Audit Logging

Security Training by Arctec Group
(www.arctecgroup.net)

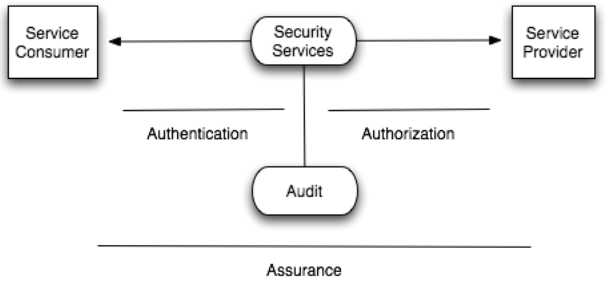
ARCTEC

Overall Goals

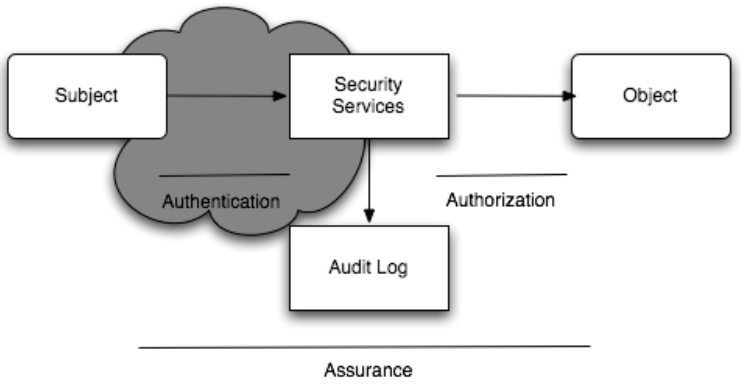
- Building Visibility In
- Audit Logging Domain Model

ARCTEC

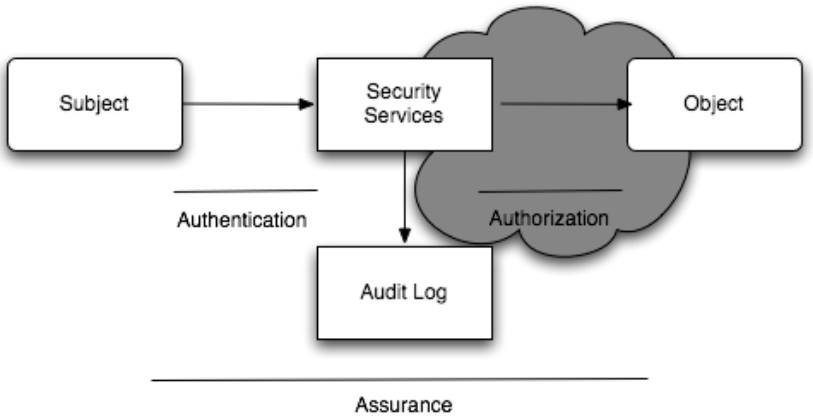
Authentication, Authorization, and Auditing



ARCTEC

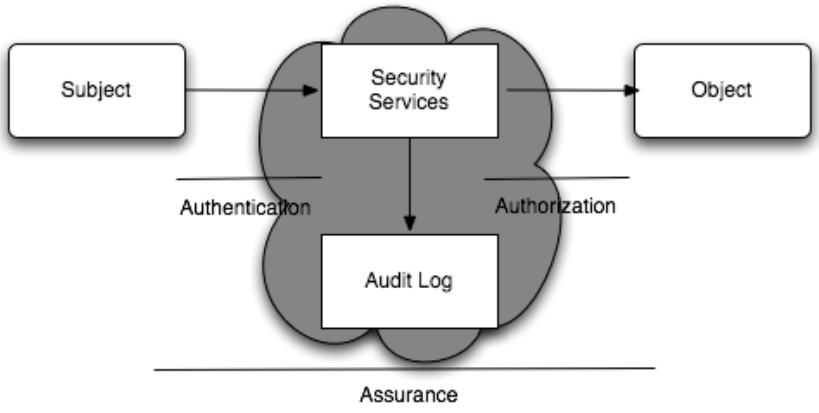


ARCTEC



ARCTEC

5



ARCTEC

6

Auditing

- What to log (Source How to Do Application Logging Right Anton Chuvakin & Gunnar Peterson)
  - AAA (Authentication, Authorization, Access)
    - Authentication/authorization decisions
    - System access, data access
  - Change
    - System/application changes (especially privilege changes)
    - Data change (creation and destruction are changes too)
  - "Badness"/ Threats
    - Invalid input
  - Resource Issues
    - Resource exhausted, capacity exceeded, etc
    - Limit reached
  - Mixed Availability Issues
    - Startups and shutdowns
    - Faults and errors
    - Backups success / failure

ARCTEC

Introduction to Auditing

- What to log (Source How to Do Application Logging Right Anton Chuvakin & Gunnar Peterson)
  - Timestamp + TZ (when)
  - System, application or component (where)
  - User (who)
  - Action (what)
  - Status (result)
  - Priority (severity, importance, rank, level, etc)
  - Reason
- Logging Context
  - Source IP (DNS name, other name, etc)
  - Logging system (process, application, component, sub- component)
  - Affected system (process, application, component, sub- component)

ARCTEC

Designing For Failure

- Developer build applications to accomplish functional requirements - “Place Order”, “Set Price”, “Execute trade”
- Secure coding involves analyzing the software’s failure modes and then design and development for modules to handle these failures in accordance with security policy, for example secure exception handlers that filter sensitive data out of raw exception messages

ARCTEC

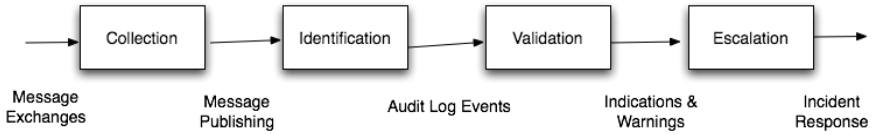
Security Principles: Defensible Networks

Principle	Software Security Example
Defensible Networks can be watched	Audit logging coverage is required for monitoring threats and control efficacy
Defensible Networks limit an intruder’s freedom	Audit logging differs from protection mechanisms, goal of audit logging Is facilitating response activities
Defensible Networks offer a minimum number of services	Audit logging must be placed in the key application and service chokepoints
Defensible networks can be kept current	Must understand the patching and version management of apps and services

- Adapted from the “Tao of Network Security Monitoring” by Richard Bejtlich

ARCTEC

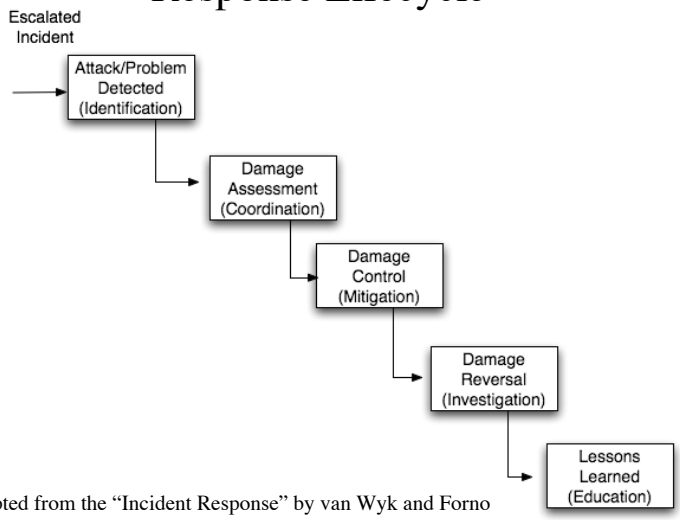
Detection Lifecycle



- Collection: observed message exchanges and events
- Identification: first level categorization of audit log events
- Validation: categorizing audit log events and gathering additional context
- Escalation: forwarding audit log event and context for further handling

- Adapted from the "Tao of Network Security Monitoring" by Richard Bejtlich

Response Lifecycle



- Adapted from the "Incident Response" by van Wyk and Forno

	Developer Logs	Audit Logs
Consumer	Developers, Ops	Security, Auditors
Usage	As needed	Always on
Content	Exceptions, faults, errors	Security incidents, attacks
Scope	Not known	Pre-defined
Time Scope	Useful for limited time	Useful for years

ARCTEC

And now a message from the Payment Card Industry

- Regularly Monitor and Test Networks
  - Requirement 10: Track and monitor all access to network resources and cardholder data.
  - Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult without system activity logs.
    - 10.1 Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.

ARCTEC

And now a message from the Payment Card Industry

- 10.2 Implement automated audit trails for all system components to reconstruct the following events:
  - 10.2.1 All individual accesses to cardholder data
  - 10.2.2 All actions taken by any individual with root or administrative privileges
  - 10.2.3 Access to all audit trails
  - 10.2.4 Invalid logical access attempts
  - 10.2 5 Use of identification and authentication mechanisms
  - 10.2.6 Initialization of the audit logs
  - 10.2.7 Creation and deletion of system-level objects

ARCTEC

And now a message from the Payment Card Industry

- 10.3 Record at least the following audit trail entries for all system components for each event:
  - 10.3.1 User identification
  - 10.3.2 Type of event
  - 10.3.3 Date and time
  - 10.3.4 Success or failure indication
  - 10.3.4 Verify success or failure indication is included in log entries.
  - 10.3.5 Origination of event
  - 10.3.6 Identity or name of affected data, system component, or resource

ARCTEC

And now a message from the Payment Card Industry

- 10.4 Synchronize all critical system clocks and times.
  - 10.4.a Verify that a known, stable version of NTP (Network Time Protocol) or similar technology, kept current per PCI DSS Requirements 6.1 and 6.2, is used for time synchronization.
  - 10.4.b Verify that internal servers are not all receiving time signals from external sources. [Two or three central time servers within the organization receive external time signals [directly from a special radio, GPS satellites, or other external sources based on International Atomic Time and UTC (formerly GMT)], peer with each other to keepaccurate time, and share the time with other internal servers.]
  - 10.4.c Verify that specific external hosts are designated from which the timeservers will accept NTP time updates (to prevent a malicious individual from changing the clock). Optionally, those updates can be encrypted with a symmetric key, and access control lists can be created that specify the IP addresses of client machines that will be provided with the NTP service (to prevent unauthorized use of internal time servers). See www.ntp.org for more information

And now a message from the Payment Card Industry

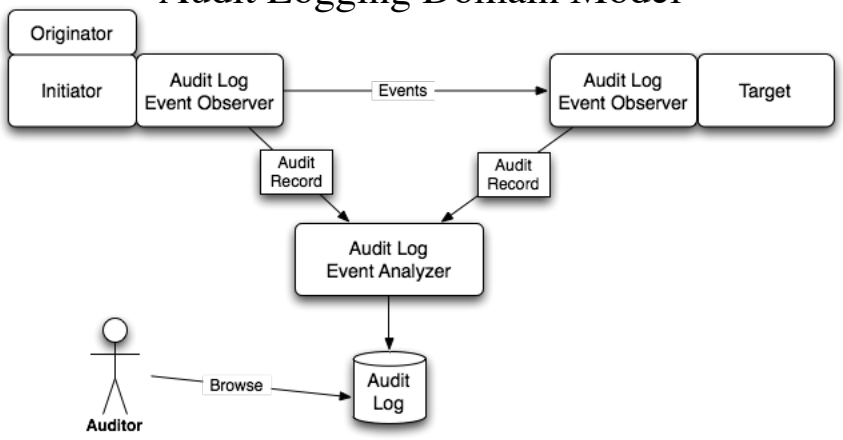
- 10.5 Secure audit trails so they cannot be altered.
  - 10.5.1 Limit viewing of audit trails to those with a job-related need.
  - 10.5.2 Protect audit trail files from unauthorized modifications.
  - 10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.
  - 10.5.4 Write logs for external-facing technologies onto a log server on the internal LAN.
  - 10.5.5 Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).

And now a message from the Payment Card Industry

- 10.6 Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion-detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS). Note: Log harvesting, parsing, and alerting tools may be used to meet compliance with Requirement 10.6
- 10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from back-up).
- More information at https://www.pcisecuritystandards.org

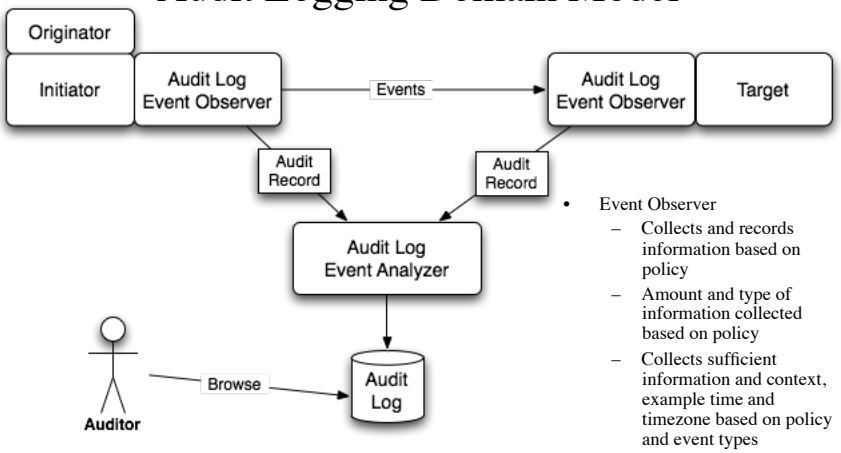
ARCTEC

Audit Logging Domain Model



ARCTEC

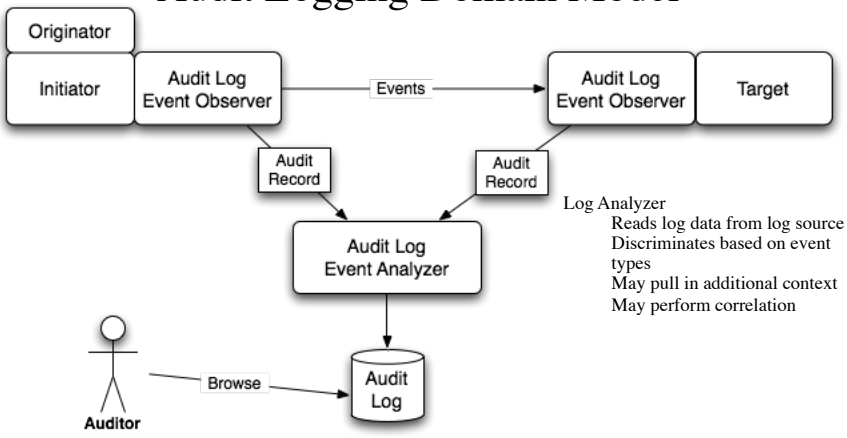
Audit Logging Domain Model



- Event Observer
  - Collects and records information based on policy
  - Amount and type of information collected based on policy
  - Collects sufficient information and context, example time and timezone based on policy and event types
  - Output is directed based on configuration
  - Often utilized at chokepoints

ARCTEC

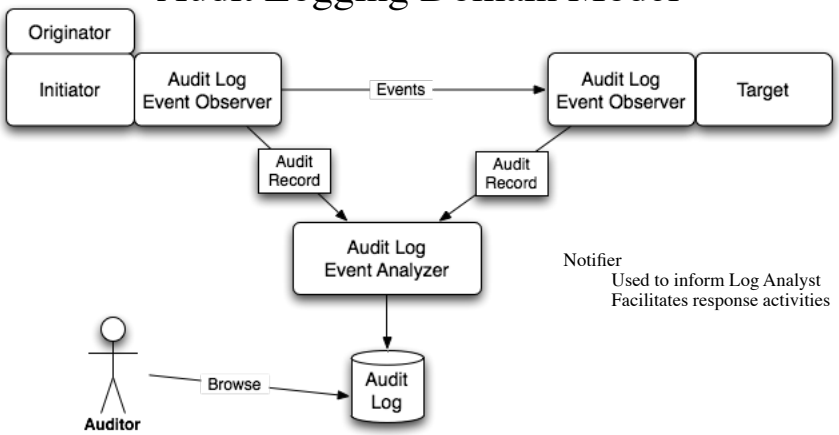
Audit Logging Domain Model



Log Analyzer
- Reads log data from log source
- Discriminates based on event types
- May pull in additional context
- May perform correlation

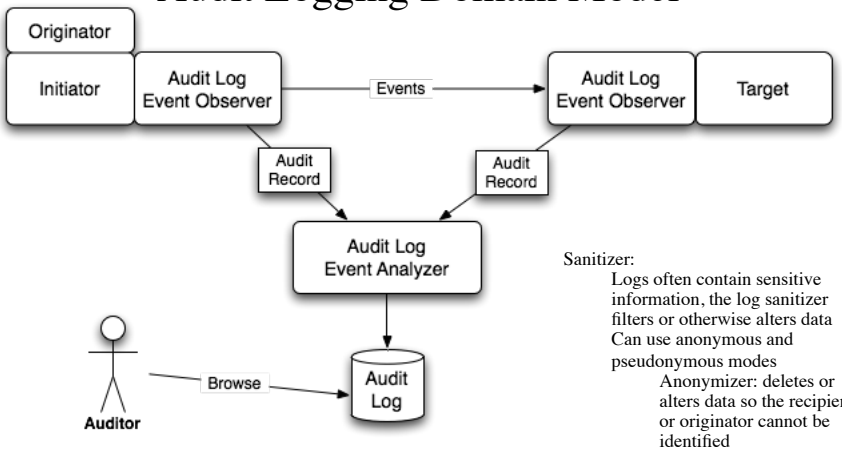
ARCTEC

Audit Logging Domain Model



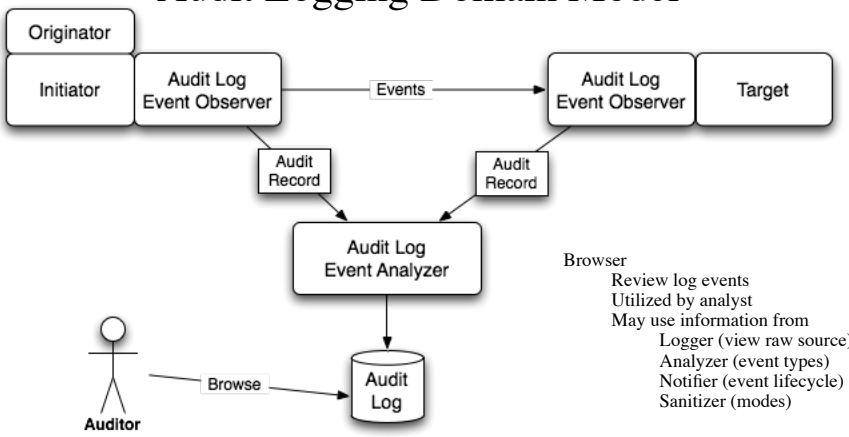
Notifier
- Used to inform Log Analyst
- Facilitates response activities

Audit Logging Domain Model



Sanitizer:
- Logs often contain sensitive information, the log sanitizer filters or otherwise alters data
- Can use anonymous and pseudonymous modes
  - Anonymizer: deletes or alters data so the recipient or originator cannot be identified
  - Pseudonymizer: deletes of alters data so the log administrator can perform correlation such as for demographic purposes

Audit Logging Domain Model



Browser
- Review log events
- Utilized by analyst
- May use information from
  - Logger (view raw source)
  - Analyzer (event types)
  - Notifier (event lifecycle)
  - Sanitizer (modes)

ARCTEC

Audit Logging Design Considerations

- Audit Log Event Record Format
- Publishing & Storing Audit Log data
- Protecting the Log Data repository
- Integrating the Audit Logger to your application
- Building an Audit Log Browser
- What Goes Wrong (and how to fix it)

ARCTEC

Audit Log Records

- Sources of Log Entry information
- Making the data useful
- What Events to Log
  - AAA (Authentication, Authorization, Access)
  - Change
  - "Badness"/ Threats
  - Resource exhausted, capacity exceeded, etc
  - Startups and shutdowns
- Securing the Audit Log events

ARCTEC

XDAS Audit Log Record Format

- Header
- Originator
- Initiator
- Target
- Source
- Event-specific data

ARCTEC

XDAS Audit Log Record Format

- Header
  - Record Length
  - XDAS Record Format Version
  - Event Time Stamp
  - Time Uncertainty Interval
  - Time Uncertainty Indicator
  - Time Source
  - Time Zone
  - Event Number (user-provided)
  - Event Outcome (user-provided).

ARCTEC

XDAS Audit Log Record Format

- Originator
  - Originator Location Name
  - Originator Location Address
  - Originator Service Type
  - Originator Authentication Authority (required)
  - Originator Principal Name (optional)
  - Originator Principal ID (required)

ARCTEC

XDAS Audit Log Record Format

- Initiator
  - Initiator Authentication Authority
  - Initiator Domain-Specific Name (optional)
  - Initiator Domain-Specific ID

XDAS Audit Log Record Format

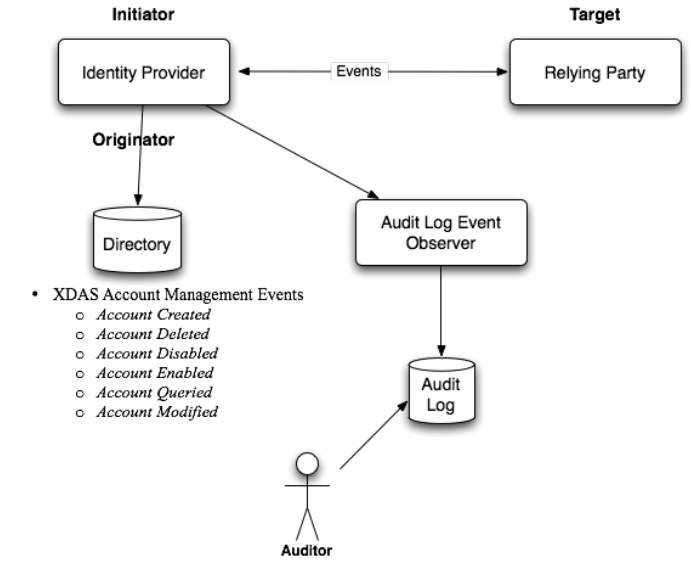
- Target
  - Target Location Name
  - Target Location Address
  - Target Service Type
  - Target Authentication Authority
  - Target Principal Name (optional)
  - Target Principal ID

XDAS Audit Log Record Format

- Source
  - Source Information String
- Event-specific data
  - Event-Specific Data Information String

XDAS Event Types

- Account Management Events
  - Create Account
  - Delete Account
  - Disable Account
  - Enable Account
  - Query Account
  - Modify Account



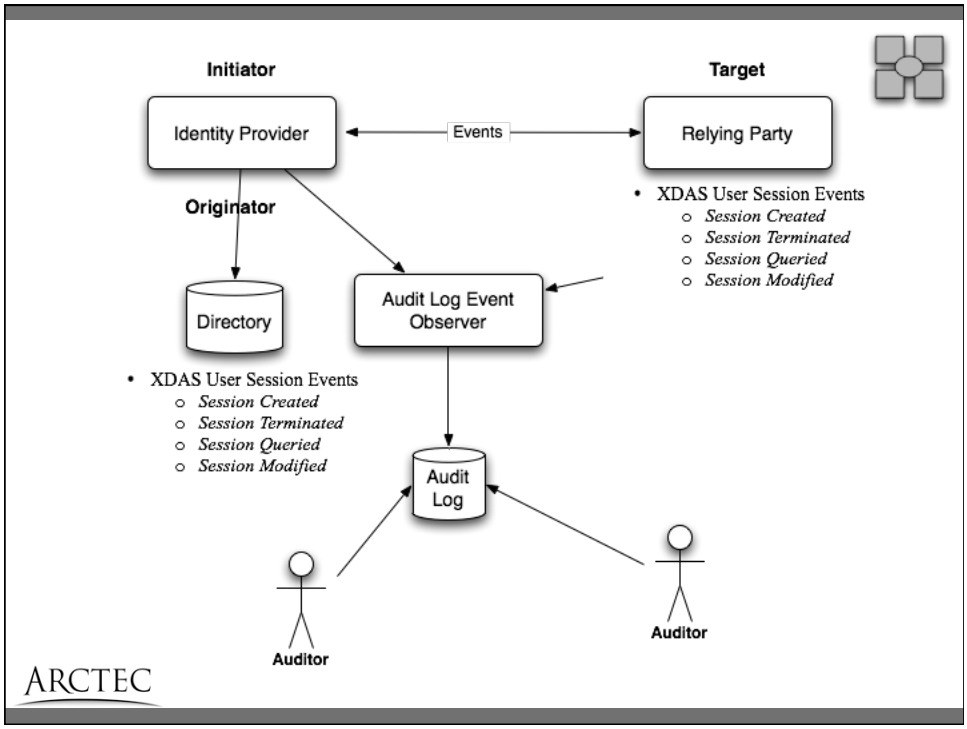
- XDAS Account Management Events
  - *Account Created*
  - *Account Deleted*
  - *Account Disabled*
  - *Account Enabled*
  - *Account Queried*
  - *Account Modified*

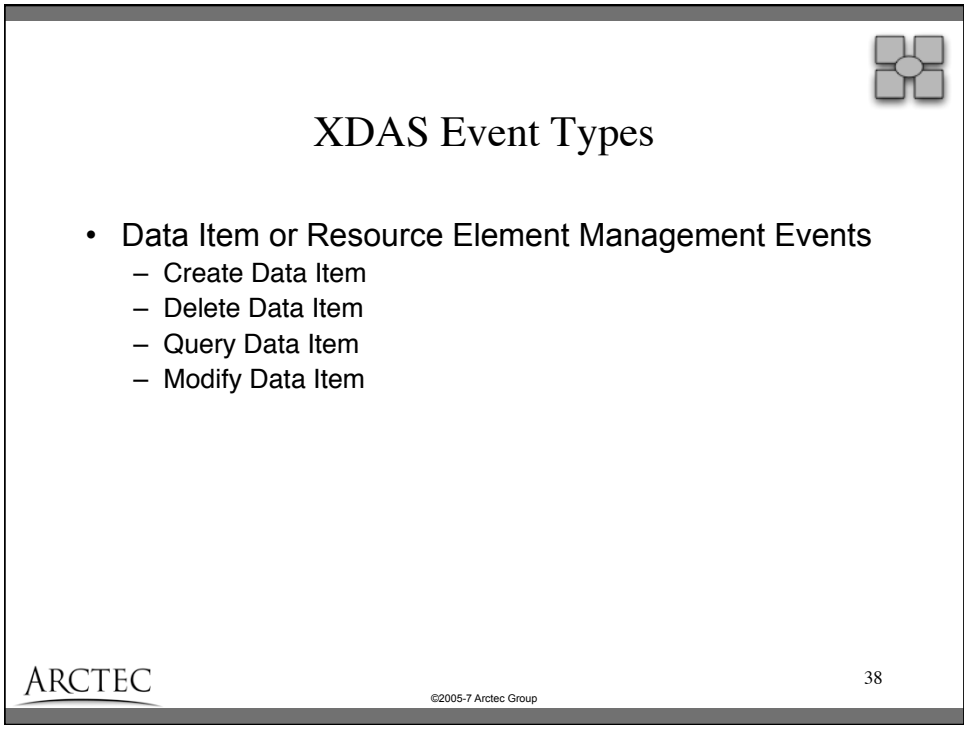
ARCTEC

XDAS Event Types

- User Session Events
  - Create Session
  - Terminate Session
  - Query Session
  - Modify Session

ARCTEC


Initiator
Target
Identity Provider
Events
Relying Party
Originator
• XDAS User Session Events
o Session Created
o Session Terminated
o Session Queried
o Session Modified
Directory
Audit Log Event Observer
• XDAS User Session Events
o Session Created
o Session Terminated
o Session Queried
o Session Modified
Audit Log
Auditor
Auditor
ARCTEC


XDAS Event Types
• Data Item or Resource Element Management Events
– Create Data Item
– Delete Data Item
– Query Data Item
– Modify Data Item
ARCTEC
38
©2005-7 Arctec Group

XDAS Event Types

- Service or Application Management Events
  - Install Service
  - Remove Service
  - Query Service Config
  - Modify Service Config
  - Disable Service
  - Enable Service

ARCTEC

XDAS Event Types

- Service or Application Utilization Events
  - Invoke Service
  - Terminate Service
  - Query Process Context
  - Modify Process Context

ARCTEC

XDAS Event Types

- Peer Association Management Events
  - Create Peer Association
  - Terminate Peer Association
  - Query Association Context
  - Modify Association Context
  - Receive Data via Association
  - Send Data via Association

ARCTEC

XDAS Event Types

- Data Item or Resource Element Content Access Events
  - Create Data Item Association
  - Terminate Data Item Association
  - Query Data Item Association
  - Modify Data Item Association
  - Query Data Item Contents
  - Modify Data Item Contents

ARCTEC

XDAS Event Types

- Exceptional Events
  - Start System
  - Shutdown System
  - Resource Exhaustion
  - Resource Corrupted
  - Backup Data Store
  - Recover Data Store

ARCTEC

XDAS Event Types

- Audit Service Management Events
  - Audit Subsystem Config
  - Audit Subsystem Diskspace Full
  - Audit Subsystem Diskspace Corrupt

ARCTEC

Publishing & Storing Audit Log data

- Logging Subsystem architecture
- Logging to database
- Logging to file system
- Building an Audit Logger API

ARCTEC

Protecting the Log Data repository

- Tamper proof logs
- Authentication
- Through the looking glass - Logging access to the log data repository
- Encrypting Log Data
- Maintenance issues - key escrow

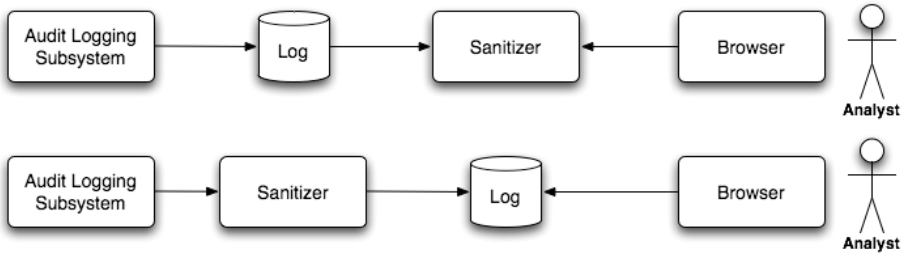
ARCTEC

Building an Audit Log Browser

- Log browser design issues
- Log browser metadata
- Sorting audit log events
- Common report types

ARCTEC

Sanitizer Placement



ARCTEC

What Goes Wrong (and how to fix it)

- Sensitive Data in Logs
  - Debug logging turned on in production
  - Sensitive personal, financial or PII written to logs
- Logging System Unavailable
- Encoding Issues
- Handling Malicious data in logs
- Log Tampering Revisited
- Storage Issues
- Delayed Events
- Sequence Attacks

ARCTEC

Audit Logging Checklist

Concern	Originator	Initiator	Target
Event Observer			
Event Publisher			
Auditable Events			
Audit Record Format			

ARCTEC

- References & Resources
  - "Build Visibility In", Richard Bejtlich, http://taosecurity.blogspot.com/2009/08/build-visibility-in.html
  - App Sensor at OWASP ESAPI
  - CEE (Arcsight/Mitre)
  - XDAS (Open Group)
  - "How to Do Application Logging Right" by Anton Chuvakin & Gunnar Peterson http://arctecgroup.net/pdf/howtoapplogging.pdf

- Email: gunnar@arctecgroup.net

ARCTEC