XDAS Audit & Logging standard for servicing today's regulatory/compliance requirements

3rd Security Practitioners Conference, Toronto

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

THE Open GROUP
Making standards work®

Agenda

- Today's Compliance Requirements
- IT Security Impact
- Today's Accountability
- XDAS – Tomorrow's Accountability
- XDAS History
- XDAS Overview
- Conclusion

Today's requirements

- Best Practices (ISO 17799)
- ISO 27001
- Sarbanes-Oxley Act (SOX) – 2002
  - It is primarily focused on the accuracy of financial reporting data
- Basel II
  - Banking industry
- Payment Card Industry Data Security Standard (PCI DSS)

Why Board Members care about it?

- If the CEO says it's ”adequate” and he is willing to sign his life away, that is all that is required!
- SOX
  - Section 302: Requires executives to certify the accuracy of corporate financial reports
  - Section 404: Requires executives and auditors to confirm the effectiveness of internal controls for financial reporting

IT Security Impact

- Confidentiality
- Integrity
- Availability

How to certify its accuracy ?

How to confirm its effectiveness ?

Accountability

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 accountability

- 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 Accountability

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

Leads To:

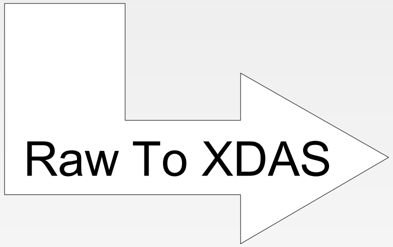
- IT visibility
  - Easily answers fundamental IT security questions
  - Enhance operations (troubleshooting, SLA monitoring, etc.)
- Machine readable trails

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

What does tomorrow look like...

- 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
```

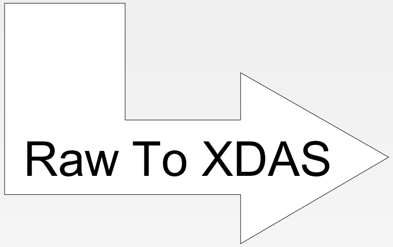


```
{
  "XDASVersion": "http://www.opengroup.org/xdas/2008",
  "Initiator": {
    "Account": {
      "Name": "user_x@netguardians.ch"
    },
    "Host": {
      "Address": {
        "Mac": "0:19:e3:6:ae:e9"
      }
    }
  },
  "Target": {
    "Host": {
      "Address": {
        "Mac": "0:b:85:8f:5c:e0"
      }
    }
  },
  "Action": {
    "Time": "14:1:34:46.00",
    "Name": "Station Association to AP",
    "Message": "bsnDot11StationAssociate",
    "actionTax": "Host Association",
    "outcomeTax": "Successful"
  },
  "Observer": {
    "Service": {
      "Name": "Wireless Access Control",
      "Component" : "Wireless Controler"
    }
  }
}
```

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
```



Raw To XDAS

```
{
  "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 history

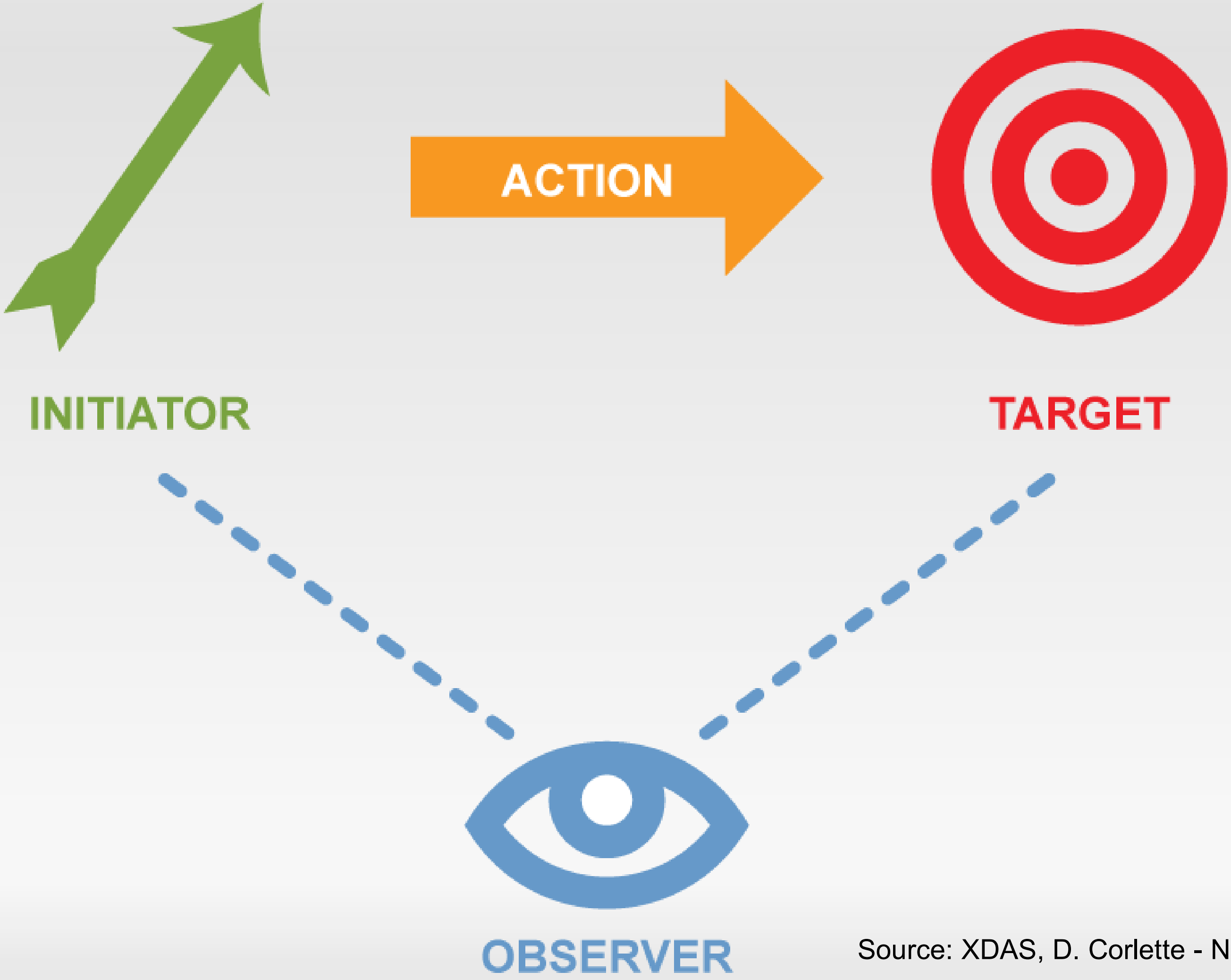
- XDAS version 1
  - Defined in 1998
  - Wide and complex scope (from event generation to event filtering)
  - Exhaustive API
  - Data Model focused on Operating System needs
- XDAS version 2
  - In progress (2009)
  - Focused on audit event format and taxonomy
  - Simple and extensible Data Model
  - Compatible with upcoming standards (CEE)

XDAS overview

- It is not a logging standard, it is an auditing standard !
- Audit trails record format and taxonomy
  - High-level data model
  - Common portable event record format
  - Extensible taxonomy of universally applicable generic security events
- Pragmatic Approach
  - As AGILE software development (Use case and test driven)
  - XDAS proposal available as a Java logging library http://xdas4j.codehaus.org

XDAS overview

- Data Model

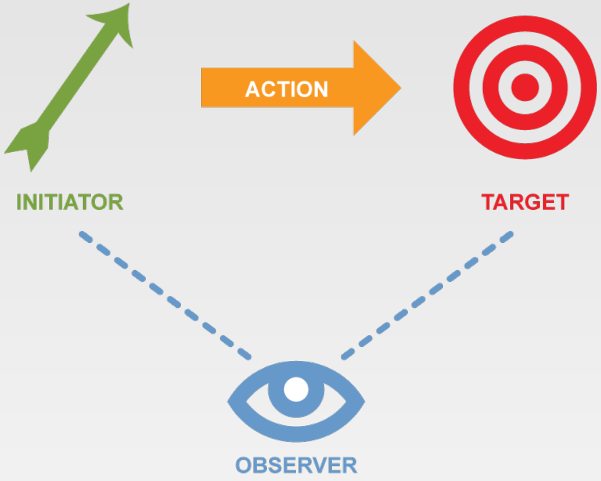


Source: XDAS, D. Corlette - Novell

XDAS overview

```
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"
      }
    }
  }
```

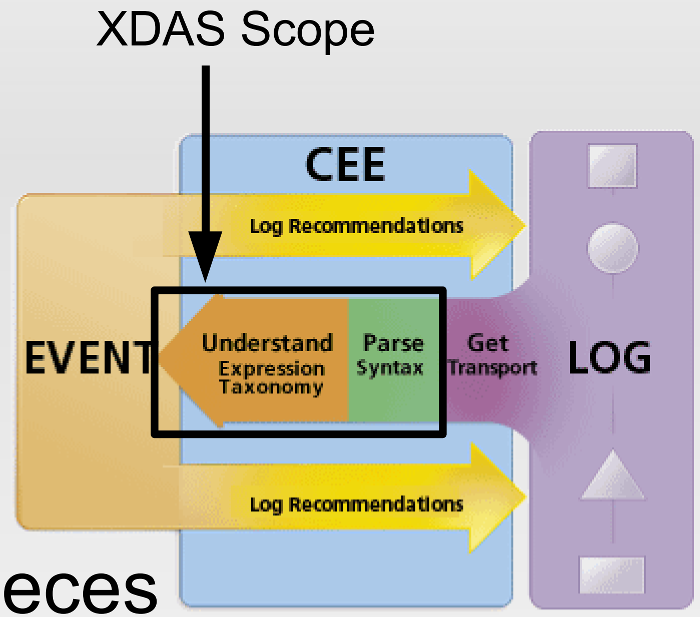


```
Target: {
   Host: {
     Name: "ADDHCP"
   }
   Service: {
     Name: "DHCP",
     Component : "Microsoft
                  Windows DHCP
                  server"
   }
 }
```

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

Other standardization efforts

- CEE (on going effort – MITRE)
  - Broader approach
    - Event generation recommendations
    - Event transportation
  - Many XDAS members are involved in CEE
  - XDAS could be one of the CEE pieces



Source: CEE, http://cee.mitre.org

- IDMEF (RFC 4765)
  - Same data model concepts
  - Focused on Intrusion Detection Messages
  - No taxonomy

Conclusion

- Compliance has a strong impact on IT operations
  - There are a lot of policies and requirements related to audit event generation

  But...

  - There is no uniform way to manage and understand audit trails

- Support on going initiatives !
  - http://www.opengroup.org/projects/security/xdas
  - http://xdas4j.codehaus.org/

Thank you