همبستگی هشدارها
(Alert Correlation)

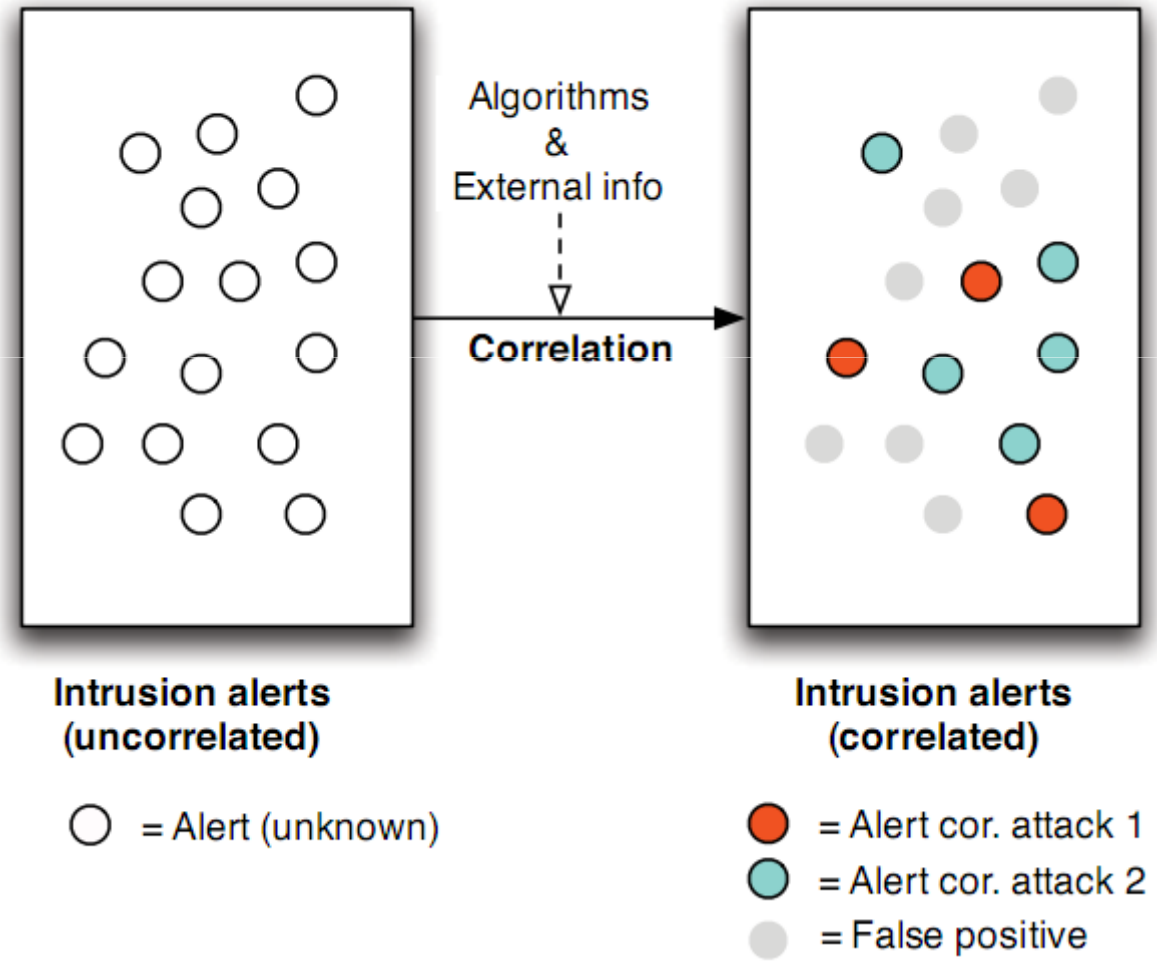
رئوس مطالب

- انگیزه
- چه چیزی را همبسته کنیم؟
  - منابع اطلاعاتی
  - سیگنال ها، رویدادها و هشدارها
  - سیاست های ثبت و هشدار
- چگونه همبستگی صورت می گیرد؟
  - هدف و مدل کلی
  - یکدست کردن هشدارها (Alert Normalization)
  - کاهش هشدارها مانند همجوشی (fusion)
  - همبستگی بین هشدارها

مشکلات IDSهای تنها

- تعداد زیاد false positive
- تعداد زیادی هشدار برای یک نفوذ
  - باعث گمراهی مدیر شبکه می شود.
- عدم وجود دید از بالا
  - نفوذگر در حال چه کاری است؟
  - می توان گام های بعدی نفوذگر را پیشبینی کرد؟
  - آیا حملات تأثیرات مخربی روی سیستم داشته اند؟

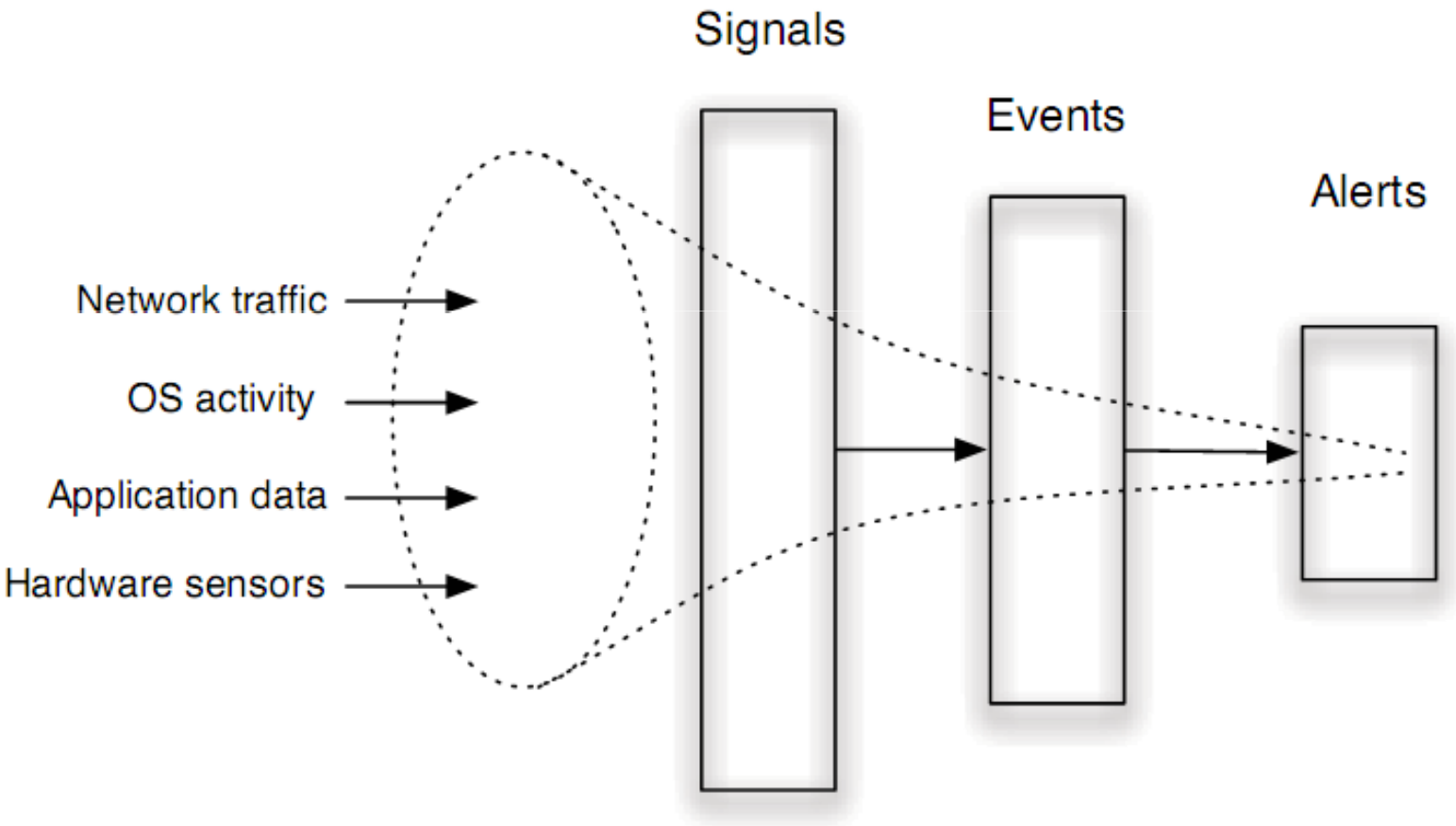
همبستگی


Algorithms
&
External info
Correlation
Intrusion alerts
(uncorrelated)
= Alert (unknown)
Intrusion alerts
(correlated)
= Alert cor. attack 1
= Alert cor. attack 2
= False positive

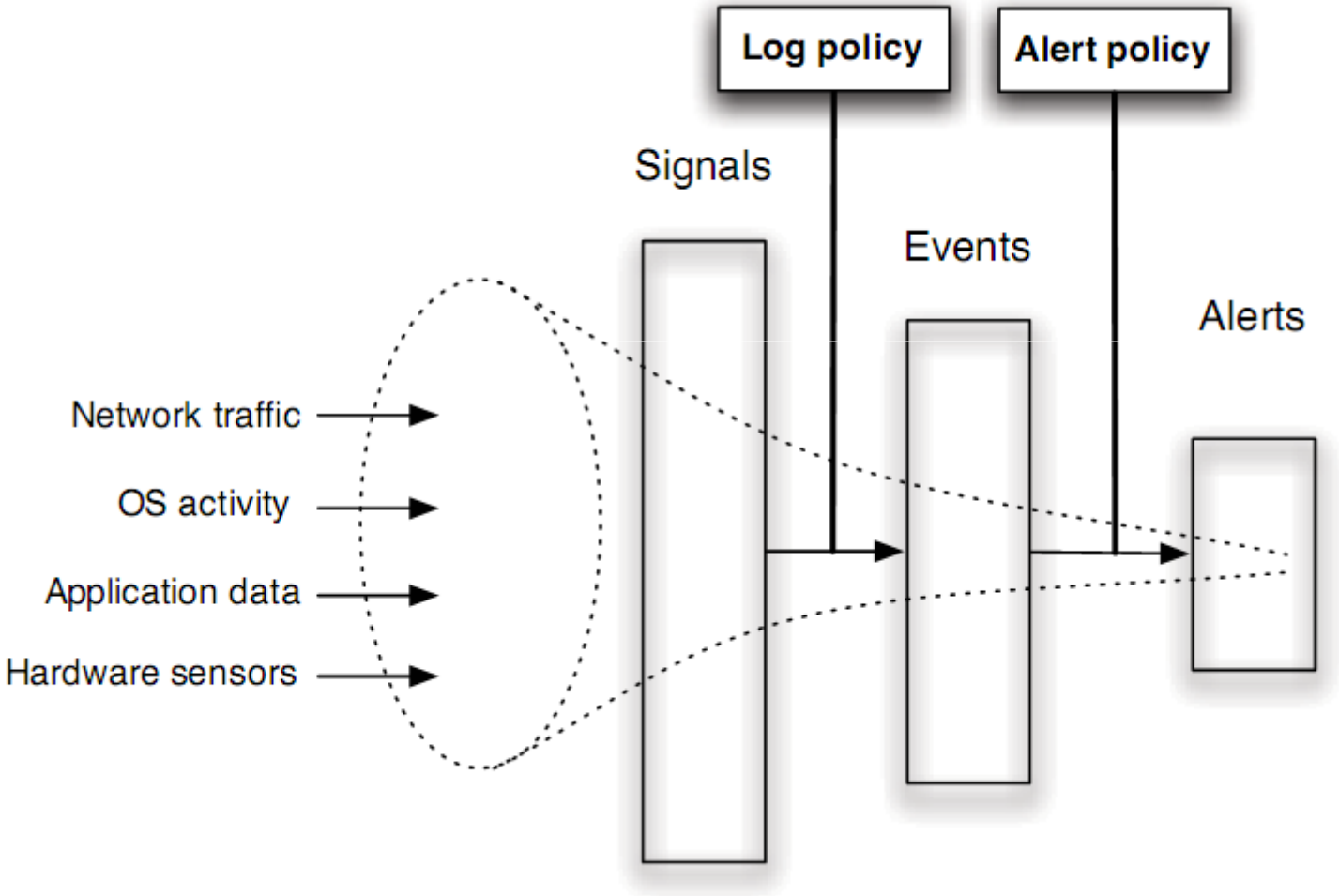
منابع اطلاعاتی

- IDSها (هشدارها)
  - IDSهای مبتنی بر میزبان
  - IDSهای مبتنی بر شبکه
  - IDSهای مبتنی بر کاربرد
- ثبت ها
  - میزبان: syslog
  - شبکه: فایروال ها، روترها و سوئیچ
  - کاربرد: Apache، IIS، Oracle و MySql

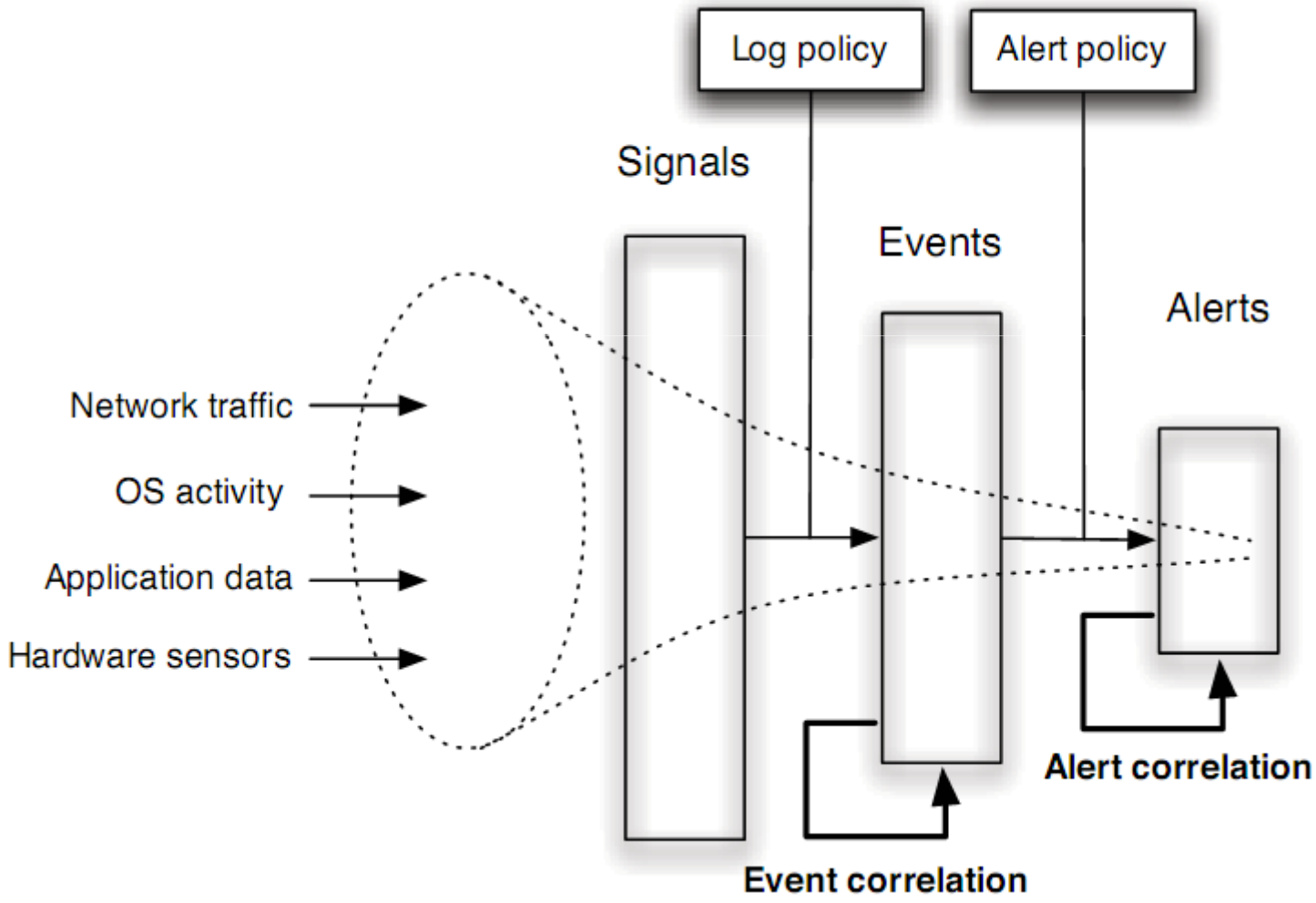
سیگنال ها، رویدادها و هشدارها



سیاست های ثبت و هشدار



همبستگی هشدارها و رویدادها



تعاریف

- همبستگی رویداد
  - تفسیر، ترکیب و تحلیل رویدادهای نامشخص از تمام منابع برای شناسایی و جلوگیری از نفوذ.
- همبستگی هشدار
  - تفسیر، ترکیب و تحلیل هشدارها و اطلاعات بیرونی IDSها برای پالایش هشدارها و بازسازی سناریوهای نفوذ.

جدول همبستگی رویداد

Attack	Log								
	Syslog	Firewall	Netflow	TCP	DNS	Auth	Web	Mail	FTP
Dictionary	×	×	×	×		×	×	×	×
FTP-Write	×			×		×			×
Imap	×	×	×	×				×	
Named	×		×		×				
Phf	×			×			×		
Sendmail	×	×	×	×	×	×		×	
Xsnoop	×		×						
Apache2	×	×	×	×			×		
Back	×			×			×		
Mailbomb	×	×	×	×				×	
SYN Flood	×	×	×	×	×				
Ping of Death		×	×	×					
Process Table		×	×	×				×	
Smurf			×	×					
Udpstorm			×	×	×				

سیاست ثبت

- چه چیزی **باید** (**نباید**) ثبت شود؟
- اطلاعات قابل ثبت (سیگنال ها)
  - فعالیت های مربوط به کاربرد، سیستم عامل، شبکه و سخت افزار
- چه سیگنال هایی به فعالیت های خرابکارانه مربوط **هستند** (**نیستند**)؟
  - شناسایی حملات شناخته شده برای ثبت ها
  - استفاده از Honeypot برای شناخت و یادگیری حملات
  - ثبت همه اطلاعات (کمک به شناسایی حملات جدید)
  - برقراری trade-off بین ثبت همه اطلاعات و هزینه های ثبت

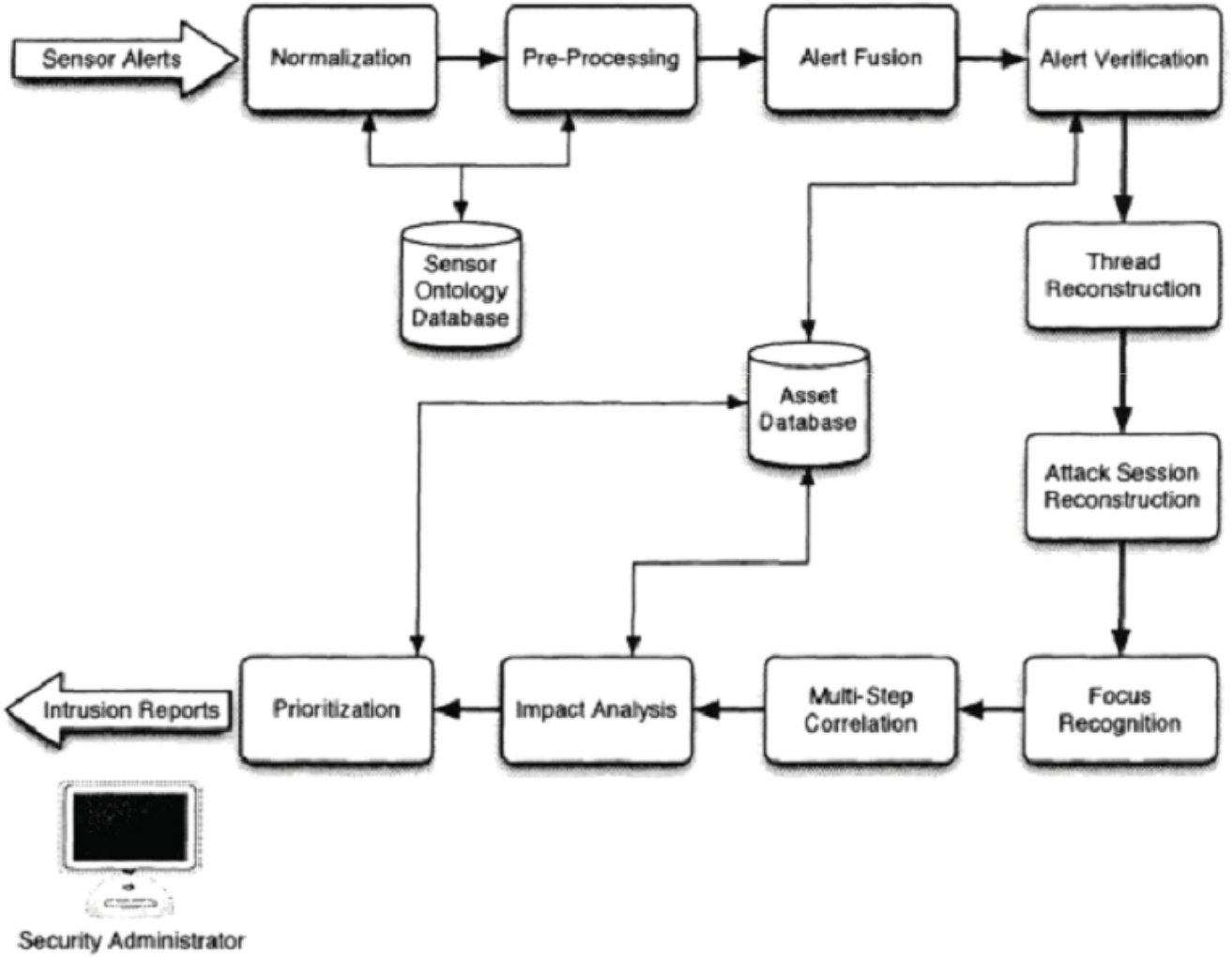
سیاست هشدار

- چه رویداد هایی منجر به هشدار **می شوند** (**نمی شوند**)؟
  - حملات روی فناوری، اطلاعات، audit logsو دارایی های سطح بالا
- چه ترکیباتی از رویدادها مشخص کننده نفوذ است؟
  - بررسی حملات شناخته شده در رویدادها
  - استفاده از Honeypot برای شناخت و یادگیری حملات
  - ایجاد قوانین کارشناسانه برای ثبت ها، رویدادها و هشدارهای امنیتی

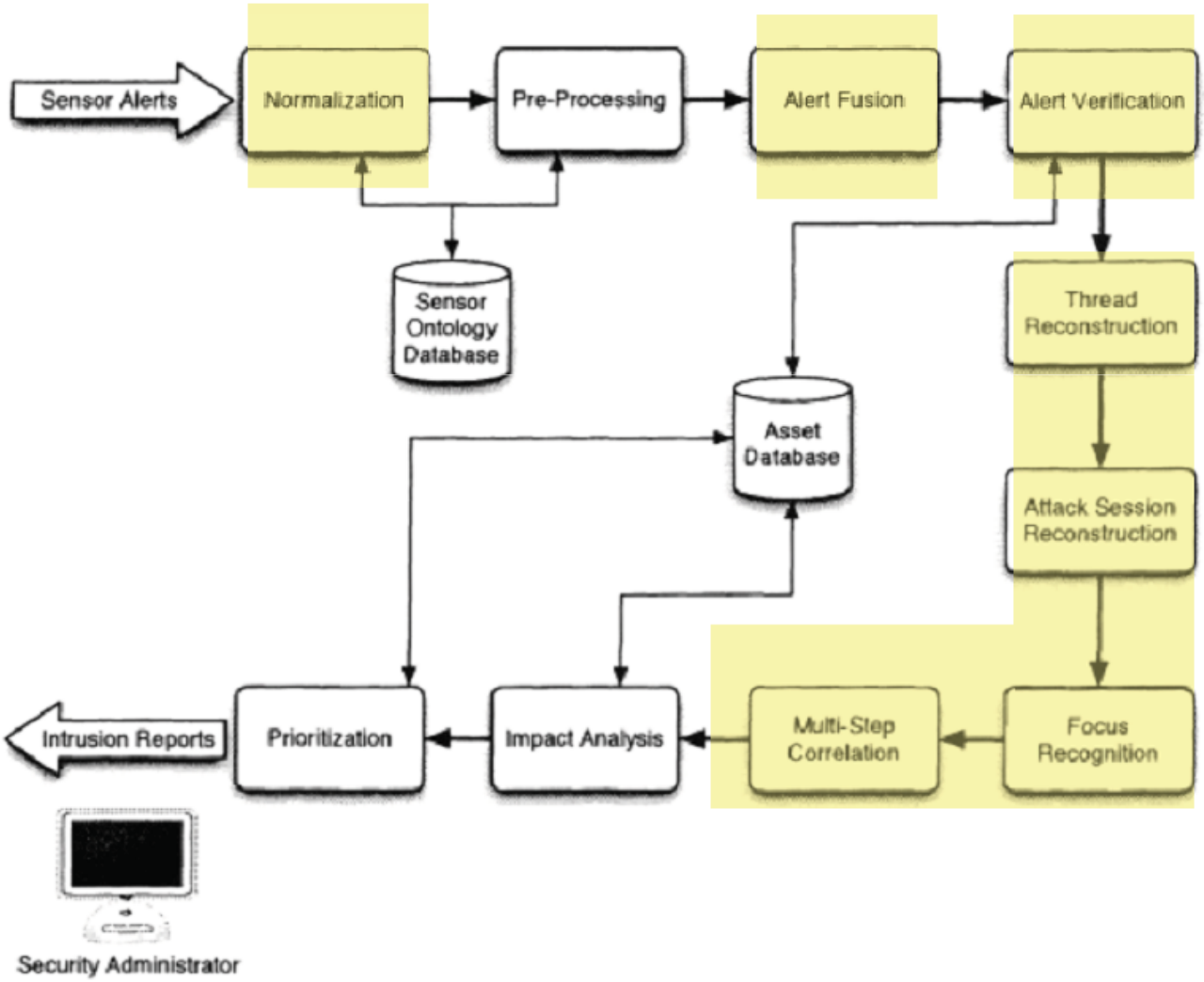
هدف همبستگی هشدار

- کاهش تعداد هشدارها
  - حذف (Elimination)
  - همجوشی (Fusion)
  - تجمع (Aggregation)
  - سنتز (Synthesis)
- بهبود تشخیص حمله
  - نوع فعالیت
  - ارتباط هشدارها
  - درستی سنجی هشدارها (Verification)

عملیات همبستگی هشدار

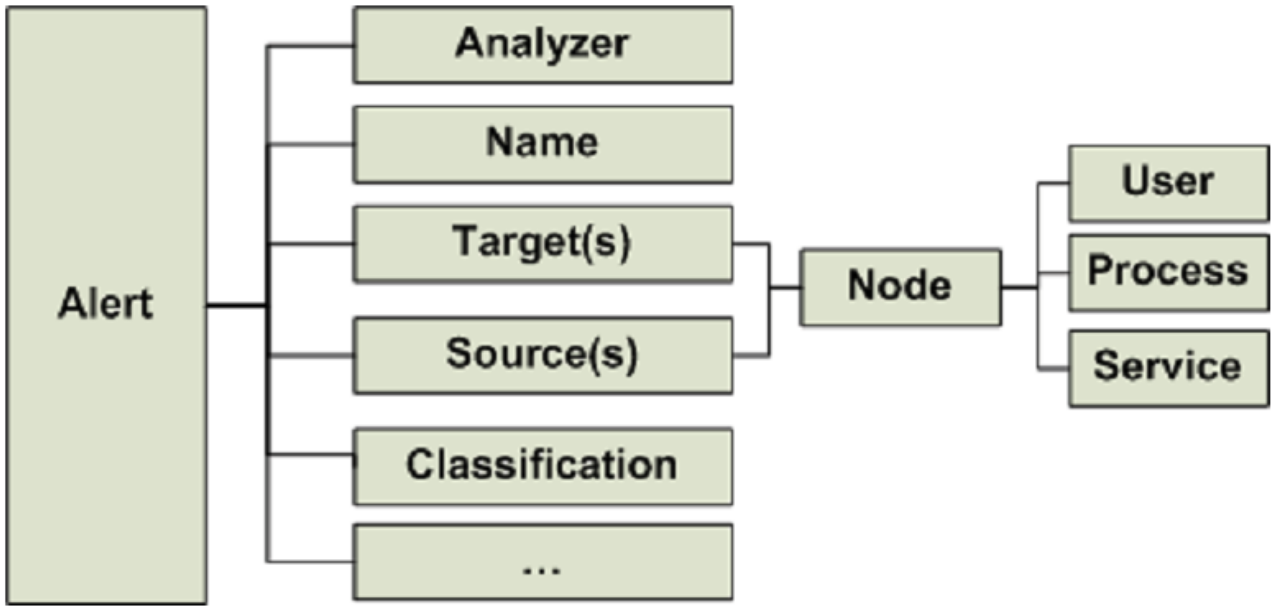


عملیات همبستگی هشدار



یکدست کردن هشدارها

- یکدست کردن syntax و semantic هشدارها
- Syntax: CIDF، IETF-IDWG و IDMEF/IDXP
- Semantic: CVE، Bugtraq و آنتولوژی هشدار
- IDMEF: Intrusion Detection Message Exchange Format

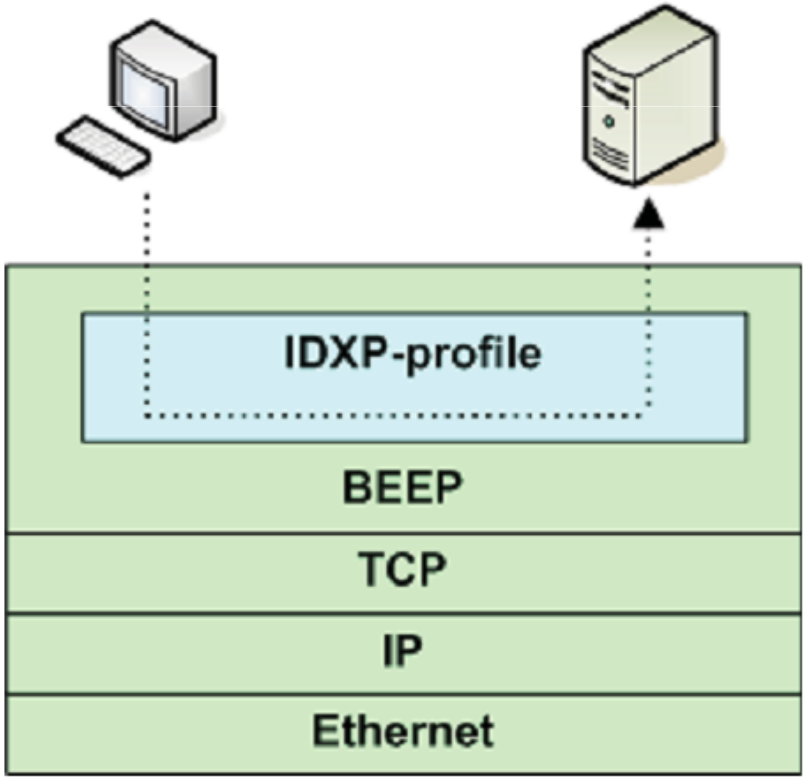


مثالی از IDMEF

```
<IDMEF-Message version="0.3">
  <Alert ident="12345" impact="unknown">
    <Analyzer analyzerid="Snort:1.8.6:9.8.7.6">
      <Node><name>brp-snort</name></Node>
    </Analyzer>
    <CreateTime ntpstamp="0xc12b141a.0xa5baa000"/>
    <Source><Node>
      <Address category="ipv4-addr">
        <address>1.2.3.4</address></Address>
    </Node></Source>
    <Target><Node>
      <Address category="ipv4-addr">
        <address>9.8.7.5</address></Address>
    </Node></Target>
    <Classification origin="vendor-specific">
    <name>ICMP PING NMAP</name></Classification>
  </Alert>
</IDMEF-Message>
```

IDXP (Intrusion Detection Exchange Protocol)

- BEEP: Block Extensible Exchange Protocol
- IDXP پیام های IDMEF را حمل می کند و به عنوان یک پروفایل BEEP پیاده سازی شده است.



کاهش هشدارها: همجوشی

- حذف هشدارهای بیهوده و تکراری از سنسورهای مختلف

$$f(A_1, A_2) = A_{12} \quad \text{with} \quad \begin{aligned} &A_{12}.\text{start time} = \min(A_1.\text{start time}, A_2.\text{start time}), \\ &A_{12}.\text{end time} = \min(A_1.\text{end time}, A_2.\text{end time}), \\ &\forall_{\text{other attributes a}} : \; A_{12}.\text{a} = A_1.\text{a} \bigcup A_2.\text{a} \end{aligned}$$

$$\begin{aligned} \text{if } (&|A_1.\text{start time} - A_2.\text{start time}| < t \;\wedge\; |A_1.\text{end time} - A_2.\text{end time}| < t \;\wedge \\ &A_1.\text{sensor} \neq A_2.\text{sensor} \;\wedge \\ &\forall_{\text{all other attributes a defined in both } A_1 \text{ and } A_2} : \; A_1.\text{a} = A_2.\text{a}) \end{aligned}$$

کاهش هشدارها: درستی سنجی

- شناسایی و حذف حملات نا موفق و نا مربوط
- منفعل
  - حذف حملاتی که روی آسیب پذیری های قدیمی و رفع شده صورت می گیرند.
  - مانیتور کردن اتفاقاتی که بعد از نفوذ صورت می گیرد.
- فعال
  - اتصال به هاست ها و چک کردن پروسس ها
  - اتصال به هاست ها و چک کردن فایل های پیکربندی

همبستگی

- دو دیدگاه برای ایجاد همبستگی:
  - خوشه بندی هشدارها
    - برقراری ارتباط بین هشدارها
    - مانند anomaly detection (آماری و احتمالی)
  - تشخیص نیت نفوذگر
    - بررسی الگوهای نفوذ
    - مانند misuse detection (الگوهای از قبل تعریف شده)

بازسازی ریسمان (thread) هشدارها

- خوشه بندی هشدارها
- بسته بندی هشدارها در ریسمان ها بر اساس شباهت های زمانی و مکانی
- هشدارهای جدید به ریسمان هایی بیشتر match باشند، اضافه می شوند. یک ریسمان نشان دهنده یک حمله (نشست) است.
  - کدام خصوصیات باید مقایسه شوند؟
  - روش مقایسه:
    - Matching دقیق یا Fuzzy Matching
  - هر خصوصیت چه وزنی دارد؟

سناریوهای حمله از قبل تعریف شده

- تشخیص نیت نفوذگر

Attack scenario	Characteristics
1 source, 1 attack, 1 target	Same src IP, dst IP, attack type
1 source, * attacks, 1 target	Same src IP, dst IP
* sources, * attacks, 1 target	Same dst IP, attack type
1 source, 1 attack, * targets	Same src IP, attack type

تحلیل پیشنیاز-پیامد

- تشخیص نیت نفوذگر

(fact, prerequisite, consequence)

- Hyper-alert
  - Fact: مشخص کننده خصوصیات یک هشدار است.
  - Prerequisite: مشخص کننده شرایط لازم برای اتفاق افتادن حمله به طور موفق آمیز
  - Consequence: مشخص کننده نتایج حمله است.
    - می تواند به عنوان پیشنیاز حملات دیگر باشد.
  - به صورت فرمول های منطقی با استفاده از AND و OR بیان می شود.

Hyper Alert Type

- (fact, prerequisite, consequence)
- SadmindBufferOverflow =

  ({VictimIP, VictimPort},

  ExistHost(VictimIP) AND
  VulnerableSadmind(VictimIP)

  {GainRootAccess(VictimIP)})

ارتباط بین هشدار ها

- یک هشدارA آماده سازی برای یک هشدار B را انجام می دهد اگر:
  - A پیش نیاز های هشدار B را فراهم کند
  - A قبل از هشدار B اتفاق بیافتد.

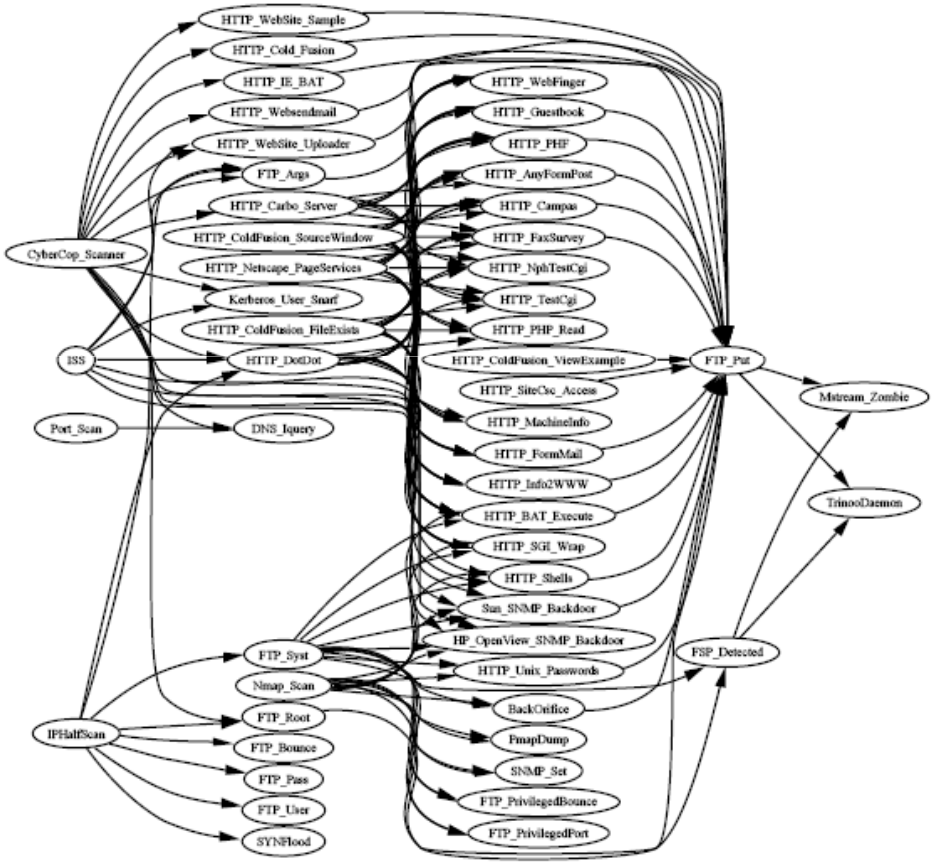
گراف همبستگی

- یک گراف جهت دار بدون دور(Direrected Acylic Graph) است که گره های آن هشدار ها و لبه های آن ارتباط "آماده سازی-برای" هشدار ها است.
- این گراف که از هشدار ها ساخته می شود می تواند بسیار بزرگ باشد.
  - با تجمیع هشدار ها می تواند کاهش داده شود.
  - برای هشدار ها در یک محدود زمانی نزدیک ایجاد شود.

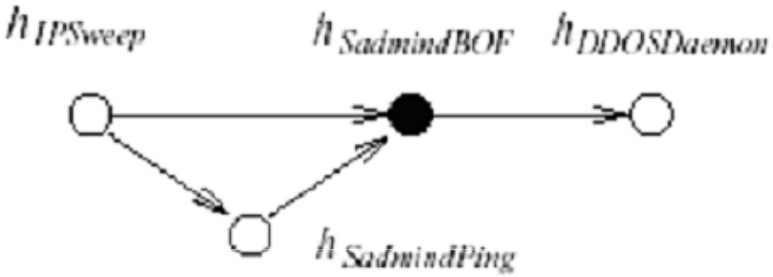
تجزیه گراف

- با استفاده از مشخصه های خاص مانند آدرس فرستنده و گیرند، هشدار ها خوشخ بندی می شوند و برای هر خوشه یک گراف جداگانه درست می شود
- مشخصه ها توسط آنالیز کننده هشدار ها تعریف می شود

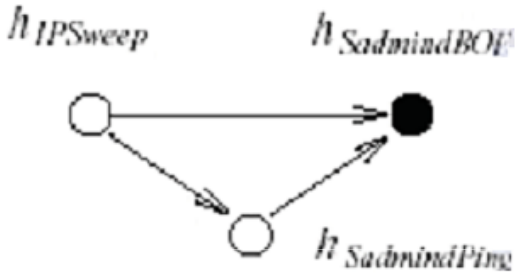
یک گراف تجریه شده و خلاصه شده



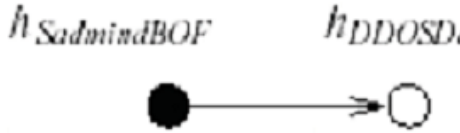
Hyper-alert



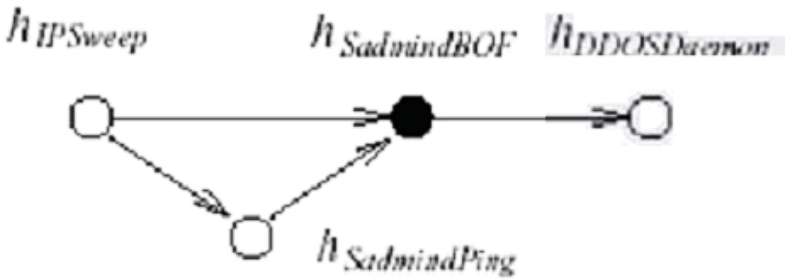
(a) A hyper-alert correlation graph HG



(b) $PG = precedent(h_{SadmindBOF}, HG)$



(c) $SG = subsequent(h_{SadmindBOF}, HG)$



(d) $CG = correlated(h_{SadmindBOF}, HG)$

تطبیق سناریو های حمله

- با در نظر گرفتن محدویت های زمانی برای هشدار ها و در نظر گرفتن مثلا آدرس IP مقصد می توان گراف هشدار ها را با سناریو های حمله های شناخته شده تطبیق داده و نوع حمله را معلوم کرد.
- تطبیق بااستفاده از شباهت گراف ها انجام می شود.

مراجع

1. P. Ning, Y. Cui, D. Reeves, "Constructing Attack Scenarios through Correlation of Intrusion Alerts", In CCS 2002

2. P. Ning, D. Reeves, Y. Cui, "Correlating Alerts Using Prerequisites of Intrusions", Technical Report, TR-2001-13, North Carolina State University, Department of Computer Science, December 2001
3. P. Ning, Y. Cui, D. Reeves, "Analyzing Intensive Intrusion Alerts via Correlation", In Recent Advances in Intrusion Detection, 2002
4. P. Ning, D. Xu, "Learning Attack Strategies from Intrusion Alerts", In CCS 2003
5. P. Ning, D. Xu, C. Healey, R. St. Amant, "Building Attack Scenarios through Integration of Complementary Alert Correlation Methods", NDSS, February 2004
6. Y. Zhai, P. Ning, P. Iyer, D. Reeves, "Reasoning about Complementary Intrusion Evidence", 20th Annual Computer Security Applications Conference, December 2004
7. D. Xu, P. Ning, "Alert Correlation Through Triggering Events and Common Resources", 20th Annual Computer Security Applications Conference, December 2004
8. P. Ning, D. Xu, "Hypothesizing and Reasoning about Attacks Missed by Intrusion Detection Systems", ACM Transactions on Information and System Security, 2004