

Case Study: The IA:AIDE System at Two

Aaron L. Temin, Ph. D.
Litton PRC
temin_aaron@prc.com



Overview

- **Background**
- **Conceptual Architecture**
- **Initial Design and Implementation**
- **Results of Live Demonstrations**
- **Changes for the Future**
- **Conclusion**



Background

- Less than **4%** of penetrated systems detected an attack, Less than **1%** responded to the penetration
- Attack correlation and attack prediction elusive
- Hard to differentiate between serious attacks and “ankle-biters”
- Auto-parsing and query mechanisms needed across DOD
- Demand for rapid dissemination of detect patterns
- No technical capability for detecting wide-scale attacks



Background

- **IA:AIDE is an advanced concept technology demonstration (ACTD) for the DoD**
- **Limited lifespan program to demonstrate the benefit of:**
 - **Visual integration of existing sensors**
 - **Correlation of multiple sensors**
 - **Hierarchical/network distribution and correlation of alerts across the DII**



Conceptual Architecture

Some Existing Tool/Technologies

Intrusion Detection

Events
ASCII Data

Firewall

Protocol
Packets

SW Integrity

Check
sums

Virus Checkers

ASCII

Network Mngmt

Events
ASCII Data

Interface
Layer

D
A
T
A

B
R
I
D
G
E

Integration Infrastructure

Correlation

Filtering

Data
Visualization

WARNING

Law Enforcement

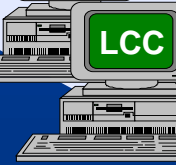
Operations

Comm/Computers

Intel

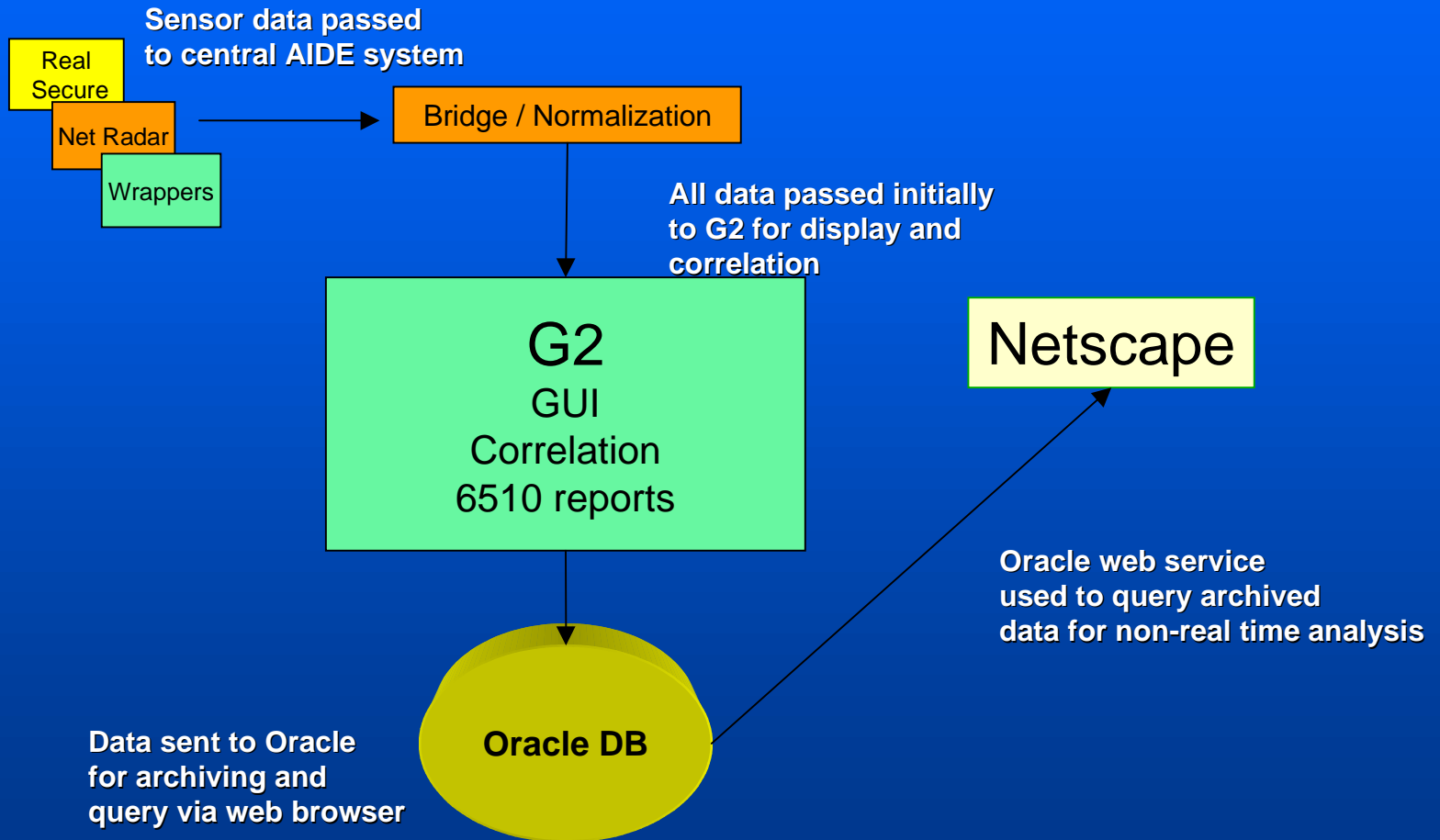
N
E
T
W
O
R
K

I
N
T
E
R
F
A
C
E





Initial Design and Implementation



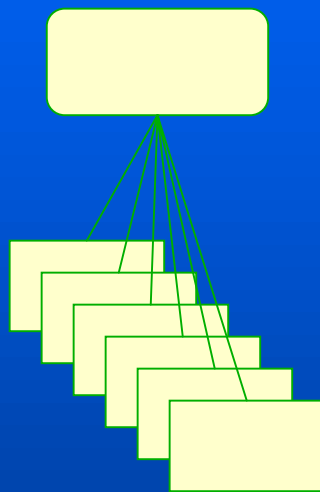


Results of Live Demonstrations

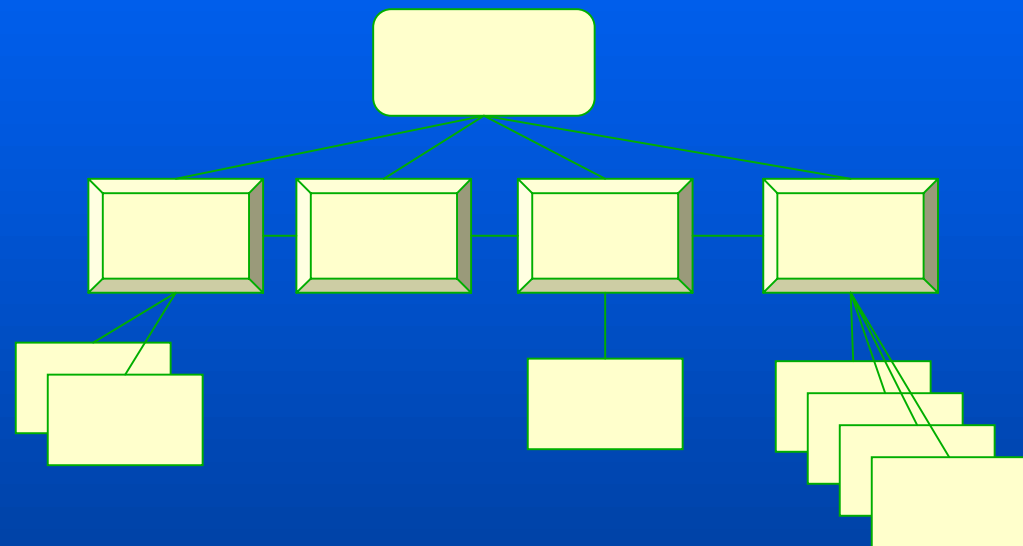
- **Networks**
- **Sensors**
- **Accomplishments**
- **Warfighter Feedback**



Networks



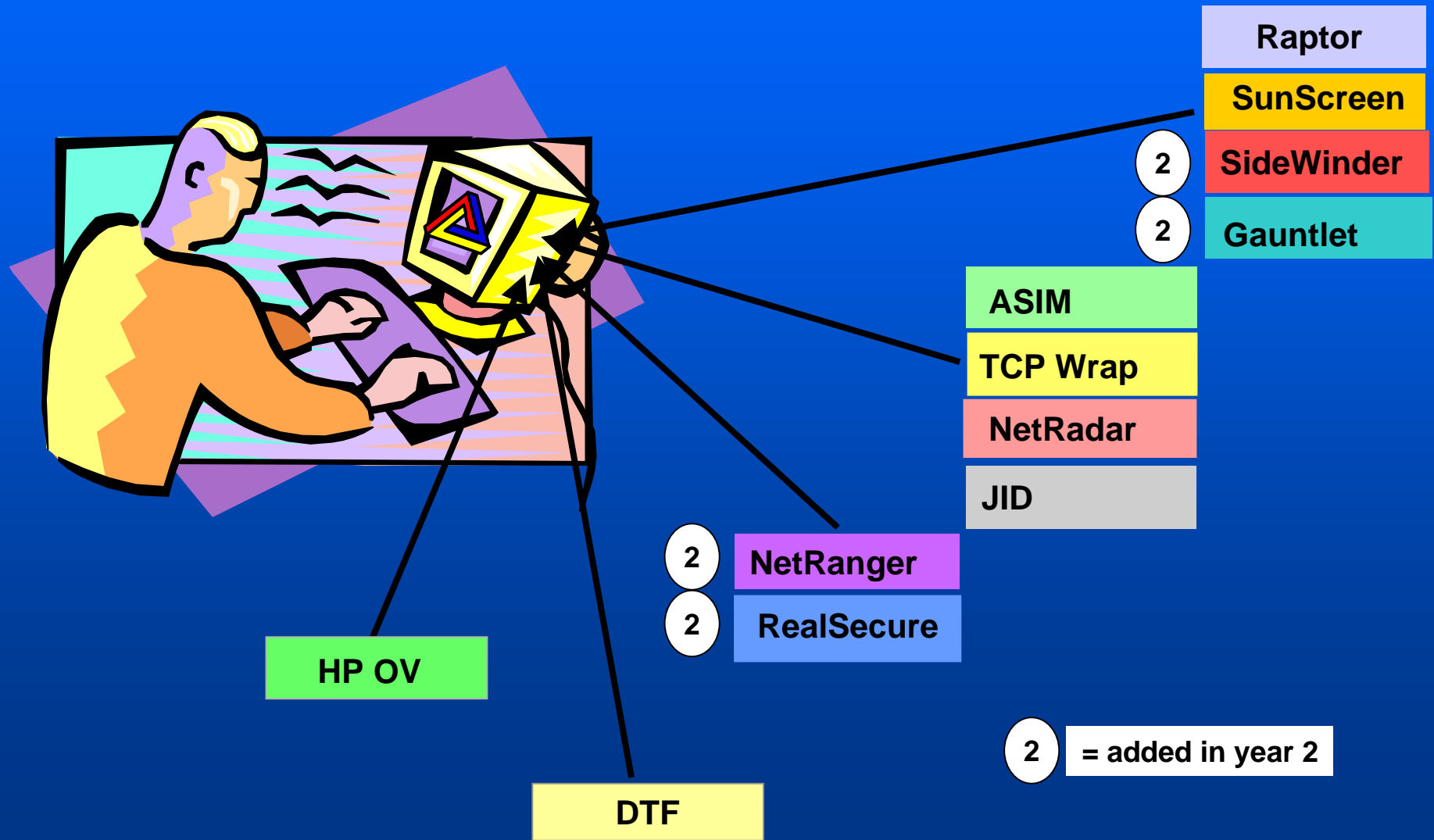
Year 1: 7 nodes, 2 levels



Year 2: 12 nodes, 3 levels



Sensors





Year One Accomplishments

- **Firsts:**
 - **Automated alert capability:**
 - Between multiple services and agencies
 - Between multiple sensors at the services and agencies
- **Improvements to DOD capability**
 - **Data Display: Single display of multi-sensor alerts**
 - **Communication: Secure reporting of events in real time both laterally and vertically**
 - **Database Storage: Single database for all intrusion and anomalous event data**



Year Two Accomplishments

- **Firsts:**
 - **Three-tiered automated reporting structure including multiple services and agencies**
 - **Normalized intrusion data across sensors and sites**
 - **Automated CJCSI 6510 Reporting requirement**
 - **Secure Remote Access to local and regional intrusion databases**
 - **Alert correlation across sensors and sites**
- **Improvements to existing DOD capability**
 - **Web accessible alert database with built-in query capability**
 - **Standardized alert and event times across sensors and sites**



Warfighter Feedback

- **Management**
 - **Considerable improvement in the conduct and planning of the demonstration**
- **Technical**
 - **3 Best Aspects of AIDE**
 - Viewing multiple sensors in one place and the integration of commercial sensors in particular
 - Having web server access to the database
 - Automatic 6510 reporting
 - **3 Worst Aspects of AIDE**
 - User Interface difficult to use
 - Performance problems
 - Data needs to be better displayed

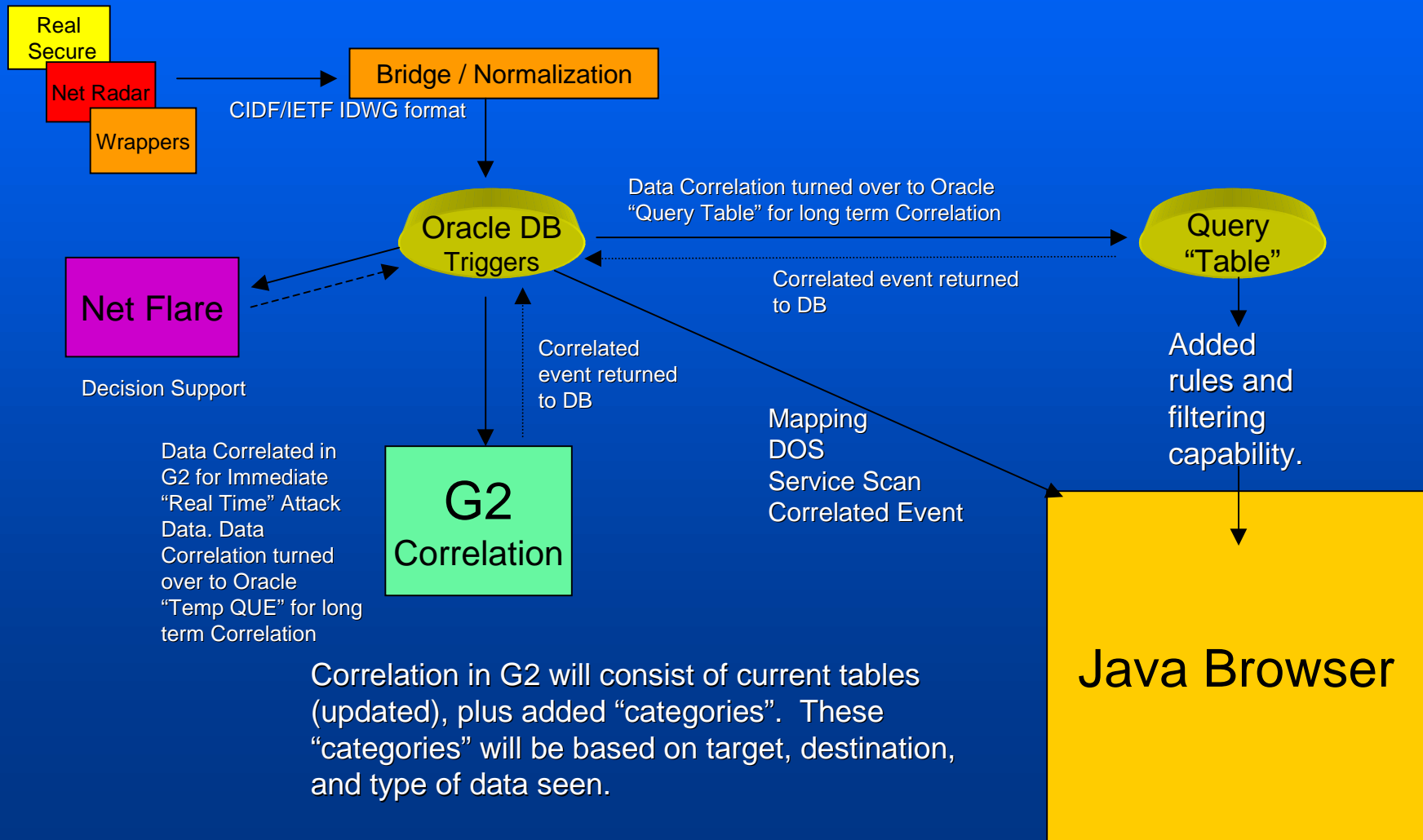


Changes for the Future

- **Data Flow**
- **Correlation**
- **G2's Role**
- **Oracle's Role**
- **Visualization Tools**



Data Flow



Correlation in G2 will consist of current tables (updated), plus added "categories". These "categories" will be based on target, destination, and type of data seen.

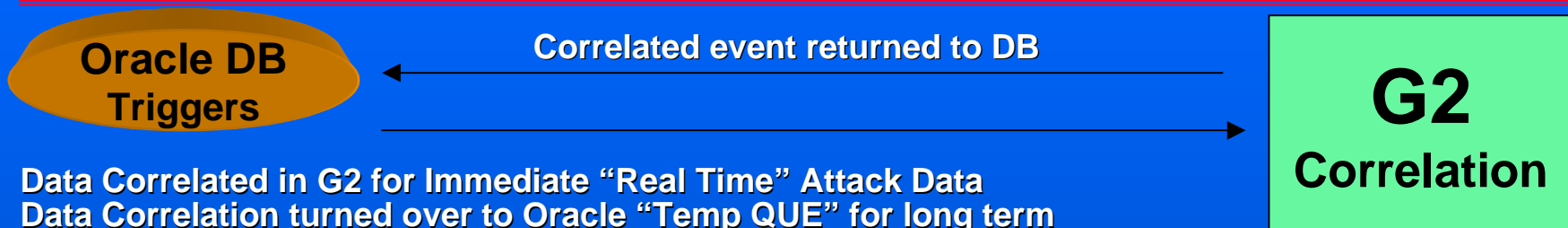


Correlation

- Correlate data from multiple sensors and support near-term and longer-term analysis of collected data:
 - Duplicate events across sensors
 - Related events within/across sensors
 - Related events across sites



G2's Role



Data Correlated in G2 for Immediate "Real Time" Attack Data
Data Correlation turned over to Oracle "Temp QUE" for long term Correlation

- **G2 correlates using current rules plus added categories**
- **Categories of Attacks**

ICMP Attacks

Host Login

System Changes

Web Server Attacks

TCP Port Activity

UDP Port Activity

FTP Server Attacks

Network Login

IP Attacks

TCP/UDP Attacks

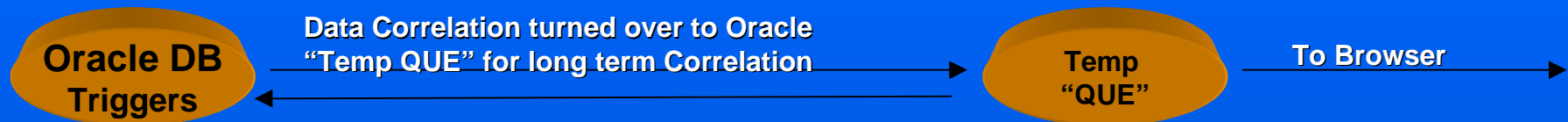
SMTP (Email) Attacks

Misc. Network Attacks

Telnet Attacks



Oracle's Role



- All events assigned Oracle sequence number
- Sequenced events sent to Query Table
- Rule set to be run at time interval on table
- Rule set can be different than G2's
- Once event triggered sent to Java front end and database
- Filtering capabilities



Web Browser to DB


Netscape: File Edit View Go Communicator Help

Back Forward Reload Home Search Netscape Print Security Stop

Location: http://fruitcakes/aide/plsql/query.reduce_frame_set What's Related

WebMail Contact People Yellow Pages Download Channels

GROUP BY DOMAIN		GROUP BY DAY				SOURCE DETAIL					
Domain	Sessions	Source	Day	Port	Sessions	ID	Destination	Signature	Keyword	Information	Username
192.67.80.37	5	192.67.80.37	06-OCT-1999	139	5	3731	128.132.46.172		NEW_TCP_SESSION_EST	Confidence: high	
						3731	128.132.46.172		CLOSE_TCP_SESSION		
						3956	128.132.46.172		NEW_TCP_SESSION_EST	Confidence: high	
						3956	128.132.46.172		CLOSE_TCP_SESSION		
						4101	128.132.46.172		NEW_TCP_SESSION_EST	Confidence: high	
						4101	128.132.46.172		CLOSE_TCP_SESSION		
						4264	128.132.46.172		NEW_TCP_SESSION_EST	Confidence: high	
						4264	128.132.46.172		CLOSE_TCP_SESSION		
						4376	128.132.46.172		NEW_TCP_SESSION_EST	Confidence: high	

 Automated Intrusion Detection Environment



3D Consolidated View

IA:AIDE Browser - C:\AIDE\scenes\GOSC.bt

File Edit Scene Tools View Help

AIDE SITE	CONTACT	EVENTS
AFIWC	0	125
ACC	0	0
AFIWC	0	0
AFRL	0	125
OFFUTT	0	0

Event Activity

- Below Avg
- Average
- Above Avg
- High

AIDE SITE SPACE

SOURCE SPACE

128.132.1.69 Event Information

Source IP	Creation Date	Description	Priority	Protocol	Status	Destination Name	Destination Port	Site Name	Sensor Name	Source
128.132.1.69	1999-07-06 16:32:07.0	unknown	2	unknown	PI	unknown	0	AFRL	ASIM_20_CONN	unkn
128.132.1.69	1999-07-06 16:32:08.0	unknown	2	unknown	PI	unknown	0	AFRL	ASIM_20_CONN	unkn
128.132.1.69	1999-07-06 16:33:40.0	unknown	2	unknown	PI	unknown	0	AFRL	ASIM_20_CONN	unkn
128.132.1.69	1999-07-06 16:39:50.0	unknown	2	unknown	PI	unknown	0	AFRL	ASIM_20_CONN	unkn
128.132.1.69	1999-07-06 16:41:01.0	unknown	2	unknown	PI	unknown	0	AFRL	ASIM_20_CONN	unkn
128.132.1.69	1999-07-06 16:43:44.0	unknown	2	unknown	PI	unknown	0	AFRL	ASIM_20_CONN	unkn
128.132.1.69	1999-07-06 16:43:50.0	unknown	2	unknown	PI	unknown	0	AFRL	ASIM_20_CONN	unkn
128.132.1.69	1999-07-06 16:47:10.0	unknown	2	unknown	PI	unknown	0	AFRL	ASIM_20_CONN	unkn
128.132.1.69	1999-07-06 16:47:13.0	unknown	2	unknown	PI	unknown	0	AFRL	ASIM_20_CONN	unkn
128.132.1.69	1999-07-06 16:47:13.0	unknown	2	unknown	PI	unknown	0	AFRL	ASIM_20_CONN	unkn
128.132.1.69	1999-07-06 16:47:41.0	unknown	2	unknown	PI	unknown	0	AFRL	ASIM_20_CONN	unkn

Start | Shortcut to AIDE_TV... | IA:AIDE Browser - ... | 128.132.1.69 Event Inf... | 5:35 PM

- Site Status
- Sensor Status
- Browser View
- Regional/Global View
- Database Browser



Conclusion

- In the first two years IA:AIDE has significant impact on IA developments
- IA:AIDE enhancements provide a system which:
 - Optimizes the output of multiple types of intrusion detection tools
 - Receives and processes data beyond traditional intrusion detection tools
 - Provides an attack correlation and warning capability
 - Provides an ability to detect patterns indicating wide scale attack





IA:AIDE Points of Contact

Brian Spink

AFRL/IFGB IA:AIDE Program Manager
(315) 330-7596 DSN587

Brad Jobe

Litton PRC Program Manager
315 330-4988

Aaron Temin

Litton PRC IA Technical Expert
703 556-2108