The Open Group Security Forum

X/Open Distributed Audit Standard

David Corlette
GRC Solution Architect
DCorlette@novell.com

A New Event Standard

- This session will discuss the ongoing revision of the XDAS event standard. It is our hope that this standard will become widespread in the industry.

- Why Do We Care?
- History
- The New Standard
- Integration Efforts

Why Do We Care?

Why Do I Care?

The Developer Perspective

- As a SIEM developer, I develop custom parsing for proprietary log/event formats every day
- If I am writing code, it would be nice to have a standard so I don't have to (re-)invent the wheel – this is boring and does not provide value
- Libraries that enforced the standard would be great so I could know I was doing the Right Thing (for example, a log4j appender)
- Even better would be standard libraries that provided security functions (like authentication) and already had logging built in!

Ouch!

```
Jan 16 14:30:47 130.57.171.1 %ASA-6-605005: Login permitted from 164.99.17.109/42258 to
management:164.99.17.6/https for user "dcorlette"

Apr 10 17:53:55 172.16.2.27 Message forwarded from ppaix: dtlogin: root logged in from
(172.16.7.15:0)

I="00031550" A="0003" N="9A54ADBE" Q="3" O="DirXML\\Login\Login_Success" L="7" G="00000000"
R="0.0.0.0" C="2008-06-18 07:41:23" B="ablake" H="0" U="10.0.0.2" V="0" F="Login success" 1="0"
2="0" 3="8" M="0" E=" " D=" "

I="002E000A" A="002E" N="49678A9D" Q="101" O="Novell Access Manager\nidp" L="7" G="00000000"
R="151.155.165.210" C="2009-01-09 17:53:20" H="0" U="cn=idp1user1,o=novell" V="0" S="Local"
F="name/password/uri" 1="0" 2="0" 3="0" M="0" E=" D=" "

|S47||SecurityAudit|100|AU1|Security Audit: Logon Event|0000007881|0|255|Fri Jan 23 00:00:00
MST 2009||0000100010|40|Security|Logon Successful (Type=B)|0000000170|2|C|C|C|101||C|033||Thu
Jan 01 16:02:06 MST
1970|Logon||AU1|B&0|0000000012||testlab_S47_00||AU1|||SAP_CCMS_testlab_S47_00|0006660452|Fri
Jan 23 00:00:00 MST 2009|SAP-SYSLOG|SecurityAudit|Thu Jan 01 16:02:06 MST
1970|S47|ADMIN|192.168.34.22
thiseventtgYear2007tgMonth06tgDay04tgHour03tgMinute53tgSecond42RN1060C2CNNACTIVEEC540EI540ET4LS
ecuritySNSecurityTAudit SuccessUNT AUTHORITY\SYSTEMCSLogon/LogoffMSuccessful Network
LogonXMSuccessful Network Logon:     User Name: NACTIVE$     Domain:  MYVM     Logon ID:
(0x0,0x1D96F)     Logon Type: 3     Logon Process: Kerberos     Authentication Package:
Kerberos     Workstation Name:      Logon GUID: {736df012-16f1-181b-90db-5358321c8ac9}
Caller User Name: -     Caller Domain: -     Caller Logon ID: -     Caller Process ID: -
Transited Services: -     Source Network Address: 192.168.175.204     Source Port: 1359
ISNACTIVE$MYVM(0x0,0x1D96F)3KerberosKerberos{736df012-16f1-181b-90db-5358321c8ac9}-----
192.168.175.2041359
```

Why Does My Company Care?

The Vendor Perspective

- Novell has gone through perhaps three different logging “standards” in the last 15 years
- Converting existing applications to a new standard is expensive
- Think about the value you can sell to your customers with a common event format for all your applications
  - Simple visibility into what your products are doing
  - Cross-product incident analysis in real time
  - Cross-product reporting
  - Easy integration with any existing enterprise SIEM/reporting tools

Why Does Everybody Else Care?
The Customer Perspective

- A standard provides additional value
  - Simple visibility into what your software is doing
  - Cross-product incident analysis in real time
  - Cross-product reporting
- Easy integration with any existing enterprise SIEM/reporting tools
- Enhanced security comes with better visibility
- Easy preparation for compliance audits
- Companies spent $650m on SIEM tools last year!

History

History of XDAS

- The Open Group created the X/Open Distributed Audit Standard in 1997 – a bit ahead of its time
- Some very good ideas
  - Standardized record format and data model
  - Event classification (taxonomy)
- Some downsides
  - Somewhat anachronistic (in retrospect) encoding
  - Heavy API dependency
  - Very heavily influenced by *nix

The OpenXDAS Library

- Opensource effort to implement the XDAS standard
- Publicly available for several years; latest release was last May (project is still active)
- Learned a lot about the difficulties in implementing the proposed API
- Not widely used; developers would have had to modify their logging code to support this exact API

:OpenXDAS:

Compliance Auditing for Everyone

An Update to XDAS

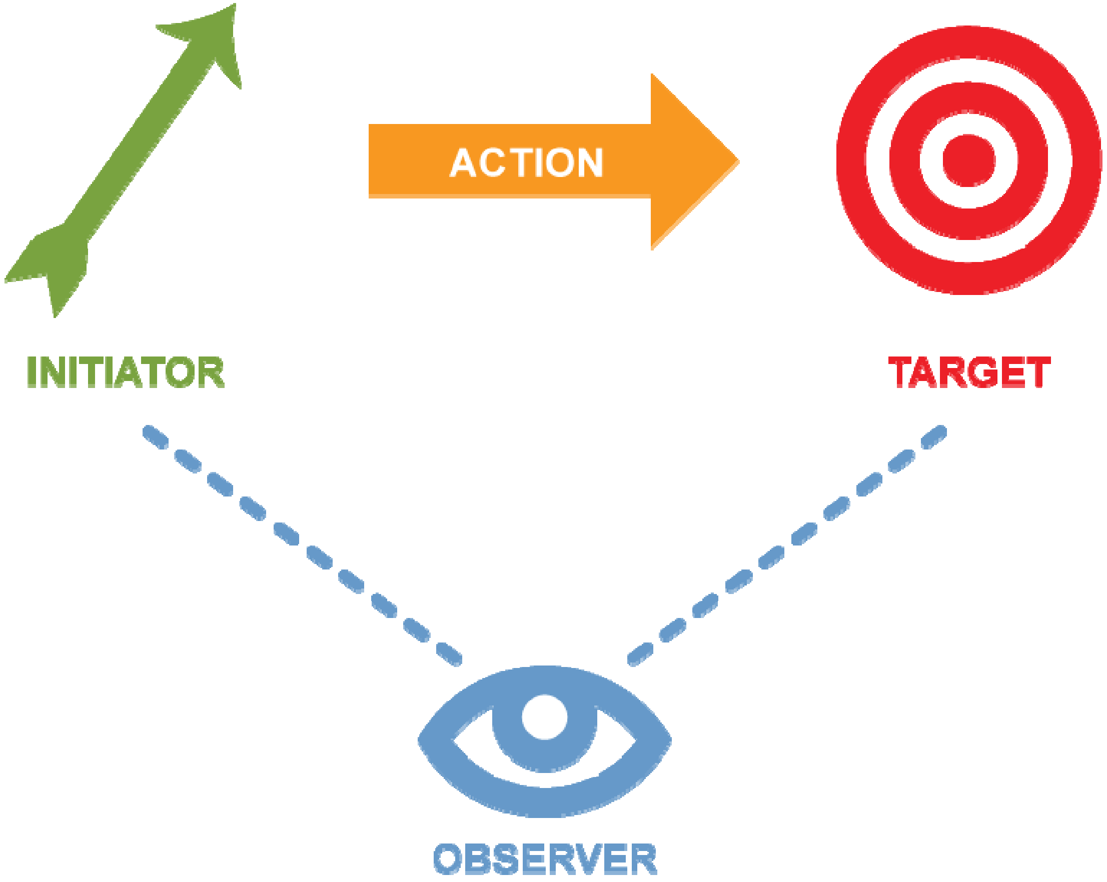
- Began working on a revision in May 2007
- Have developed a data model and basic concepts – are now working out the details
  - Eliminated API dependency
  - Format is flexible and based on standards (JSON, XML, delimited, etc) – these are just encodings
- Need as broad vendor and customer participation as possible
- Work has partly been slow due to outreach efforts (more on that later)

The New Standard

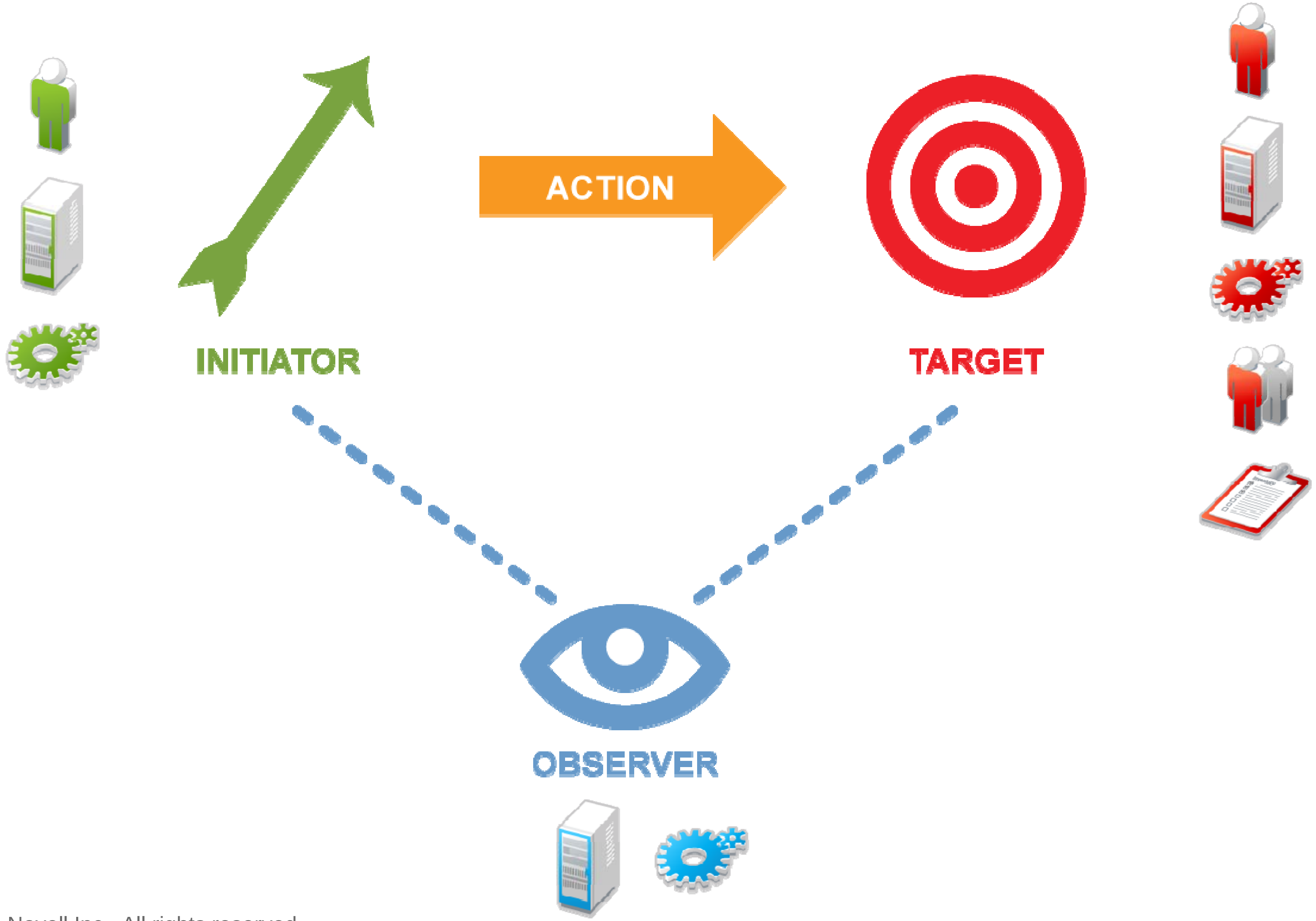
Challenges

- Too many things to express
  - Focus on interesting use cases
  - Constrained scope
- Conversion
  - Will be driven by customers (and SIEM vendors?)
  - In the meantime, can create converters (and charge for them!)
- Details
  - “login” or “auth” or...?
  - How to express time?
  - Event classification (taxonomy)

The XDAS Data Model



The XDAS Data Model



ACTION

INITIATOR

TARGET

OBSERVER

Domain Objects

- Account object:

Name	*String*	The source-specific account name, typically in human-readable form
ID	*String*	The source-specific account identifier, usually an opaque code used to reference the account internally
Domain	*Path*	The source-specific domain or namespace in which the account exists

Taxonomy

- Classify:
  - Type of event source
    - OS, IDS, DB, etc
      - Need to answer questions like “Who modified my firewalls' configuration?”
  - Type of activity
    - Auth, Read, Delete, etc
      - Need to answer questions like “Who logged in?”
  - Result of activity
    - Success, Failure, Denial
      - Need to answer questions like “Whose login attempts were denied?”
  - Specific target of activity
    - Account, File, Configuration
      - Need to know what the activity affected

Integration Efforts

Integration With CEE

- CEE has a broader scope – it also covers transport, specifically calls out best practices, and is attempting to cover non-security and compliance logs
- Members of the XDAS working group are also members of the CEE editorial board, and vice versa
- The idea is that XDAS will become the – or at least one of the – supported event formats that can be expressed in the CEE domain

Q&A