MIMOS

Innovation for Life

Intrusion Alert Correlation

by
Norazah Aziz (GCIA)
Cyberspace Security Lab, MIMOS Berhad

Outline

- Why Correlation?
- Correlation Process
- Correlation Techniques
- Conclusion

Terminologies

- **Correlation**
  - The degree to which or more attributes or measurements on the same group of elements show a tendency to vary together. Source: http://dictionary.reference.com/browse/correlation
- **Event**
  - Low level entity that analyzed by IDS eg: Network packets
- **Alert**
  - Generated by IDS to notify of the interesting events.
- **Alert Correlation**
  - Multi step process that receives alerts from one or more intrusion detection systems as input and produces a high-level description of the malicious activity on the network.

Outline

- Why Correlation?
- Correlation Process
- Correlation Techniques
- Conclusion
- Q&A

Correlation can address some if the IDS weaknesses

- Alert Flooding
  - generate a large amount of alerts
- Context
  - not group related alerts
- False Alert
  - generate a false negative and false positive
- Scalability
  - difficult to achieve large-scale deployment

With correlation..

- Can capture a high level view of the attack activity on the target network without losing security-relevant information.

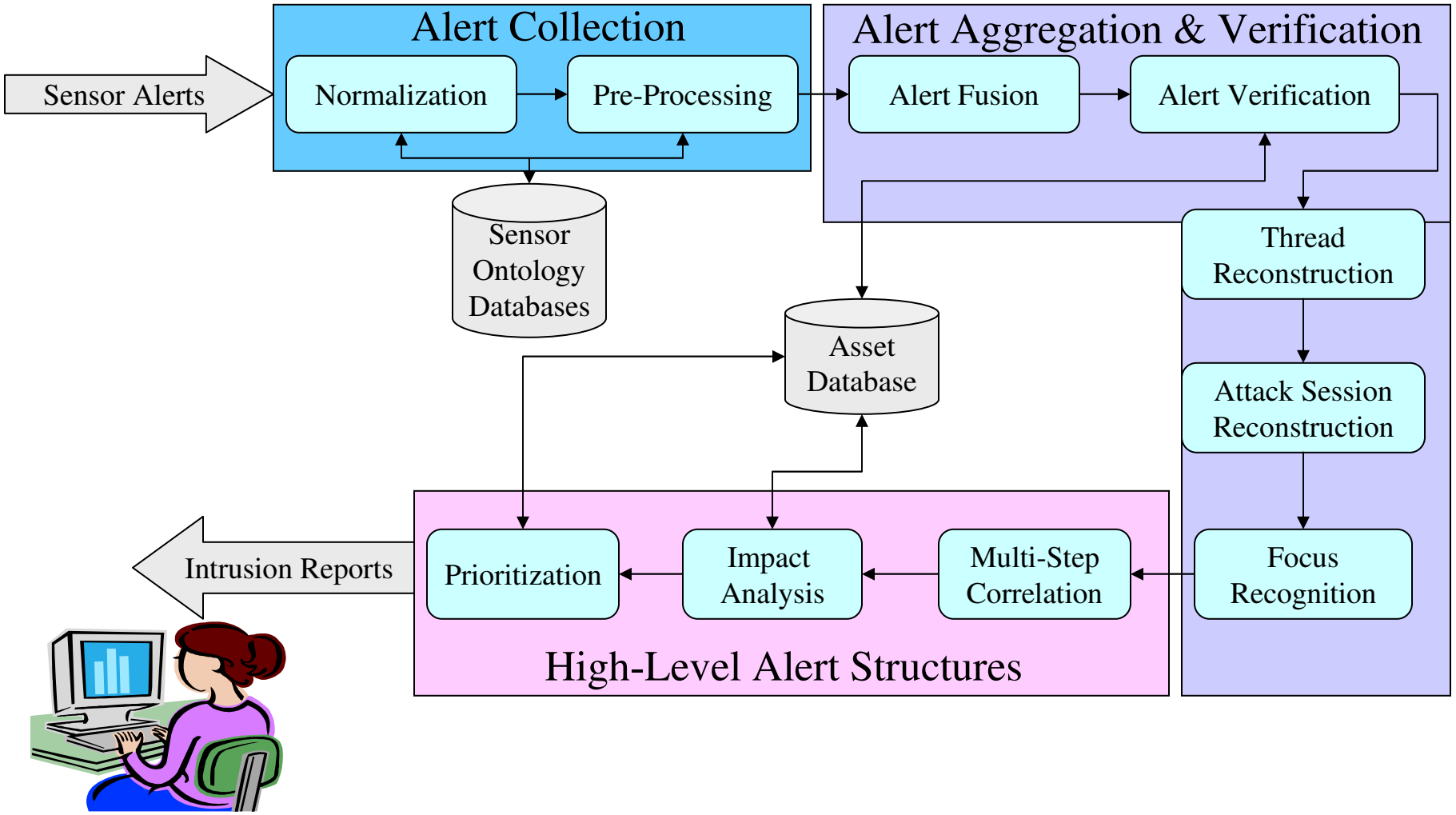
Outline

- Why Correlation?
- Correlation Process
- Correlation Techniques
- Conclusion
- Q&A

Main correlation process

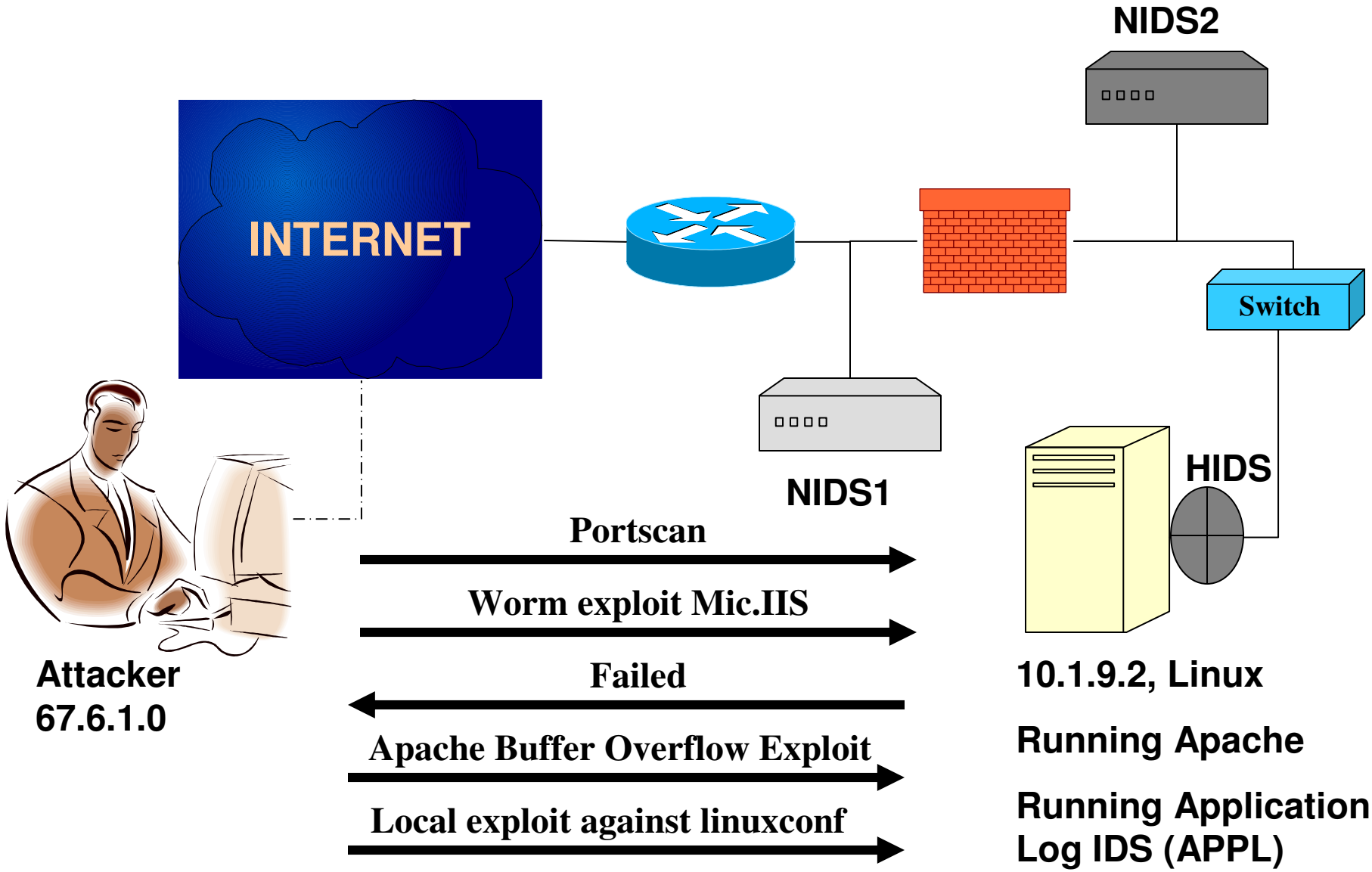
- Alert Collection
- Alert Aggregation and Verification
- High Level Alert Structures

Correlation Process



Sources: Kruegel et.al, Intrusion Detection and Correlation Challenges and Solution.

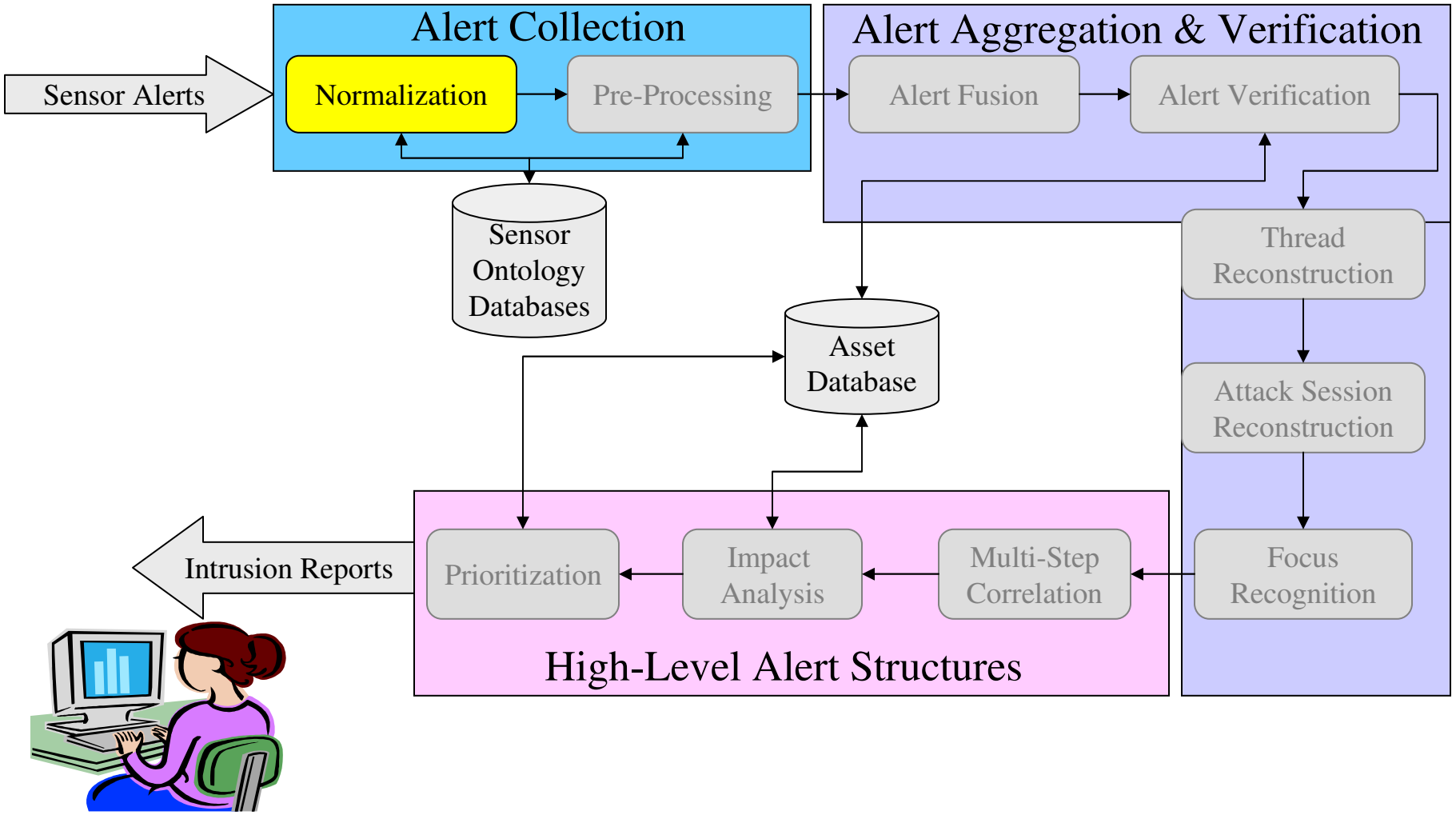
Attack Scenario Example



Attack Scenario Alerts

ID	Signature	Start/End	Src IPs	Dest IPs	Sensor	Tag
1	Scanning	09:1/13:9	67.6.1.0	10.1.9.2	NIDS2	
2	Portscan	09:0/14:1	67.6.1.0	10.1.9.2	NIDS1	
3	IIS Exploit	11:5/11:5	20.9.0.1	10.1.9.2, port:80	NIDS1	
4	Apache Exploit	19:0/19:0	67.6.1.0	10.1.9.2 port:80	NIDS1	
5	Bad Request	19:1/19:1		Localhost, Apache	APPL	
6	Local Exploit	21:3/21:3		linuxconf	HIDS	
7	Local Exploit	21:4/21:4		linuxconf	HIDS	

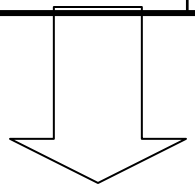
Alert Normalization



Sources: Kruegel *et.al*, Intrusion Detection and Correlation Challenges and Solution.

Alert Normalization

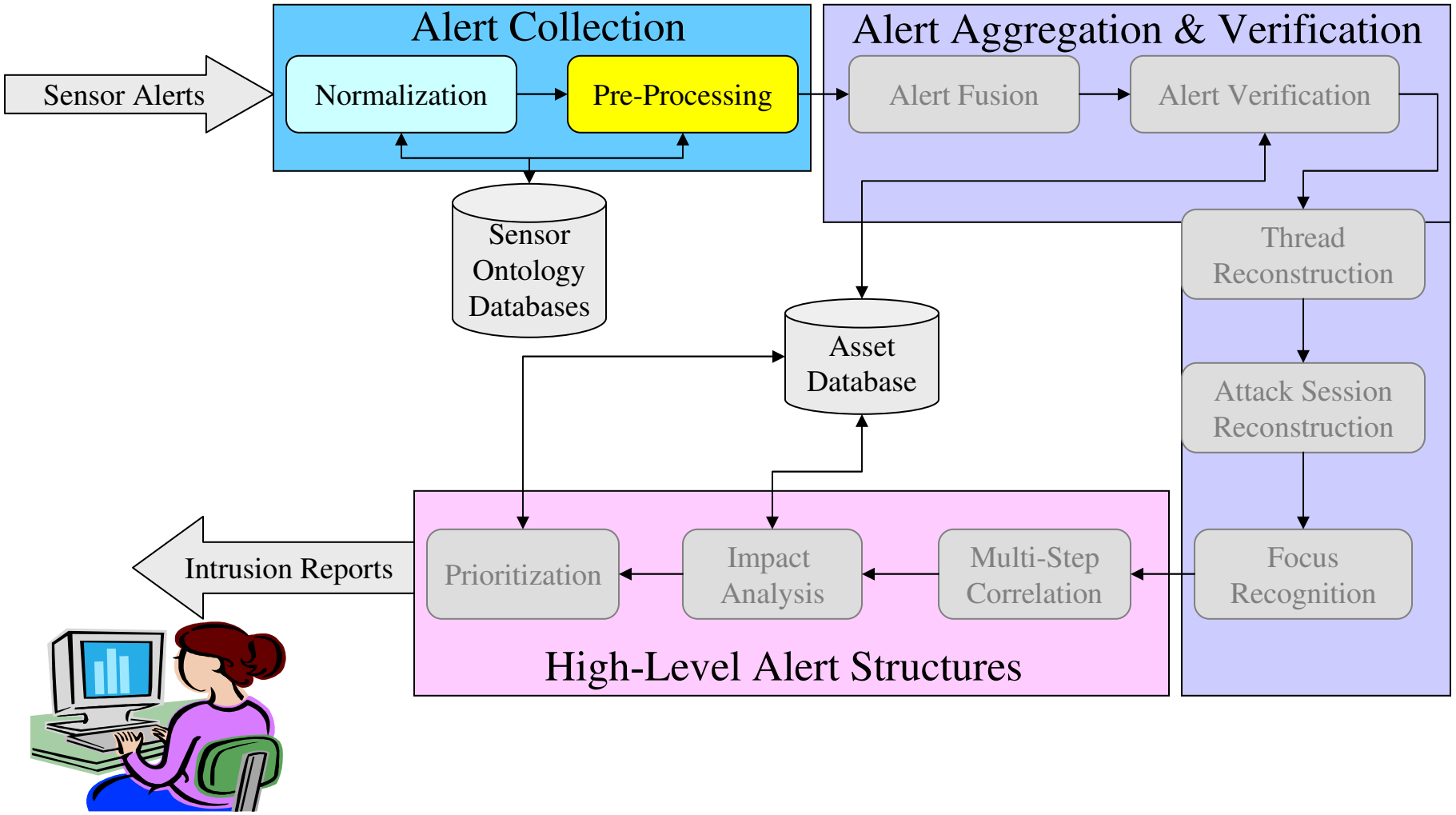
ID	Signature	Start/End	Src IPs	Dest IPs	Sensor	Tag
1	Scanning	09:1/13:9	67.6.1.0	10.1.9.2	NIDS2	
2	Portscan	09:0/14:1	67.6.1.0	10.1.9.2	NIDS1	
3	IIS Exploit	11:5/11:5	20.9.0.1	10.1.9.2, port:80	NIDS1	
4	Apache Exploit	19:0/19:0	67.6.1.0	10.1.9.2 port:80	NIDS1	
5	Bad Request	19:1/19:1		Localhost, Apache	APPL	
6	Local Exploit	21:3/21:3		linuxconf	HIDS	
7	Local Exploit	21:4/21:4		linuxconf	HIDS	



Standardize the alert messages in different formats using CVE (Common Vulnerabilities and Exposures)

ID	Signature	Start/End	Src IPs	Dest IPs	Sensor	Tag
1	Portscan	09:1/13:9	67.6.1.0	10.1.9.2	NIDS2	
2	Portscan	09:0/14:1	67.6.1.0	10.1.9.2	NIDS1	

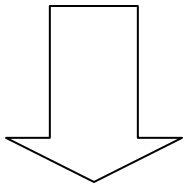
Alert Preprocessing



Sources: Kruegel et.al, Intrusion Detection and Correlation Challenges and Solution.

Alert Preprocessing

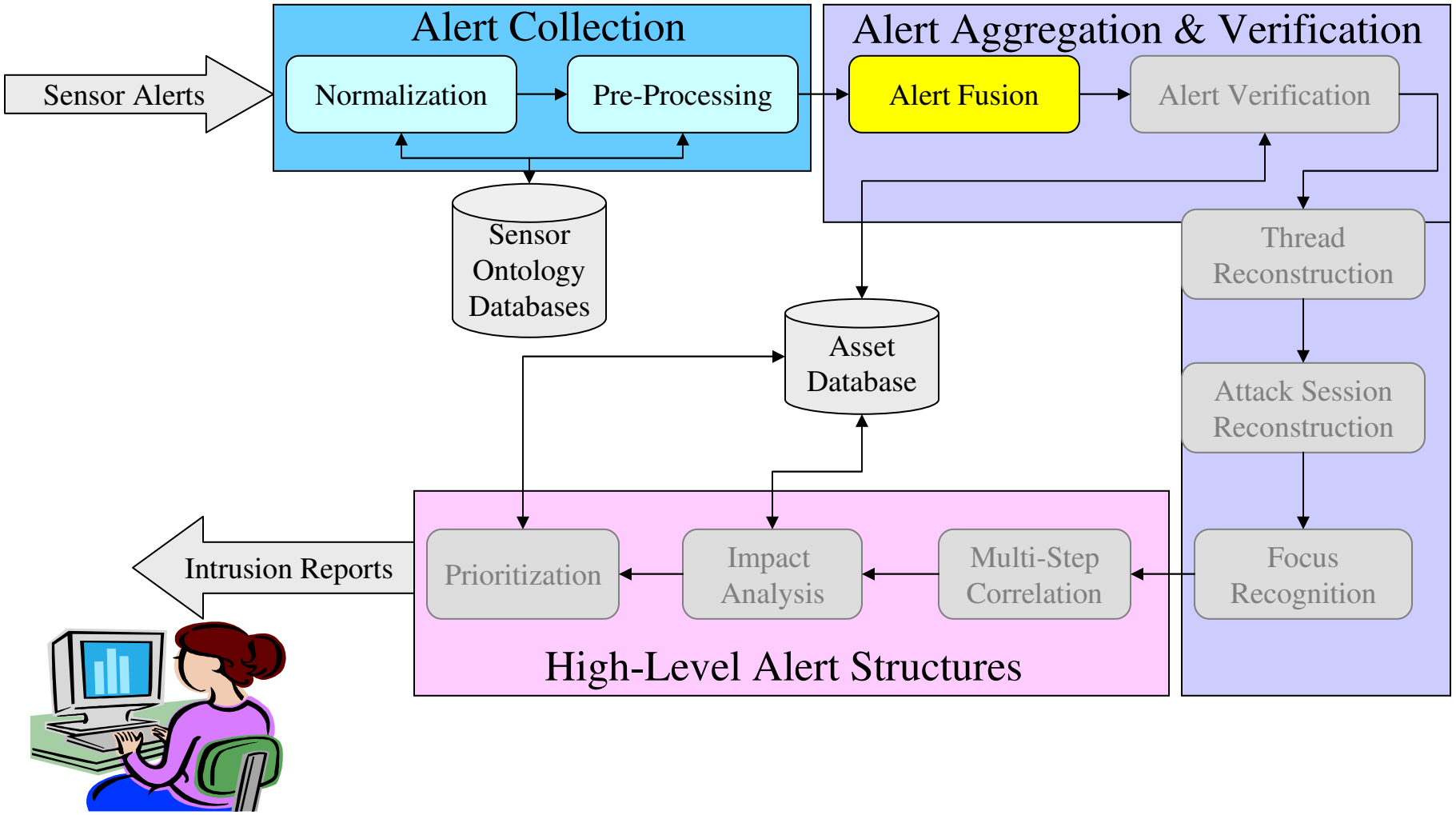
ID	Signature	Start/End	Src IPs	Dest IPs	Sensor	Tag
1	Portscan	09:1/13:9	67.6.1.0	10.1.9.2	NIDS2	
2	Portscan	09:0/14:1	67.6.1.0	10.1.9.2	NIDS1	
3	IIS Exploit	11:5/11:5	20.9.0.1	10.1.9.2, port:80	NIDS1	
4	Apache Exploit	19:0/19:0	67.6.1.0	10.1.9.2 port:80	NIDS1	
5	Bad Request	19:1/19:1		Localhost, Apache	APPL	
6	Local Exploit	21:3/21:3		linuxconf	HIDS	
7	Local Exploit	21:4/21:4		linuxconf	HIDS	



Supply best-effort values information by determine the alert's source and target

ID	Signature	Start/End	Src IPs	Dest IPs	Sensor	Tag
5	Bad Request	19:1/19:1	10.1.9.2	10.1.9.2, Apache	APPL	
6	Local Exploit	21:3/21:3	10.1.9.2	10.1.9.2, linuxconf	HIDS	
7	Local Exploit	21:4/21:4	10.1.9.2	10.1.9.2, linuxconf	HIDS	

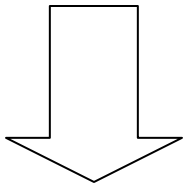
Alert Fusion



Sources: Kruegel et.al, Intrusion Detection and Correlation Challenges and Solution.

Alert Fusion

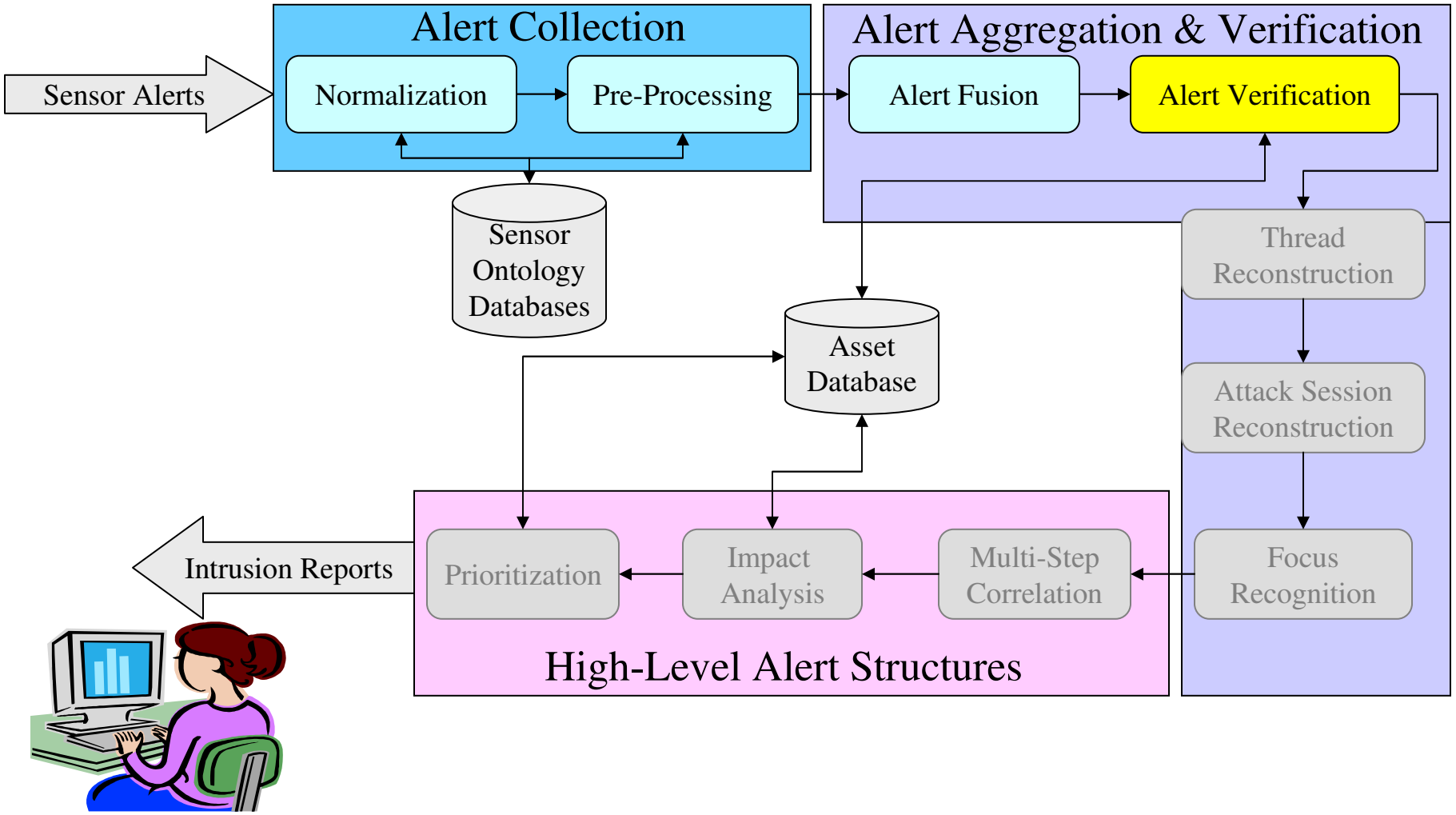
ID	Signature	Start/End	Src IPs	Dest IPs	Sensor	Tag
1	Portscan	09:1/13:9	67.6.1.0	10.1.9.2	NIDS2	
2	Portscan	09:0/14:1	67.6.1.0	10.1.9.2	NIDS1	
3	IIS Exploit	11:5/11:5	20.9.0.1	10.1.9.2, port:80	NIDS1	
4	Apache Exploit	19:0/19:0	67.6.1.0	10.1.9.2 port:80	NIDS1	
5	Bad Request	19:1/19:1	10.1.9.2	10.1.9.2, Apache	APPL	
6	Local Exploit	21:3/21:3	10.1.9.2	10.1.9.2, linuxconf	HIDS	
7	Local Exploit	21:4/21:4	10.1.9.2	10.1.9.2, linuxconf	HIDS	



Identifies alerts that refer to the same underlying event

ID	Signature	Start/End	Src IPs	Dest IPs	Sensor	Tag
7	Local Exploit	21:4/21:4	10.1.9.2	10.1.9.2, linuxconf	HIDS	
8	Meta-Alert-	09:0/13:9	67.6.1.0	10.1.9.2	{NIDS1,NIDS2}	{1,2}

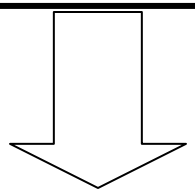
Alert Verification



Sources: Kruegel et.al, Intrusion Detection and Correlation Challenges and Solution.

Alert Verification

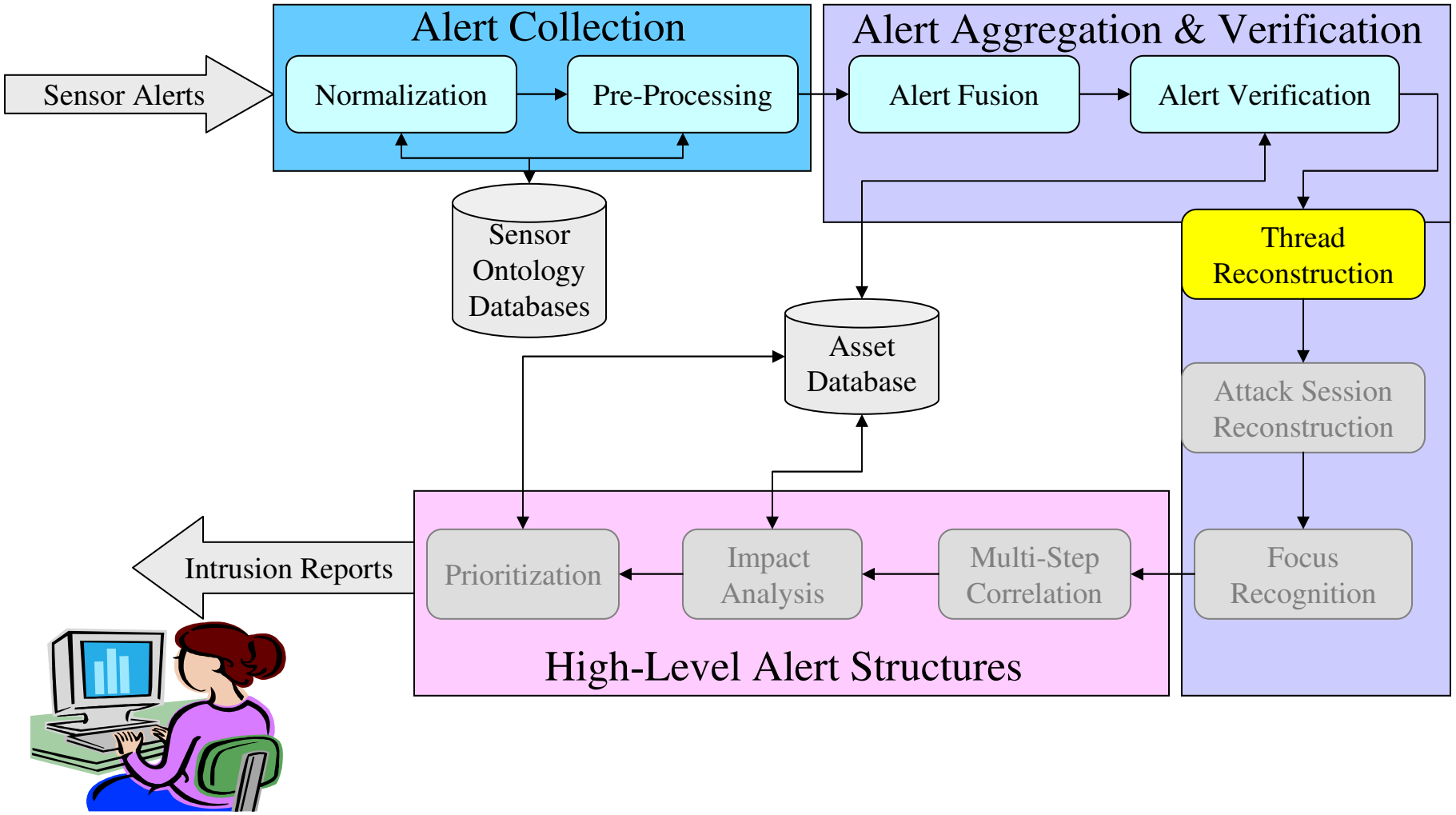
ID	Signature	Start/End	Src IPs	Dest IPs	Sensor	Tag
1	Portscan	09:1/13:9	67.6.1.0	10.1.9.2	NIDS2	
2	Portscan	09:0/14:1	67.6.1.0	10.1.9.2	NIDS1	
3	IIS Exploit	11:5/11:5	20.9.0.1	10.1.9.2, port:80	NIDS1	
4	Apache Exploit	19:0/19:0	67.6.1.0	10.1.9.2 port:80	NIDS1	
5	Bad Request	19:1/19:1	10.1.9.2	10.1.9.2, Apache	APPL	
6	Local Exploit	21:3/21:3	10.1.9.2	10.1.9.2, linuxconf	HIDS	
7	Local Exploit	21:4/21:4	10.1.9.2	10.1.9.2, linuxconf	HIDS	
8	Meta-Alert-	09:0/13:9	67.6.1.0	10.1.9.2	{NIDS1,NIDS2}	{1,2}



Remove or ignore the irrelevant alerts, e.g. unsuccessful alert

ID	Signature	Start/End	Src IPs	Dest IPs	Sensor	Tag
3	IIS Exploit	11:5/11:5	20.9.0.1	10.1.9.2, port:80	NIDS1	Irrelevant
4	Apache Exploit	19:0/19:0	67.6.1.0	10.1.9.2 port:80	NIDS1	

Attack Thread Reconstruction



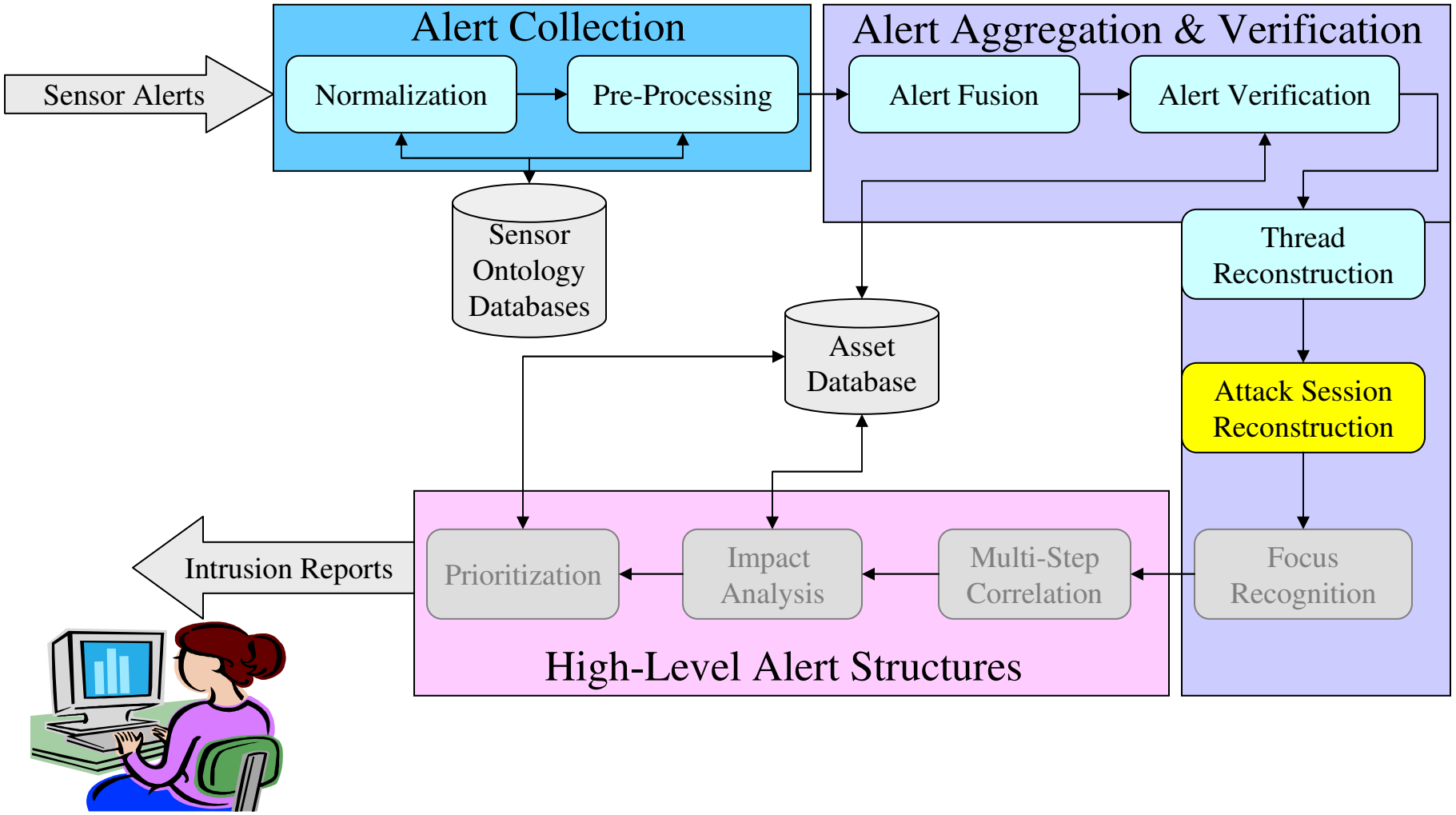
Sources: Kruegel et.al, Intrusion Detection and Correlation Challenges and Solution.

Thread Reconstruction

ID	Signature	Start/End	Src IPs	Dest IPs	Sensor	Tag
1	Portscan	09:1/13:9	67.6.1.0	10.1.9.2	NIDS2	
2	Portscan	09:0/14:1	67.6.1.0	10.1.9.2	NIDS1	
3	IIS Exploit	11:5/11:5	20.9.0.1	10.1.9.2, port:80	NIDS1	irrelevant
4	Apache Exploit	19:0/19:0	67.6.1.0	10.1.9.2, port:80	NIDS1	correlated
5	Bad Request	19:1/19:1	10.1.9.2	10.1.9.2, Apache	APPL	
6	Local Exploit	21:3/21:3	10.1.9.2	10.1.9.2, linuxconf	HIDS	correlated
7	Local Exploit	21:4/21:4	10.1.9.2	10.1.9.2, linuxconf	HIDS	correlated
8	Meta-Alert	09:0/13:9	67.6.1.0	10.1.9.2	{NIDS1,NIDS2}	{1,2} correlated
9	Meta-Alert	09:0/19:0	67.6.1.0	10.1.9.2, port:80	{NIDS1,NIDS2}	{4,8}
10	Meta-Alert	21:3/21:4	10.1.9.2	10.1.9.2, linuxconf	HIDS	{6,7}

Combines a series of alerts that refer to attacks launched by one attacker against a single target.

Attack Session Reconstruction



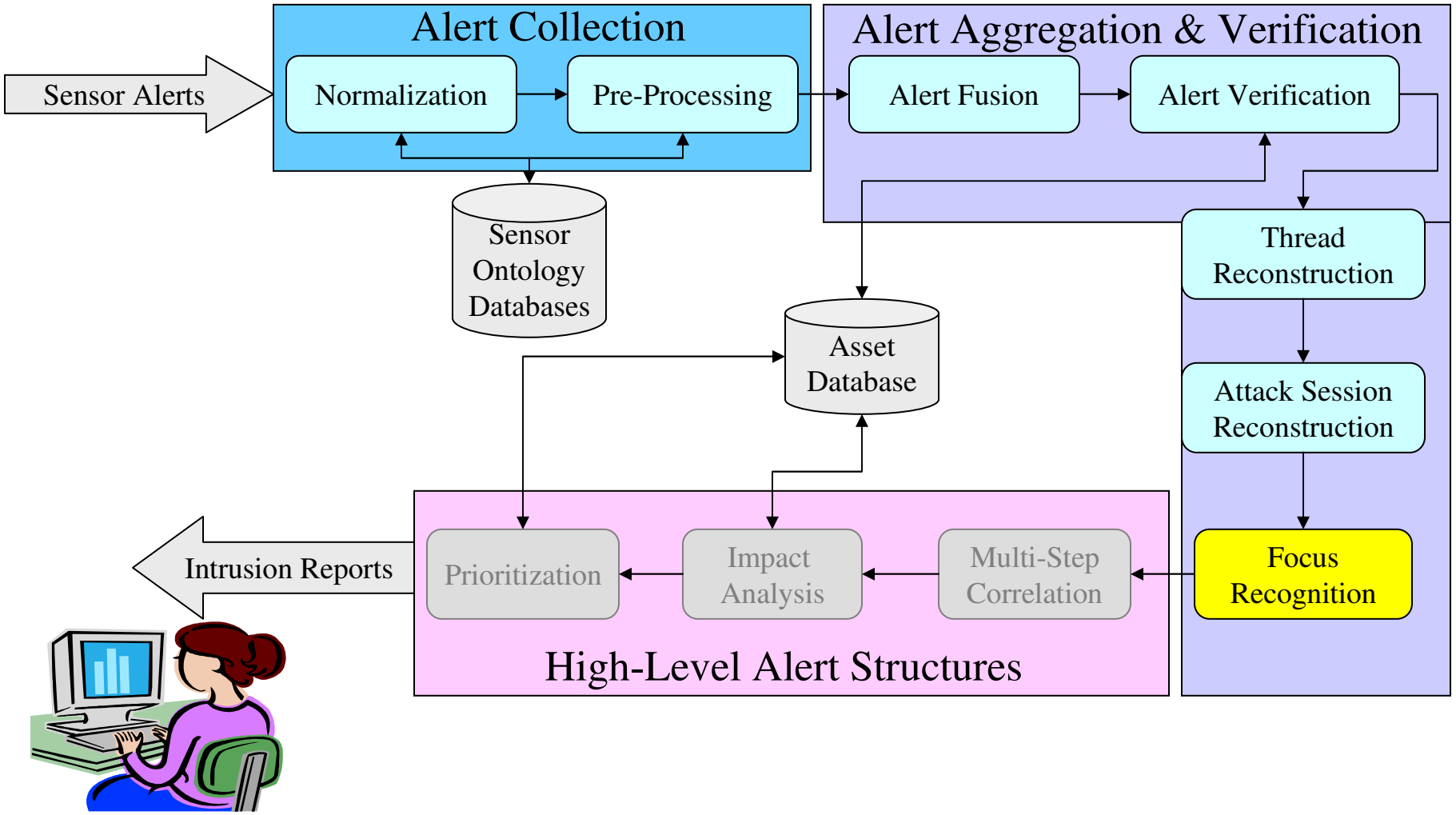
Sources: Kruegel et.al, Intrusion Detection and Correlation Challenges and Solution.

Session Reconstruction

ID	Signature	Start/End	Src IPs	Dest IPs	Sensor	Tag
1	Portscan	09:1/13:9	67.6.1.0	10.1.9.2	NIDS2	
2	Portscan	09:0/14:1	67.6.1.0	10.1.9.2	NIDS1	
3	IIS Exploit	11:5/11:5	20.9.0.1	10.1.9.2, port:80	NIDS1	irrelevant
4	Apache Exploit	19:0/19:0	67.6.1.0	10.1.9.2, port:80	NIDS1	correlated
5	Bad Request	19:1/19:1	10.1.9.2	10.1.9.2, Apache	APPL	
6	Local Exploit	21:3/21:3	10.1.9.2	10.1.9.2, linuxconf	HIDS	correlated
7	Local Exploit	21:4/21:4	10.1.9.2	10.1.9.2, linuxconf	HIDS	correlated
8	Meta-Alert	09:0/13:9	67.6.1.0	10.1.9.2	{NIDS1,NIDS2}	{1,2} correlated
9	Meta-Alert	09:0/19:0	67.6.1.0	10.1.9.2, port:80	{NIDS1,NIDS2}	{4,8}
10	Meta-Alert	21:3/21:4	10.1.9.2	10.1.9.2, linuxconf	HIDS	{6,7}
11	Meta-Alert	09:0/19:1	{67.6.1.0 ,10.1.9.2}	10.1.9.2, port:80, Apache	{NIDS1,NIDS2, APPL}	{5,9}

Linking network-based to host-based alerts

Attack Focus Recognition

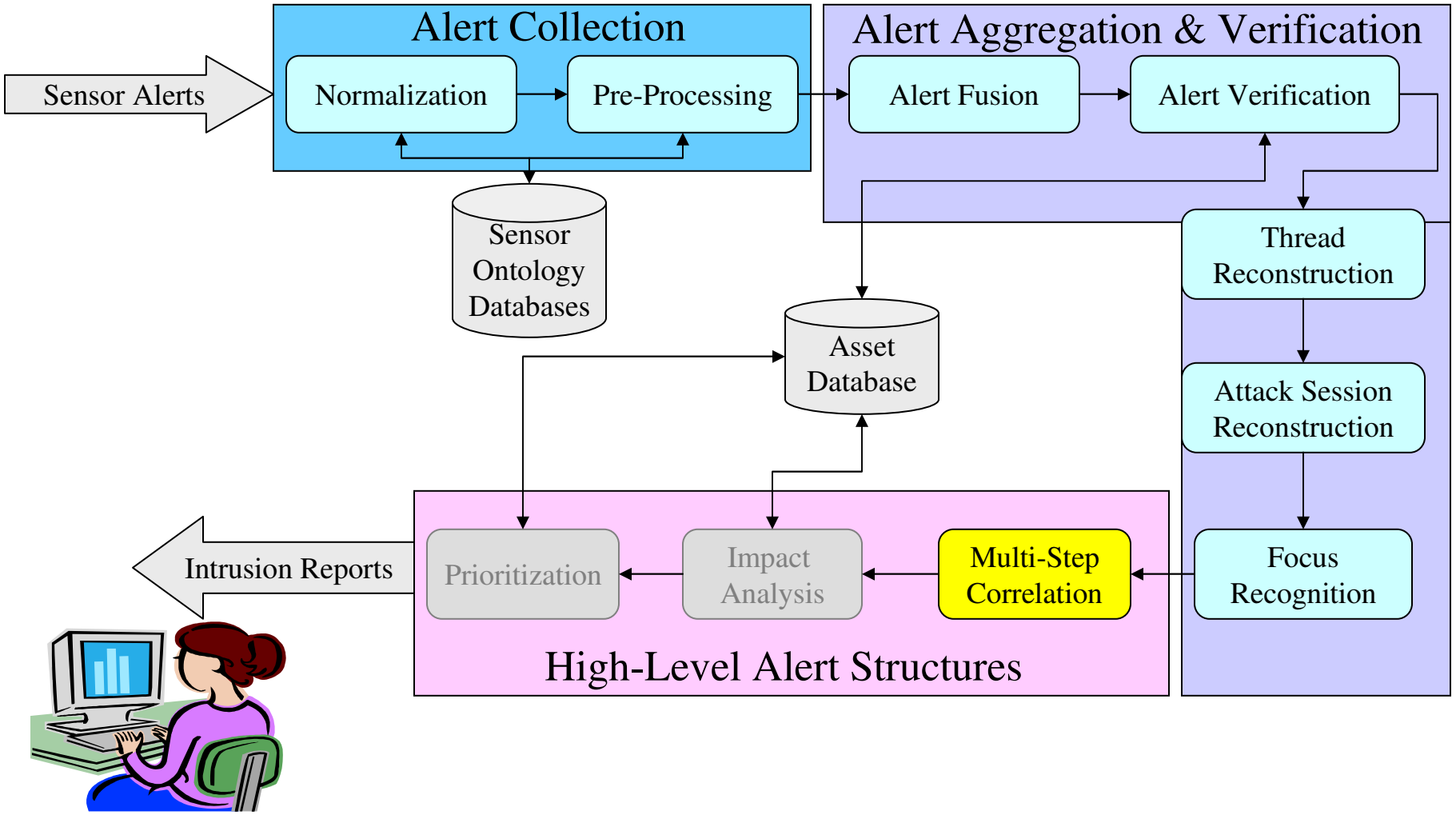


Sources: Kruegel et.al, Intrusion Detection and Correlation Challenges and Solution.

Attack Focus Recognition

- To identify hosts that are either source or the target of a substantial amount of attacks.
- Effective in reducing the number of alerts caused by DDoS and portscan activity.
- Example: Several portscan alerts against multiple targets from the same source, alerts would be merged into a one2many meta-alert.

Multi Step Correlation



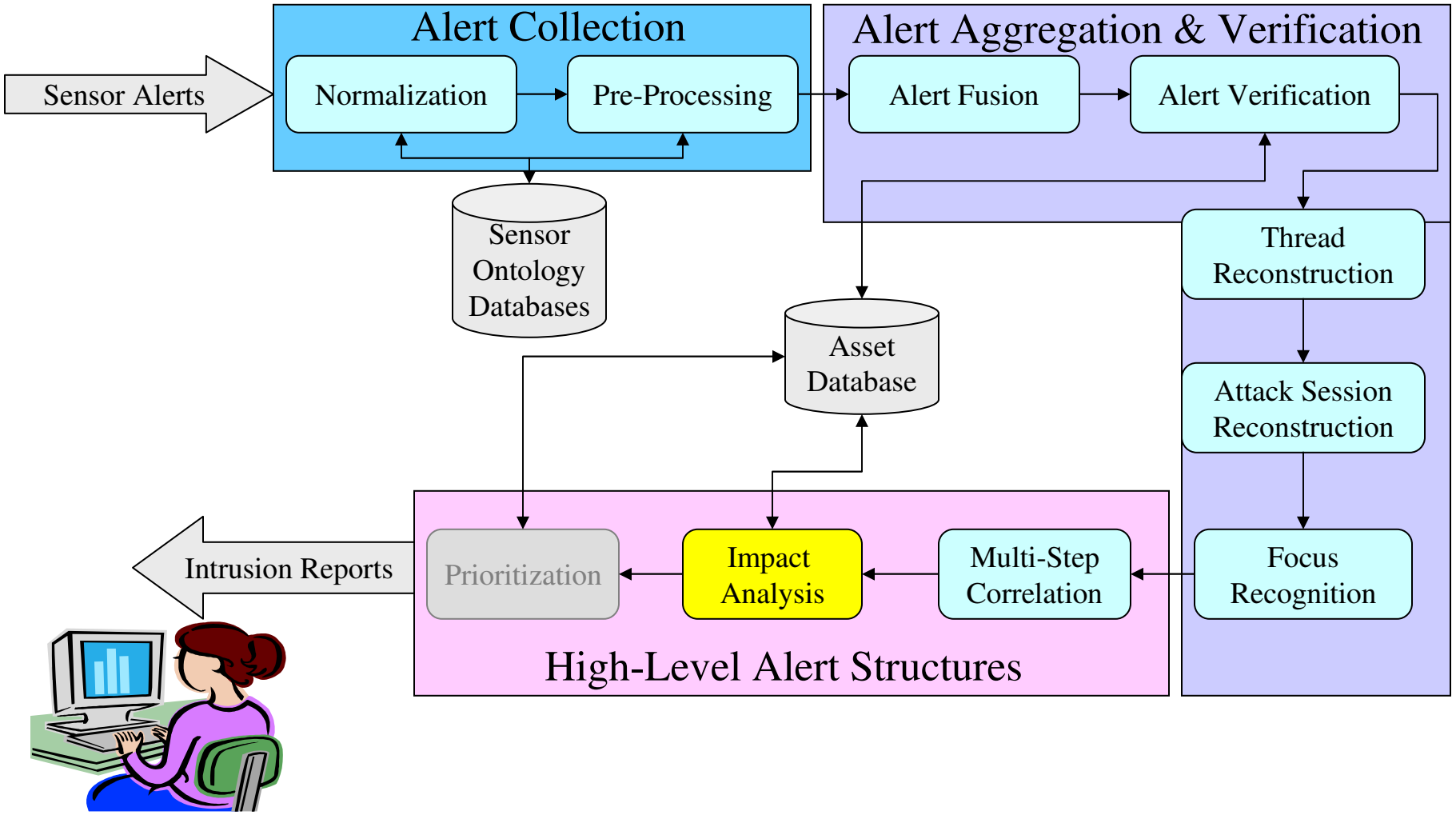
Sources: Kruegel et.al, Intrusion Detection and Correlation Challenges and Solution.

Multistep Correlation

ID	Signature	Start/End	Src IPs	Dest IPs	Sensor	Tag
1	Portscan	09:1/13:9	67.6.1.0	10.1.9.2	NIDS2	
2	Portscan	09:0/14:1	67.6.1.0	10.1.9.2	NIDS1	
3	IIS Exploit	11:5/11:5	20.9.0.1	10.1.9.2, port:80	NIDS1	irrelevant
4	Apache Exploit	19:0/19:0	67.6.1.0	10.1.9.2, port:80	NIDS1	correlated
5	Bad Request	19:1/19:1	10.1.9.2	10.1.9.2, Apache	APPL	
6	Local Exploit	21:3/21:3	10.1.9.2	10.1.9.2, linuxconf	HIDS	correlated
7	Local Exploit	21:4/21:4	10.1.9.2	10.1.9.2, linuxconf	HIDS	correlated
8	Meta-Alert	09:0/13:9	67.6.1.0	10.1.9.2	{NIDS1,NIDS2}	{1,2} correlated
9	Meta-Alert	09:0/19:0	67.6.1.0	10.1.9.2, port:80	{NIDS1,NIDS2}	{4,8}
10	Meta-Alert	21:3/21:4	10.1.9.2	10.1.9.2, linuxconf	HIDS	{6,7} correlated
11	Meta-Alert	09:0/19:1	{67.6.1.0 ,10.1.9.2}	10.1.9.2, port:80, Apache	{NIDS1,NIDS2,APPL}	{5,9} correlated
12	Meta-Alert	09:0/21:4	{67.6.1.0 ,10.1.9.2}	10.1.9.2, port:80, Apache, linuxconf	{NIDS1,NIDS2,APPL,HIDS}	{10,11}

Defined by using some form of expert knowledge (attack scenario)

Impact Analysis

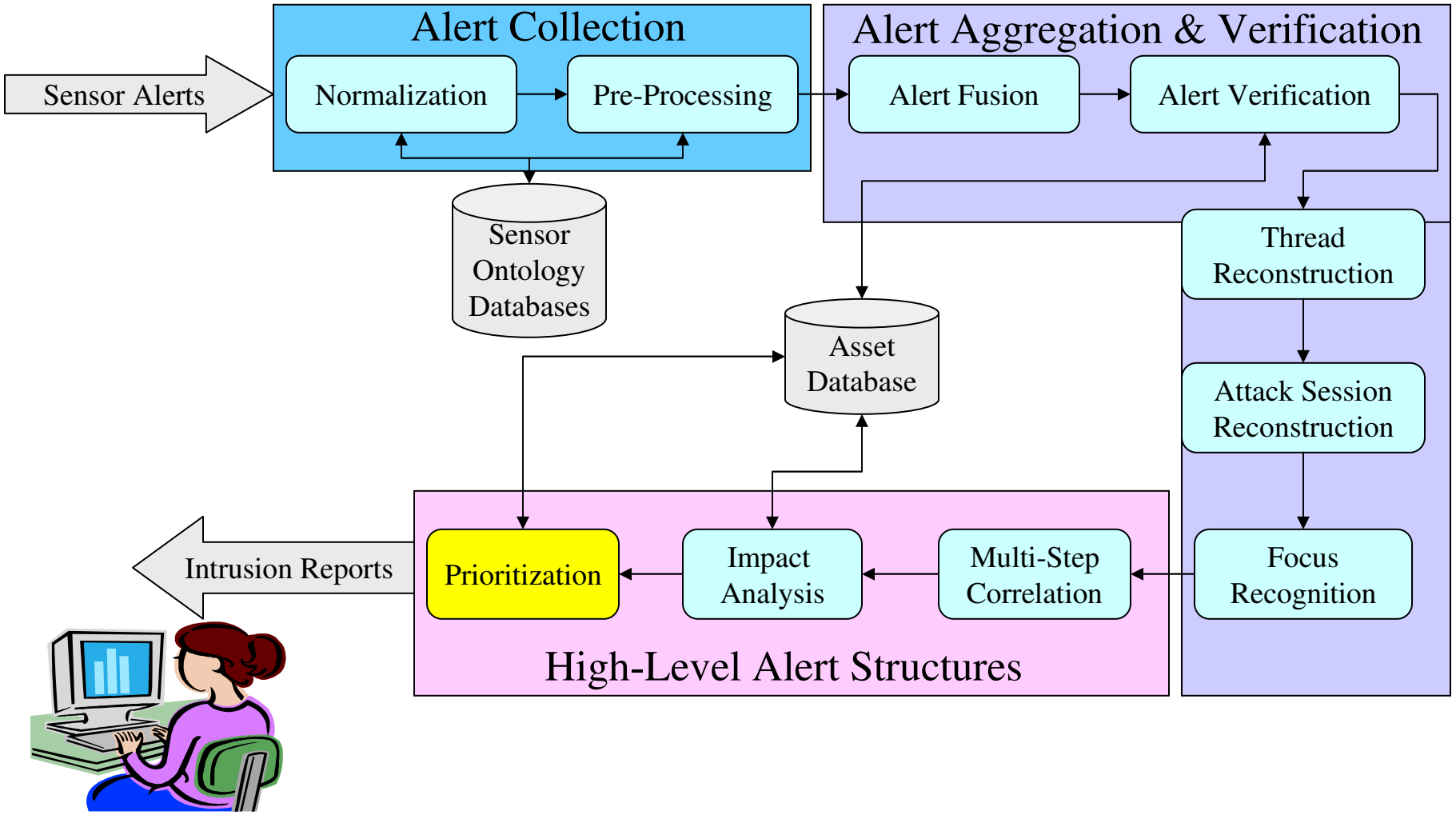


Sources: Kruegel et.al, Intrusion Detection and Correlation Challenges and Solution.

Impact Analysis

- To analyze alerts with regard to their impact on the network infrastructure and the attached resources.
- Example:
  - Dependency between mail services that requires an operational domain name service (DNS) to work properly.

Alert Prioritization



Sources: Kruegel et.al, Intrusion Detection and Correlation Challenges and Solution.

Prioritization

ID	Signature	Description	Priority	Tag	Ref Tag
1	Portscan		LOW	correlated	
2	Portscan		LOW	correlated	
3	IIS Exploit		LOW	Irrelevant	
4	Apache Exploit		LOW	correlated	
5	Bad Request		LOW	correlated	
6	Local Exploit		LOW	correlated	
7	Local Exploit		LOW	correlated	
8	Meta-Alert	Fused Portscan	LOW	correlated	{2,3}
9	Meta-Alert	Remote Attack Thread	LOW	correlated	{8,4}
10	Meta-Alert	Local Attack Thread	LOW	correlated	{6,7}
11	Meta-Alert	Remote Attack Session	LOW	correlated	{9,5}
12	Meta-Alert	Multistep Attack Scenario	HIGH		{11,10}

To define appropriate priorities related to the attack's impact and the effect of a response by classify alerts (high, medium or low)

Outline

- Why Correlation?
- Correlation Process
- Correlation Techniques
- Conclusion
- Q&A

Correlation Techniques

- Similar Attack Attributes
- Pre-defined Attack Scenarios
- Pre & Post Condition of Individual Attack
- Statistical Causality Analysis

Technique 1: Similar Attack Attributes

- Alerts belonging to the same attack often have similar attributes
- To recognize correlation – inspect alert attributes and finding similarities between them
- Well-founded list of alert attributes such as *sensor, alert thread, source and destination IPs, ports* and *time*.
- Emerald system is an example of such implementation

Technique 2: Pre-defined Attack Scenarios

- Process of filling in attack scenarios templates and formulate them.
- Attack scenarios are broken down to explicit correlation rules.
- Restricted to known attacks and misuse detection only
- Specified by human users or learned through training datasets
- Example of implementation : Attack Specification Language (ASL)

Technique 3: Pre & Post Condition of Individual Attack

- Powerful mechanism of expressing correlation criteria
- Based on the preconditions and consequences of individual attacks; correlates alerts if the pre-condition of some later alerts are satisfied by the consequences of some earlier alerts.
- Uncover the causal relationship between alerts, and is not restricted to known attack scenarios.

Technique 4: Statistical Causality Analysis

- Misuse detection toward anomaly detection
- Not feasible solution for the complete correlation process
- But it can be utilized as a part of a larger system to pre-process alerts or to provide meta-alert signatures.
- Example of implementation: Granger Causality Test (GCT)

Outline

- Why Correlation?
- Correlation Process
- Correlation Techniques
- Conclusion
- Q&A

Conclusion

- IDS is still needed and the correlation is the effective means to analyze the alert to high level view picture.
- Research on better correlation with detectable unknown attack need to be done.

References

- Christopher Kruegel, Fredrik Valeur, Giovanni Vigna (2005). Intrusion Detection and Correlation, Challenges and Solution, Springer Science+Business Media Inc, USA.
- Antti Hatala, *et al*, “Event Data Exchange and Intrusion Alert Correlation in Heterogeneous Networks”, Proceeding of the 8th Collogquium for Information Systems Security Education West Point, NY, June 2004
- Xinzhou Qin, *et al*, “Statistical Causality of INFOSEC Alert Data”; in Proceedings of Recent Advances in Intrusion Detection 2003.
- Hervé Debar and Andreas Wespi: “Aggregation and correlation of Intrusion-Detection Alerts”; in Proceedings of Recent Advances in Intrusion Detection 2001.
- Peng Ning , *et al*, “Constructing attack scenarios through correlation of intrusion alerts”; in Proceedings of the 9th ACM conference on Computer and Communications security; 2002.
- Hervé Debar and Andreas Wespi: “Aggregation and correlation of Intrusion-Detection Alerts”; in Proceedings of Recent Advances in Intrusion Detection 2001.

MIMOS

Innovation for Life

Thank You