Understanding audit trails of heterogeneous applications without cost

23rd Enterprise Architecture Practitioners Conference, Toronto

Joël Winteregg – CEO NetGuardians SA, CISSP
winteregg@netguardians.ch

THE Open GROUP
Making standards work®

Agenda

- How does it work today ?
- Tomorrow's audit trails
- XDAS overview
- Xdas4j
- Demonstration
- How to convince a software company to use it ?
- Try it and support it

How does it work today ?

- Each IT vendor define its own audit trails
  - No uniform accountability mechanism
  - Hard to monitor IT controls
  - Hard to understand and track IT issues
- Expensive SIEM solutions
  - Focused on audit trails collection
  - Focused on audit trails understanding
  - Audit trails analysis is left behind

Today's audit trails

- Cisco Wireless Controler:

```
Cold Start-sysUpTimeInstance = 14:1:34:46.00  snmpTrapOID.0 = bsnDot11StationAssociate
bsnStationAPMacAddr.0 = 0:b:85:8f:5c:e0  bsnStationAPIfSlotId.0 = 0
bsnStationMacAddress.0 = 0:19:e3:6:ae:e9  bsnStationUserName.0 = user_x@netguardians.ch
```

- Microsoft DHCP

```
ADDHCP 02/07/09,15:57:04,Assign,10.192.68.96,HOSTX.mydomain.com,00:40:96:A9:50:38
```

- Nortel Switch

```
CPU5 [10/06/08 08:41:36] SSH INFO SSH: User Manager login /pty/sshd1. from 10.192.49.110
```

XDAS – Tomorrow's audit trails

- Standardized audit trails
  - Uniform format
  - Uniform meaning (taxonomy)

Leads To:

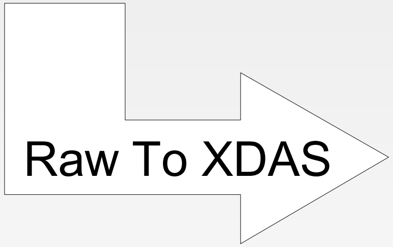
- IT visibility
  - Easily answers fundamental IT security questions
  - Enhance operations (troubleshooting, SLA monitoring, etc.)
- Machine readable trails

- Assumptions:
  - All vendors need to generate XDAS compliant trails

What does tomorrow look like...

- Microsoft DHCP

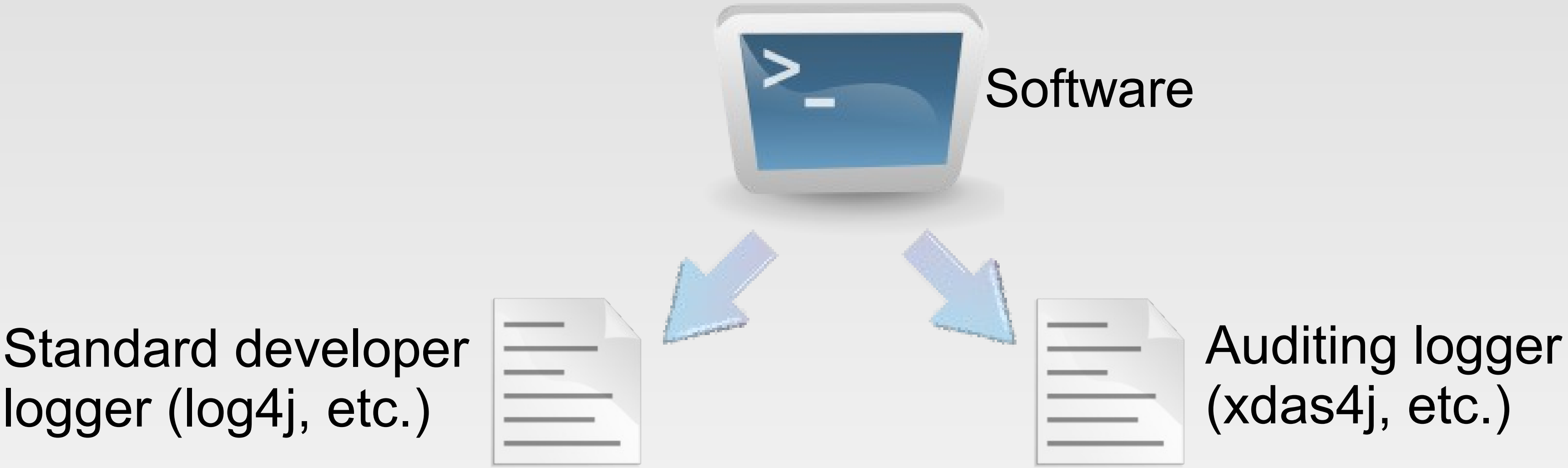
```
ADDHCP 02/07/09,15:57:04,Assign,10.192.68.96,
HOSTX.mydomain.com,00:40:96:A9:50:38
```



```
{
  "XDASVersion": "http://www.opengroup.org/xdas/2008",
  "Initiator": {
    "Host": {
      "Name": "HostX.mydomain.com"
      "Address": {
        "Mac": "00:40:96:A9:50:38"
      }
      "Address": {
        "ipv4": "10.192.68.96"
     }
    }
  },
  "Target": {
    "Host": {
      "Name": "ADDHCP"
    }
    "Service": {
      "Name": "DHCP",
      "Component" : "Microsoft Windows DHCP server"
    }
  },
  "Action": {
    "Time": "02/07/09 15:57:04",
    "Name": "Assigned IP Address",
    "actionTax": "Address Assigned",
    "outcomeTax": "Successful"
  },
  "Observer": {
    "Host": {
      "Name": "ADDHCP"
    }
    "Service": {
      "Name": "DHCP",
      "Component" : "Microsoft Windows DHCP server"
    }
  }
}
```

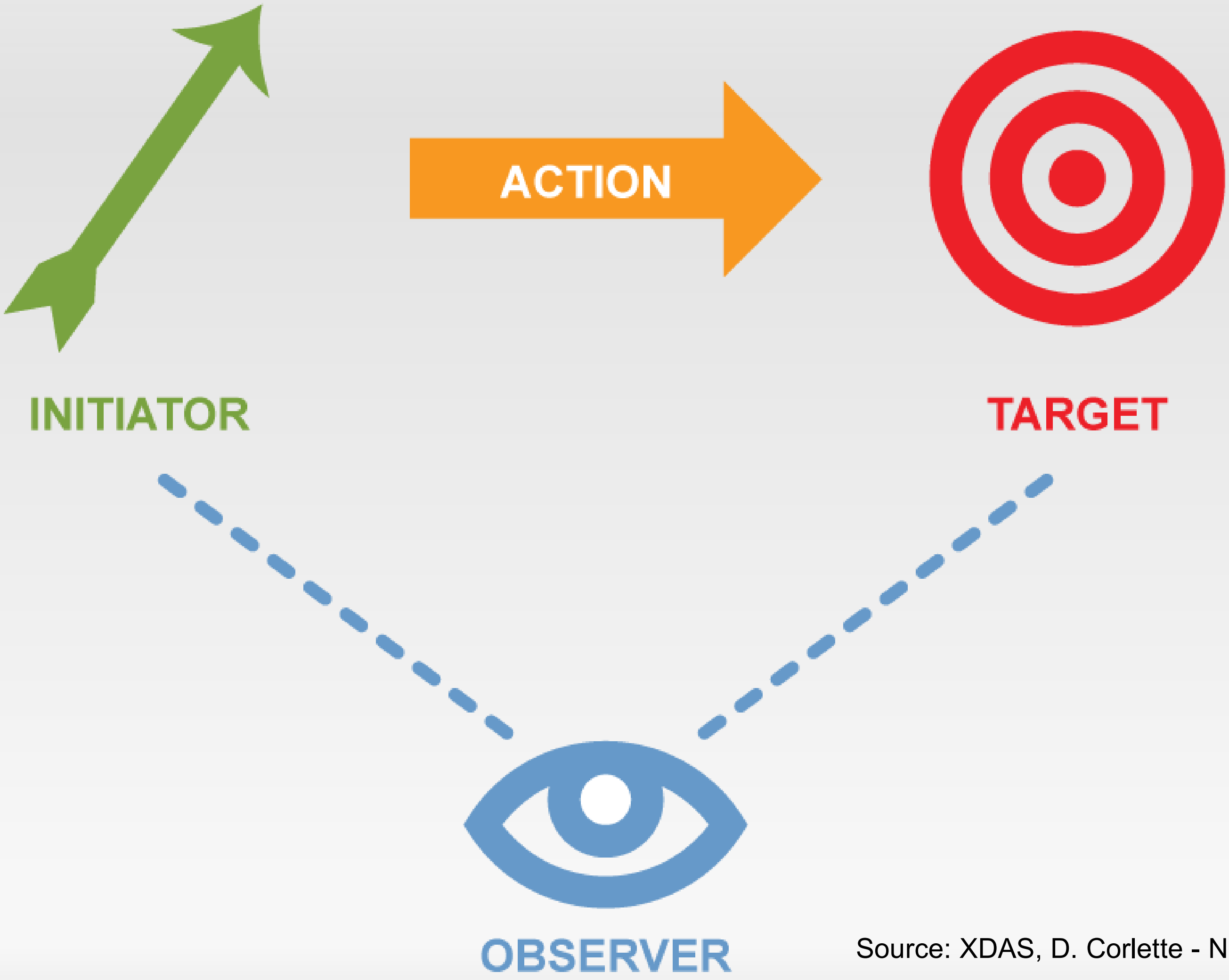
XDAS overview

- It is not a logging standard, it is an auditing standard !


Software
Standard developer logger (log4j, etc.)
Auditing logger (xdas4j, etc.)

"*Syslog is for logging, XDAS is for auditing*" - John Calcote, Novell

XDAS audit trails

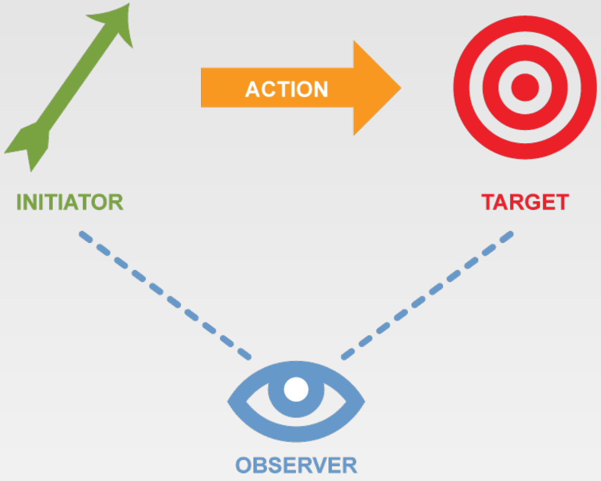


Source: XDAS, D. Corlette - Novell

XDAS audit trails

```
Action: {
    Time: "02/07/09 15:57:04",
    Name: "Assigned IP Address",
    actionTax: "Address Assigned",
    outcomeTax: "Successful"
}
```

```
Initiator: {
    Host: {
      Name: "HostX.mydomain.com"
      Address: {
        Mac: "00:40:96:A9:50:38"
      }
      Address: {
        ipv4: "10.192.68.96"
      }
    }
  }
```



```
Target: {
   Host: {
     Name: "ADDHCP"
   }
   Service: {
     Name: "DHCP",
     Component : "Microsoft
                  Windows DHCP
                  server"
   }
 }
```

```
Observer: {
   Host: {
     Name: "ADDHCP"
   }
   Service: {
     Name: "DHCP",
     Component : "Microsoft Windows DHCP server"
   }
 }
```

Xdas4j - http://xdas4j.codehaus.org

- OpenSource and business friendly Java library (LGPL)
- Built on top of *log4j* logging framework
  - Many available appenders (Syslog, SMTP, JMS, etc.)
  - Well known logging architecture
- Pragmatic Approach to develop XDAS standard
  - As AGILE software development (Use case and test driven approach)
  - XDAS proposal available as a Java logging library

Demonstration

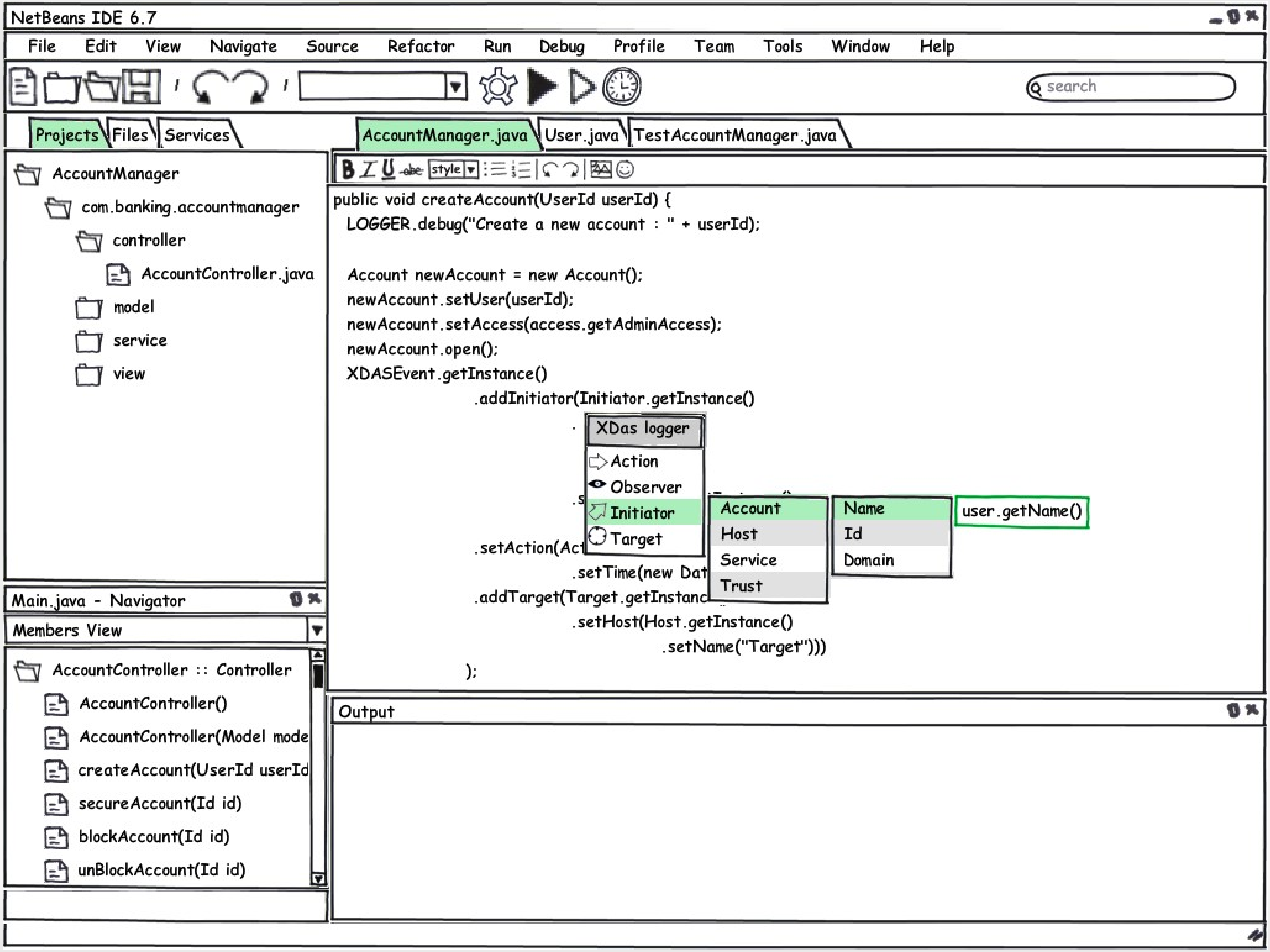
- Available at:

  http://xdas4j.codehaus.org/demo/

How to convince a software company to use it ?

- Business side
  - Enhance relationships between users (IT operations) and software vendors
  - Compatible with future XDAS trails analysis solutions
- Developer side
  - Uniform conventions
    - A single audit trail data model to know
  - Easy to use
    - Graphical auto-completion using NetBeans IDE plugin
    - Maven project

How to convince a software company to use it ?



```
public void createAccount(UserId userId) {
  LOGGER.debug("Create a new account : " + userId);

  Account newAccount = new Account();
  newAccount.setUser(userId);
  newAccount.setAccess(access.getAdminAccess);
  newAccount.open();
  XDASEvent.getInstance()
            .addInitiator(Initiator.getInstance()
                     .
                     .s
            .setAction(Act
                     .setTime(new Dat
            .addTarget(Target.getInstanc
                     .setHost(Host.getInstance()
                            .setName("Target")))
            );
```

Try it and support it

- Join XDAS working group
  - http://www.opengroup.org/projects/security/xdas
- Join xdas4j project
  - http://xdas4j.codehaus.org/
- Provide feedback
  - winteregg@netguardians.ch

Thank you