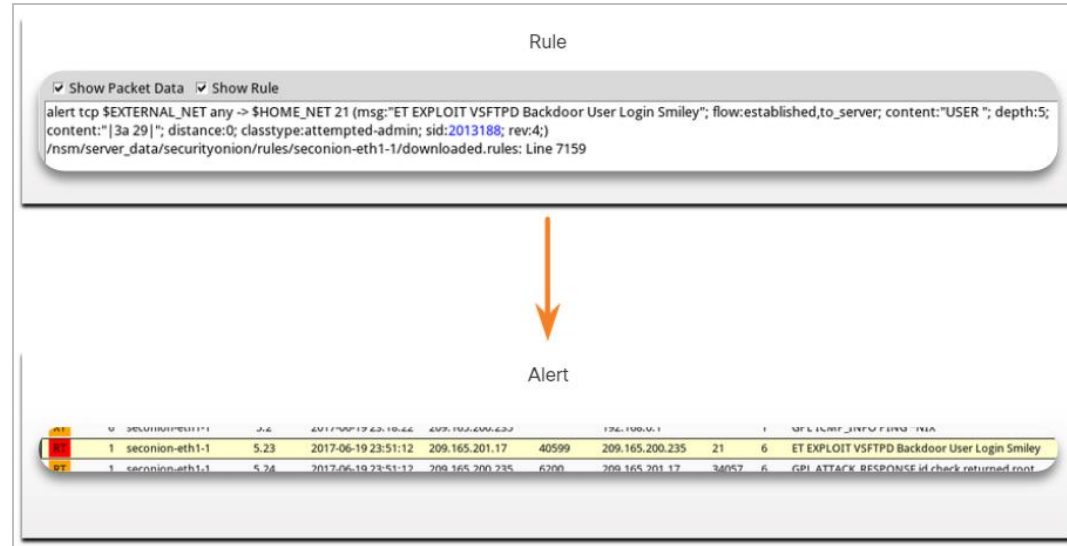
The screenshot displays the Sguil-0.9.0 interface, titled "Sguil-0.9.0 - Connected To localhost". The top menu bar includes "File", "Query", "Reports", "Sound: Off", "ServerName: localhost", "UserName: analyst", "UserID: 2", and a timestamp "2020-07-17 15:55:09 GMT". Below the menu, there are tabs for "RealTime Events" and "Escalated Events". The main table lists alerts with columns: ST, CNT, Sensor, Alert ID, Date/Time, Src IP, SPort, Dst IP, DPort, Pr, and Event Message. The table contains 15 rows of alert data, including events like "GPL RPC portmap using TCP 111", "GPL RPC portmap mountd request UDP", "ET SCAN Suspicious Inbound to PostgreSQL port 5432", and "ET SCAN Suspicious Inbound to Oracle SQL port 1521". Below the table, there are sections for "IP Resolution", "Agent Status", "Short Statistics", "System Msgs", and "User Msgs". The "System Msgs" section is active, showing "Reverse DNS" and "Enable External DNS" options. To the right, there is a "Show Packet Data" section with a "Show Rule" checkbox. Below this, a packet details table is visible, showing "Source IP", "Dest IP", "Ver", "HL", "TOS", "len", "ID", "Flags", "Offset", "TTL", and "ChkSum". The "TCP" section shows "Source Port", "Dest Port", "Seq #", "Ack #", "Offset", "Res", "Window", "Up", and "ChkSum". The "DATA" section is also present. At the bottom, there is a "Search Packet Payload" field and checkboxes for "Hex", "Text", and "NoCase".

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	3	seconion...	7.2089	2020-05-10 23:16:38	209.165.201.17	60574	209.165.200.235	111	6	GPL RPC portmap using TCP 111
RT	3	seconion...	7.2090	2020-05-10 23:16:38	209.165.201.17	44811	209.165.200.235	111	17	GPL RPC portmap mountd request UDP
RT	3	seconion...	5.1796	2020-05-10 23:16:38	209.165.201.17	60574	209.165.200.235	111	6	GPL RPC portmap NFS request TCP
RT	3	seconion...	5.1797	2020-05-10 23:16:38	209.165.201.17	44811	209.165.200.235	111	17	GPL RPC portmap mountd request UDP
RT	1	seconion...	5.1814	2020-06-15 18:40:03	209.165.201.17	37517	209.165.200.235	1433	6	ET SCAN Suspicious Inbound to MSSQL port 1433
RT	1	seconion...	5.1815	2020-06-15 18:40:03	209.165.201.17	37517	209.165.200.235	5432	6	ET SCAN Suspicious Inbound to PostgreSQL port 5432
RT	1	seconion...	5.1816	2020-06-15 18:40:03	209.165.201.17	37517	209.165.200.235	1521	6	ET SCAN Suspicious Inbound to Oracle SQL port 1521
RT	1	seconion...	5.1817	2020-06-15 18:40:03	209.165.201.17	37517	209.165.200.235	5810	6	ET SCAN Potential VNC Scan 5800-5820
RT	4	seconion...	3.301	2020-06-15 19:04:14	192.168.0.1		192.168.0.10		1	GPL ICMP_INFO PING *NIX
RT	6	seconion...	7.2138	2020-06-17 15:58:17	209.165.201.17	58016	209.165.200.235	80	6	ET CURRENT_EVENTS QNAP Shellshock CVE-2014-6271
RT	6	seconion...	5.1849	2020-06-17 15:58:17	209.165.201.17	58016	209.165.200.235	80	6	ET CURRENT_EVENTS QNAP Shellshock CVE-2014-6271
RT	1	seconion...	1.2330	2020-06-17 16:42:09	0.0.0.0		0.0.0.0		0	[OSSEC] unix_chkpwd: Password check failed.
RT	1	seconion...	7.4281	2020-06-17 16:45:23	209.165.201.17	58524	209.165.200.235	80	6	ET TROJAN CozyDuke APT HTTP Checkin

Sguil Window

# Rules and Alerts

- Alertas podem vir de várias fontes:
  - NIDS** - Snort, Zeek, and Suricata
  - HIDS** - OSSEC, Wazuh
  - Gestão e monitoramento de ativos** - Sistema de Detecção passiva de Ativos (PADS)
  - HTTP, DNS, and TCP transactions** - Gravado por Zeek e pcaps
  - Syslog messages** - Múltiplas fontes



- As informações encontradas nos alertas exibidos no Sguil diferem no formato de mensagem porque vêm de diferentes fontes.
- O alerta Sguil na figura foi acionado por uma regra que foi configurada em Snort.

# Snort Rule Structure

As regras do snort consistem em duas seções, como mostrado na figura: o cabeçalho de regra e as opções de regra. O Local de Regra às vezes é adicionado por Sguil.

```
alert ip any any -> any any (msg:"GPL ATTACK_RESPONSE id check returned root";  
content:"uid=0|28|root|29|"; fast_pattern:only; classtype:bad-unknown; sid:2100498;  
rev:8;)  
/nsm/server_data/securityonion/rules/seconion-eth1-1/downloaded.rules:Line 692
```

Component	Example (shortened...)	Explanation
rule header	alert ip any any -> any any	Contém a ação a ser tomada, endereços de origem e destino e porto, e a direção do fluxo de tráfego
rule options	(msg:"GPL ATTACK_RESPONSE ID CHECK RETURNED ROOT";...)	Inclui a mensagem a ser exibida, detalhes do conteúdo do pacote, tipo de alerta, ID de origem e detalhes adicionais, como uma referência à regra ou vulnerabilidade
rule location	/nsm/server_data/securityonio n/rules/...	Adicionado por Sguil para indicar a localização da regra na estrutura do arquivo Security Onion e no arquivo de regra especificado

# Snort Rule Structure (Contd.)

## O cabeçalho de regra

O cabeçalho de regra contém as informações de ação, protocolo, endereçamento e porta, conforme mostrado na figura. A estrutura da porção do cabeçalho é consistente entre a regra de alerta Snort. O Snort pode ser configurado para usar variáveis para representar endereços IP internos e externos.

```
alert ip any any -> any any (msg:"GPL ATTACK_RESPONSE id check returned root";  
content:"uid=0|28|root|29|"; fast_pattern:only; classtype:bad-unknown; sid:2100498;  
rev:8;)  
/nsm/server_data/securityonion/rules/seconion-eth1-1/downloaded.rules:Line 692
```

Component	Explanation
alert	a ação a ser tomada é emitir um alerta, outras ações são log e passar
ip	o protocolo
any any	a fonte especificada é qualquer endereço IP e qualquer porta da Camada 4
->	a direção do fluxo é da fonte para o destino
any any	o destino especificado é qualquer endereço IP e qualquer porta da Camada 4

# Snort Rule Structure (Contd.)

## As Opções de Regras

A estrutura da seção de opções da regra é variável. É a parte da regra que está fechada entre parênteses, como mostra a figura. Ele contém a mensagem de texto que identifica o alerta. Ele também contém metadados sobre o alerta, como uma URL.

As mensagens de regra snort podem incluir a fonte da regra. Três fontes comuns para as regras de Snort são:

- **GPL** - Regras mais antigas do Snort que foram criadas pelo Sourcefire e distribuídas sob um GPLv2. O ruleset gpl não é certificado pela Cisco Talos. O ruleset GPL é pode ser baixado no site do Snort, e está incluído no Security Onion.
- **ET** - Regras de snort de Ameaças Emergentes que é um ponto de coleta para regras Snort de múltiplas fontes. O ruleset ET contém regras de várias categorias. Um conjunto de regras de ET está incluído com a Security Onion. Ameaças Emergentes é uma divisão da Proofpoint, Inc.
- **VRT** - Essas regras estão imediatamente disponíveis para assinantes e são liberadas para usuários cadastrados 30 dias após sua criação, com algumas limitações. Eles agora são criados e mantidos pela Cisco Talos.

# Snort Rule Structure (Contd.)

```
alert ip any any -> any any (msg:"GPL ATTACK_RESPONSE id check returned root";  
content:"uid=0|28|root|29|"; fast_pattern:only; classtype:bad-unknown; sid:2100498;  
rev:8;)  
/nsm/server_data/securityonion/rules/seconion-eth1-1/downloaded.rules:Line 692
```

Component	Explanation
msg:	Texto que descreve o alerta.
content:	Refere-se ao conteúdo do pacote. Neste caso, um alerta será enviado se o texto literal "uid=0(raiz)" aparecer em qualquer lugar nos dados do pacote. Valores especificando a localização do texto podem ser fornecidos.
reference:	Isso não é mostrado na figura. Muitas vezes é um link para uma URL que fornece mais informações sobre a regra. Neste caso, o sid é hiperligado à fonte da regra na internet.
classtype:	Uma categoria para o ataque. Snort inclui um conjunto de categorias padrão que têm um dos quatro valores prioritários.
sid:	Um identificador numérico único para a regra.
rev:	A revisão da regra que é representada pelo sid.

# Lab - Snort and Firewall Rules

Neste laboratório, você completará os seguintes objetivos:

Realize o monitoramento ao vivo do IDS e eventos.

Configure sua própria regra de firewall personalizada para impedir que os hosts internos entrem em contato com um servidor de hospedagem de malware.

Crie um pacote malicioso e lance-o contra um alvo interno.

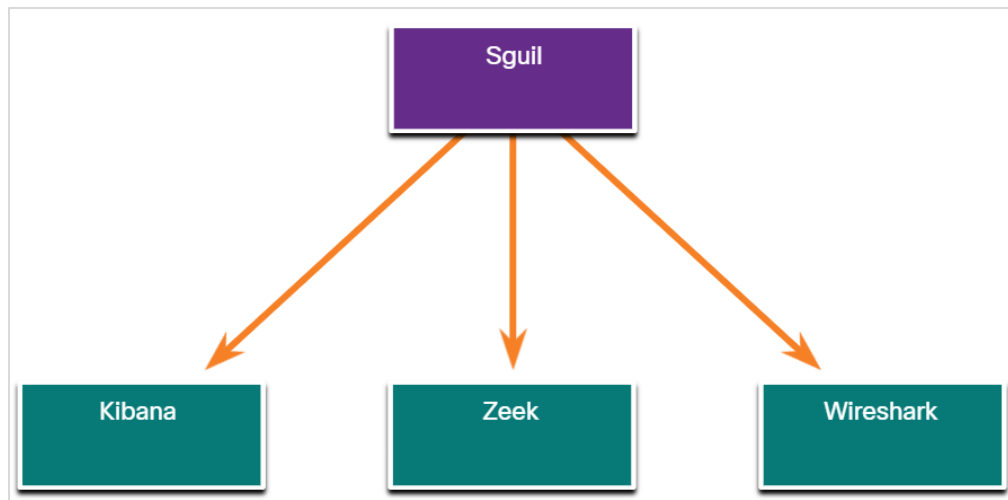
Crie uma regra IDS personalizada para detectar o ataque personalizado e emitir um alerta com base nele.



# 26.2 Overview of Alert Evaluation


# The Need for Alert Evaluation

- O cenário de ameaças está em constante mudança à medida que novas vulnerabilidades e ameaças são descobertas. À medida que as necessidades do usuário e da organização mudam, a superfície de ataque também muda.
- Atores de ameaças aprenderam como variar rapidamente características de suas façanhas, a fim de escapar da detecção.
- É melhor ter alertas que às vezes são gerados pelo tráfego inocente, do que ter regras que perdem o tráfego malicioso.
- É necessário que analistas especializados em segurança cibernética investiguem alertas para determinar se uma exploração realmente ocorreu.
- Os analistas de cibersegurança de nível 1 trabalharão através de filas de alertas em uma ferramenta como o Sguil, pivotando em ferramentas como Zeek, Wireshark e Kibana para verificar se um alerta representa uma exploração real.



**Principais ferramentas para o analista de cibersegurança nível 1**

# Evaluating Alerts

- Incidentes de segurança são classificados usando um esquema emprestado de diagnósticos médicos. Esse esquema de classificação é utilizado para orientar ações e avaliar procedimentos diagnósticos. A preocupação é que qualquer diagnóstico pode ser preciso, ou verdadeiro, ou impreciso, ou falso.
- Na análise de segurança da rede, o analista de segurança cibernética é apresentado com um alerta. O analista de cibersegurança precisa determinar se esse diagnóstico é verdadeiro.
- Os alertas podem ser classificados da seguinte forma:
  - **True Positive:** O alerta foi verificado como um incidente de segurança real.
  - **False Positive:** O alerta não indica um incidente de segurança real. Atividade benigna que resulta em um falso positivo é às vezes referido como um gatilho benigno.
- Uma situação alternativa é que um alerta não foi gerado. A ausência de um alerta pode ser classificada como:
  -  **True Negative:** Nenhum incidente de segurança ocorreu. A atividade é benigna.
  - **False Negative:** Um incidente não detectado ocorreu.

# Evaluating Alerts (Contd.)

Quando um alerta é emitido, ele receberá uma das quatro classificações possíveis:

	True	False
Positive (Alert exists)	Incident occurred	No incident occurred
Negative (No alert exists)	No incident occurred	Incident occurred

- **True positives** são o tipo de alerta desejado. Eles significam que as regras que geram alertas têm funcionado corretamente.
- **False positives** não são desejáveis. Embora não indiquem que uma exploração não detectada ocorreu, elas são caras porque os analistas de segurança cibernética devem investigar falsos alarmes.
- **True negatives** são desejáveis. Eles indicam que o tráfego normal benigno é corretamente ignorado, e alertas errôneos não estão sendo emitidos.
- **False negatives** são perigosos. Eles indicam que as explorações não estão sendo detectadas pelos sistemas de segurança que estão no local.

**Note:** “Eventos verdadeiros são desejáveis. Eventos “falsos” são indesejáveis e potencialmente perigosos.

# Evaluating Alerts (Contd.)

- Eventos benignos são aqueles que não devem disparar alertas. Eventos benignos em excesso indicam que algumas regras ou outros detectores precisam ser melhorados ou eliminados.
- Quando se suspeitam de verdadeiros pontos positivos, um analista de segurança cibernética é obrigado a aumentar o alerta para um nível mais alto para investigação. O investigador seguirá em frente com a investigação para confirmar o incidente e identificar qualquer dano potencial que possa ter sido causado.
- Um analista de segurança cibernética também pode ser responsável por informar o pessoal de segurança que falsos positivos estão ocorrendo na medida em que o tempo do analista de segurança cibernética é seriamente impactado.
- Falsos negativos podem ser descobertos bem depois de uma exploração ter ocorrido. Isso pode acontecer por meio da análise retrospectiva de segurança (RSA). O RSA pode ocorrer quando regras recém-obtidas ou outra inteligência de ameaça é aplicada a dados de segurança de rede arquivados.
- Por essa razão, é importante monitorar a inteligência de ameaças para aprender sobre novas vulnerabilidades e explorações e avaliar a probabilidade de que a rede estava vulnerável a eles em algum momento no passado.

# Deterministic Analysis and Probabilistic Analysis

- A análise determinística avalia o risco com base no que se sabe sobre uma vulnerabilidade. Este tipo de análise de risco só pode descrever o pior caso.
- A análise probabilística estima o potencial sucesso de uma exploração, estimando a probabilidade de que, se um passo em uma exploração tiver sido concluído com sucesso, o próximo passo também será bem-sucedido.
- Em uma análise determinística, todas as informações para realizar uma exploração são consideradas conhecidas.
- Na análise probabilística, supõe-se que os números das portas que serão utilizados só podem ser previstos com algum grau de confiança.
- As duas abordagens são resumidas abaixo.
  - **Deterministic Analysis** - Para que uma exploração seja bem sucedida, todos os passos anteriores na exploração também devem ser bem sucedidos. O analista de cibersegurança conhece os passos para uma exploração bem sucedida.
  - **Probabilistic Analysis** - Técnicas estatísticas são usadas para determinar a probabilidade de que uma exploração bem sucedida ocorra com base na probabilidade de que cada passo na exploração terá sucesso.

# 26.3 Avaliando o resumo dos alertas

# O que aprendi neste módulo?

- Security Onion é um conjunto de ferramentas nSM (Network Security Monitoring, monitoramento de segurança de rede) de código aberto que são executadas em uma distribuição Ubuntu Linux.
- As ferramentas security Onion fornecem três funções principais para o analista de segurança cibernética: captura completa de pacotes e tipos de dados, sistemas de detecção de intrusões baseados em rede e host e alerta ferramentas de analista.
- A Security Onion integra os dados e o IDS faz logon em uma única plataforma através das seguintes ferramentas:
- Sguil - serve como ponto de partida na investigação de alertas de segurança.
- Kibana - É uma interface interativa de painel para dados da Elasticsearch.
- O aplicativo de captura de pacotes Wireshark é integrado ao conjunto Security Onion.
- Zeek é um analisador de tráfego de rede que serve como monitor de segurança.



# O que aprendi neste módulo? (Contd.)

- Snort é um Sistema de Detecção de Intrusões de Rede (NIDS). É uma importante fonte dos dados de alerta que é indexada na ferramenta de análise Sguil.
- Os alertas podem ser classificados como True Positive (O alerta foi verificado como um incidente de segurança real) ou False Positive (O alerta não indica um incidente de segurança real).
- Uma situação alternativa é que um alerta não foi gerado. A ausência de um alerta pode ser classificada como: True Negative (Nenhum incidente de segurança ocorreu. A atividade é benigna.) e Falso Negativo (Ocorreu um incidente não detectado).
- A análise determinística avalia o risco com base no que se sabe sobre uma vulnerabilidade.
- A análise probabilística estima o potencial sucesso de uma exploração, estimando a probabilidade de que, se um passo em uma exploração tiver sido concluído com sucesso, o próximo passo também será bem-sucedido.

