Audit Log Normalization

Steve Grubb
Red Hat

Audit Log Normalizer

Audit Logs are ugly

Audit Log Normalizer

What if the events could be easier to understand?

Common Criteria

- Time & Date
- Who did it
- What did they do
- What was being acted upon
- What was the results

On 1-node at 2-time 3-subj 4-acting-as 5-results 6-action 7-what 8-using

Which maps to:
1) node
2) time
3) auid, failed logins=remote system
4) uid (only when uid != auid)
5) res - successfully / unsuccessfully
6) op, syscall, type, key
7) path, address, account, policy, rules,
8) exe, comm

```
At 13:48:17 sgrubb, acting as root,
successfully deleted /root/.xauthrAfmkX
using /usr/bin/xauth
```

```
type=PROCTITLE msg=audit(01/28/2017 13:48:17.238:2619) :
proctitle=/usr/bin/xauth -f /root/.xauthrAfmkX nmerge -

type=PATH msg=audit(01/28/2017 13:48:17.238:2619) : item=1
name=/root/.xauthrAfmkX inode=3932578 dev=08:05 mode=file,600 ouid=root
ogid=sgrubb rdev=00:00 obj=system_u:object_r:xauth_home_t:s0
nametype=DELETE

type=PATH msg=audit(01/28/2017 13:48:17.238:2619) : item=0 name=/root/
inode=3932161 dev=08:05 mode=dir,550 ouid=root ogid=root rdev=00:00
obj=system_u:object_r:admin_home_t:s0 nametype=PARENT

type=CWD msg=audit(01/28/2017 13:48:17.238:2619) : cwd=/home/sgrubb

type=SYSCALL msg=audit(01/28/2017 13:48:17.238:2619) : arch=x86_64
syscall=unlink success=yes exit=0 a0=0x556bb2ed7010 a1=0x0
a2=0x7fa22ffa8b78 a3=0x556bb2ed84a0 items=2 ppid=2274 pid=2278
auid=sgrubb uid=root gid=root euid=root suid=root fsuid=root egid=root
sgid=root fsgid=root tty=pts1 ses=3 comm=xauth exe=/usr/bin/xauth
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=delete
```

```
type=PROCTITLE msg=audit(01/28/2017 13:48:17.238:2619) :
proctitle=/usr/bin/xauth -f /root/.xauthrAfmkX nmerge -

type=PATH msg=audit(01/28/2017 13:48:17.238:2619) : item=1
name=/root/.xauthrAfmkX inode=3932578 dev=08:05 mode=file,600 ouid=root
ogid=sgrubb rdev=00:00 obj=system_u:object_r:xauth_home_t:s0
nametype=DELETE

type=PATH msg=audit(01/28/2017 13:48:17.238:2619) : item=0 name=/root/
inode=3932161 dev=08:05 mode=dir,550 ouid=root ogid=root rdev=00:00
obj=system_u:object_r:admin_home_t:s0 nametype=PARENT

type=CWD msg=audit(01/28/2017 13:48:17.238:2619) : cwd=/home/sgrubb

type=SYSCALL msg=audit(01/28/2017 13:48:17.238:2619) : arch=x86_64
syscall=unlink success=yes exit=0 a0=0x556bb2ed7010 a1=0x0
a2=0x7fa22fa8b78 a3=0x556bb2ed84a0 items=2 ppid=2274 pid=2278
auid=sgrubb uid=root gid=root euid=root suid=root fsuid=root egid=root
sgid=root fsgid=root tty=pts1 ses=3 comm=xauth exe=/usr/bin/xauth
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=delete
```

```
type=PROCTITLE msg=audit(01/28/2017 13:48:17.238:2619) :
proctitle=/usr/bin/xauth -f /root/.xauthrAfmkX nmerge -

type=PATH msg=audit(01/28/2017 13:48:17.238:2619) : item=1
name=/root/.xauthrAfmkX inode=3932578 dev=08:05 mode=file,600 ouid=root
ogid=sgrubb rdev=00:00 obj=system_u:object_r:xauth_home_t:s0
nametype=DELETE

type=PATH msg=audit(01/28/2017 13:48:17.238:2619) : item=0 name=/root/
inode=3932161 dev=08:05 mode=dir,550 ouid=root ogid=root rdev=00:00
obj=system_u:object_r:admin_home_t:s0 nametype=PARENT

type=CWD msg=audit(01/28/2017 13:48:17.238:2619) : cwd=/home/sgrubb

type=SYSCALL msg=audit(01/28/2017 13:48:17.238:2619) : arch=x86_64
syscall=unlink success=yes exit=0 a0=0x556bb2ed7010 a1=0x0
a2=0x7fa22ffa8b78 a3=0x556bb2ed84a0 items=2 ppid=2274 pid=2278
auid=sgrubb uid=root gid=root euid=root suid=root fsuid=root egid=root
sgid=root fsgid=root tty=pts1 ses=3 comm=xauth exe=/usr/bin/xauth
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=delete
```

```
type=PROCTITLE msg=audit(01/28/2017 13:48:17.238:2619) :
proctitle=/usr/bin/xauth -f /root/.xauthrAfmkX nmerge -

type=PATH msg=audit(01/28/2017 13:48:17.238:2619) : item=1
name=/root/.xauthrAfmkX inode=3932578 dev=08:05 mode=file,600 ouid=root
ogid=sgrubb rdev=00:00 obj=system_u:object_r:xauth_home_t:s0
nametype=DELETE

type=PATH msg=audit(01/28/2017 13:48:17.238:2619) : item=0 name=/root/
inode=3932161 dev=08:05 mode=dir,550 ouid=root ogid=root rdev=00:00
obj=system_u:object_r:admin_home_t:s0 nametype=PARENT

type=CWD msg=audit(01/28/2017 13:48:17.238:2619) : cwd=/home/sgrubb

type=SYSCALL msg=audit(01/28/2017 13:48:17.238:2619) : arch=x86_64
syscall=unlink success=yes exit=0 a0=0x556bb2ed7010 a1=0x0
a2=0x7fa22ffa8b78 a3=0x556bb2ed84a0 items=2 ppid=2274 pid=2278
auid=sgrubb uid=root gid=root euid=root suid=root fsuid=root egid=root
sgid=root fsgid=root tty=pts1 ses=3 comm=xauth exe=/usr/bin/xauth
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=delete
```

```
type=PROCTITLE msg=audit(01/28/2017 13:48:17.238:2619) :
proctitle=/usr/bin/xauth -f /root/.xauthrAfmkX nmerge -

type=PATH msg=audit(01/28/2017 13:48:17.238:2619) : item=1
name=/root/.xauthrAfmkX inode=3932578 dev=08:05 mode=file,600 ouid=root
ogid=sgrubb rdev=00:00 obj=system_u:object_r:xauth_home_t:s0
nametype=DELETE

type=PATH msg=audit(01/28/2017 13:48:17.238:2619) : item=0 name=/root/
inode=3932161 dev=08:05 mode=dir,550 ouid=root ogid=root rdev=00:00
obj=system_u:object_r:admin_home_t:s0 nametype=PARENT

type=CWD msg=audit(01/28/2017 13:48:17.238:2619) : cwd=/home/sgrubb

type=SYSCALL msg=audit(01/28/2017 13:48:17.238:2619) : arch=x86_64
syscall=unlink success=yes exit=0 a0=0x556bb2ed7010 a1=0x0
a2=0x7fa22ffa8b78 a3=0x556bb2ed84a0 items=2 ppid=2274 pid=2278
auid=sgrubb uid=root gid=root euid=root suid=root fsuid=root egid=root
sgid=root fsgid=root tty=pts1 ses=3 comm=xauth exe=/usr/bin/xauth
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=delete
```

```
type=PROCTITLE msg=audit(01/28/2017 13:48:17.238:2619) :
proctitle=/usr/bin/xauth -f /root/.xauthrAfmkX nmerge -

type=PATH msg=audit(01/28/2017 13:48:17.238:2619) : item=1
name=/root/.xauthrAfmkX inode=3932578 dev=08:05 mode=file,600 ouid=root
ogid=sgrubb rdev=00:00 obj=system_u:object_r:xauth_home_t:s0
nametype=DELETE

type=PATH msg=audit(01/28/2017 13:48:17.238:2619) : item=0 name=/root/
inode=3932161 dev=08:05 mode=dir,550 ouid=root ogid=root rdev=00:00
obj=system_u:object_r:admin_home_t:s0 nametype=PARENT

type=CWD msg=audit(01/28/2017 13:48:17.238:2619) : cwd=/home/sgrubb

type=SYSCALL msg=audit(01/28/2017 13:48:17.238:2619) : arch=x86_64
syscall=unlink success=yes exit=0 a0=0x556bb2ed7010 a1=0x0
a2=0x7fa22ffa8b78 a3=0x556bb2ed84a0 items=2 ppid=2274 pid=2278
auid=sgrubb uid=root gid=root euid=root suid=root fsuid=root egid=root
sgid=root fsgid=root tty=pts1 ses=3 comm=xauth exe=/usr/bin/xauth
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=delete
```

Normalized Log View

- Ausearch output in CSV format
  - Analyzed by ooffice / Excel
  - Pull into database
  - R scripts
    - Charts
    - Models
    - Machine Learning

Normalized API

- Standardized access
  - Session, subject's primary identity, subject's secondary identity, object's primary identity, object's secondary identity, second object, results, key, SE Linux labels, time
- Metadata
  - Kind of event, kind of subject, kind of action being performed, kind of object

Audit Event Feeds

- Kernel
  - Promiscuous socket, coredumps, symlinks, netfilter, tty
- Trusted Programs
  - Pam
  - Login, sshd, gdm, kdm, vsftp, sudo, cronie
  - Shadow-utils, passwd
  - Semanage, systemd, libvirt, dbus, sssd, cups, hwclock, clevis
- Policy Engines
  - SE Linux, seccomp
- Integrity Apps
  - Aide, fapolicyd, usb_guard, IMA