SANS

The Most Trusted Source for Information Security Training, Certification, and Research

"The course is a very good introduction to a very complex topic. It balances the technical and theory extremely well."
-Andrew Mayhew, **Alcoa**

CYBER SECURITY TRAINING

Sydney 2019

Grace Hotel Sydney | 4-23 November

Protect Your Organisation Advance Your Career

12 hands-on, immersion-style courses taught by real-world practitioners

Courses offered in:

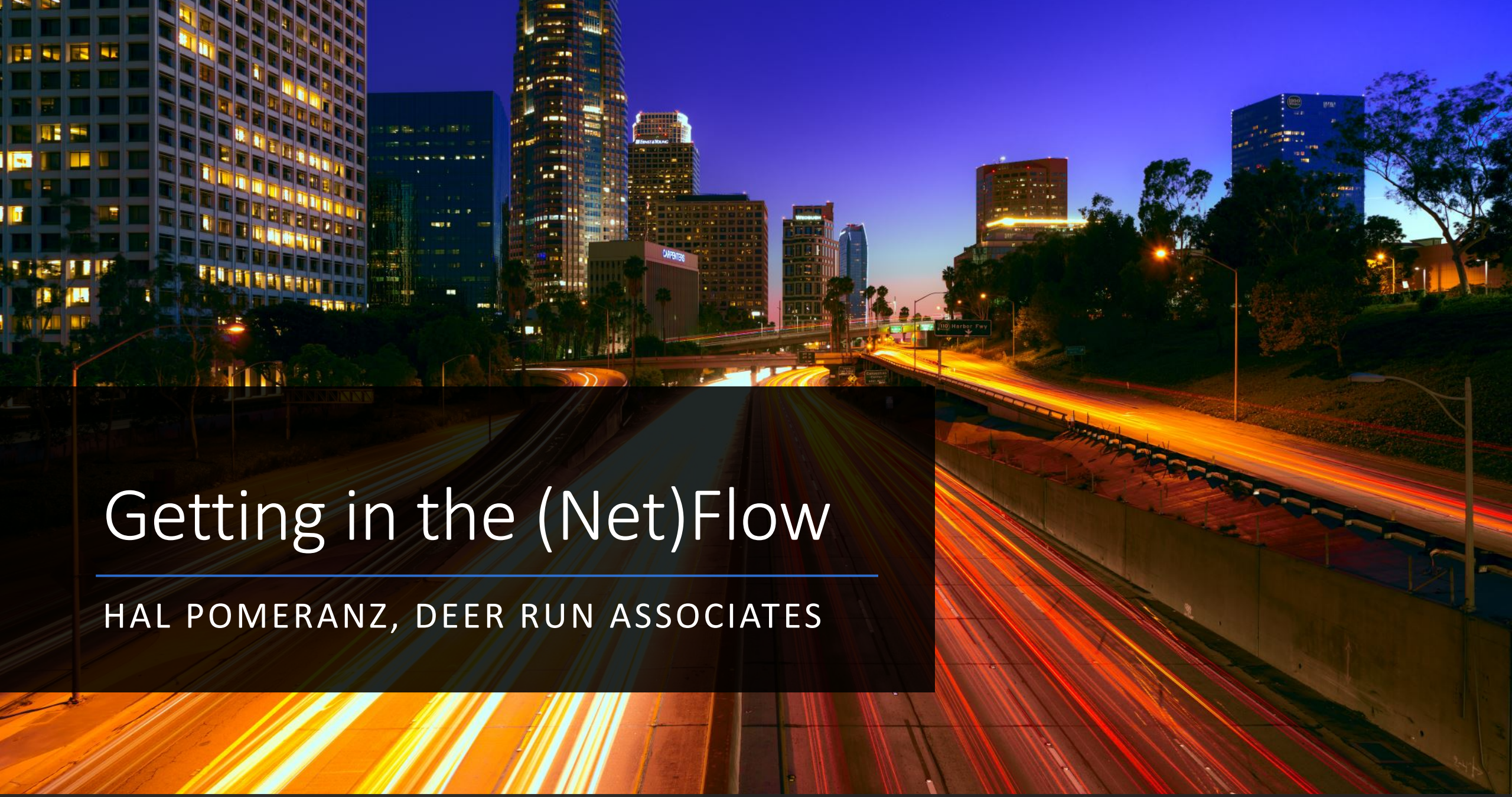
- Cyber Defence
- Penetration Testing
- Digital Forensics
- Ethical Hacking
- Security Management
- Cyber Threat Intelligence
- ICS/SCADA Security

GIAC CERTIFICATIONS

www.sans.org/sydney-2019

anz@sans.org

SANS Community Sessions



Getting in the (Net)Flow

HAL POMERANZ, DEER RUN ASSOCIATES

Packet Capture

Expensive!

- Taps and collectors
- Storage
- Analysis engines

Legal restrictions

	0	1	2	3
0x00	srcAddr			
0x04	dstAddr			
0x08	nextHop			
0x0C	inputSNMP		outputSNMP	
0x10	dPkts			
0x14	dOctets			
0x18	first			
0x1C	last			
0x20	srcPort		dstPort	
0x24	pad1	tcpFlags	prot	TOS
0x28	srcAS		dstAS	
0x2C	srcMask	dstMask	pad2	

NetFlow

Started as routing optimization

Just summary data

- Src/dest IP and port
- Protocol
- Start/end time
- Total packets/bytes sent

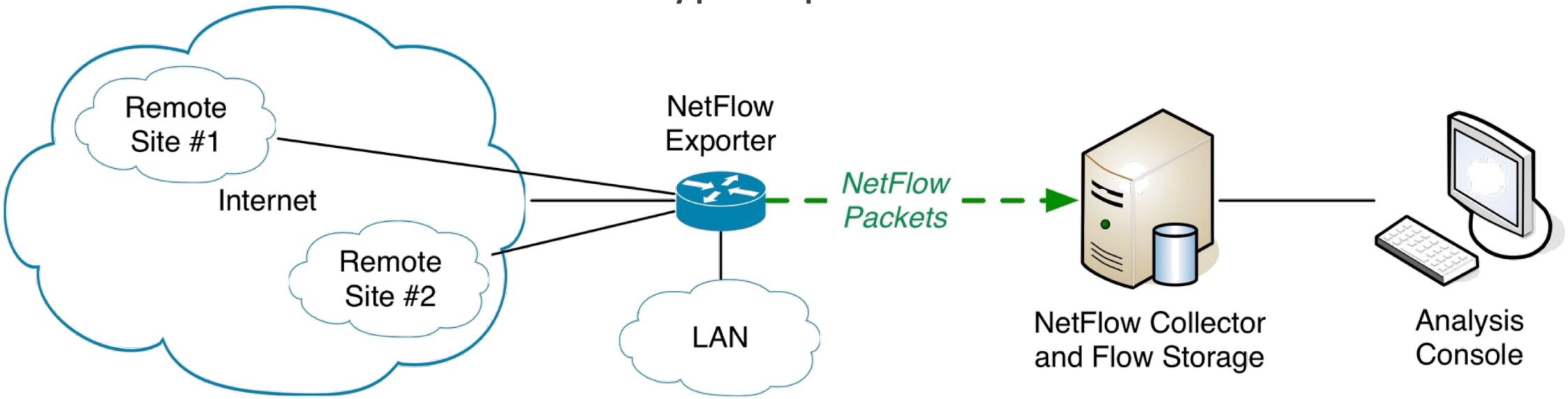
Benefits

Already in your infrastructure

Store data longer– great for hunting!

Rapidly spot suspicious activity

Encrypted protocols? No difference!



Collectors

nfcapd

SiLK

SOF-ELK

Various commercial

Get With the Demo Already!

Data Store

Top 10 dest IPs by total bytes sent

Order by bytes

Ignore internal hosts

```
SIFT$ nfdump -R netflow/ -s dstip/bytes -O bytes 'not dst net 10.0.0.0/8'
Top 10 Dst IP Addr ordered by bytes:
Date first seen          Duration  Proto  Dst IP Addr        Flows(%)    Packets(%)       Bytes(%)
2012-04-03 01:03:09.877 322713.426 any    199.73.28.114    37453(29.6) 254045(32.4)   59.1 M(38.1)
2012-04-03 00:32:51.022 323790.597 any    207.58.245.179    1226( 1.0)  67919( 8.7)   46.0 M(29.6)
2012-04-02 21:52:24.449  94555.891 any    199.59.148.87     5114( 4.0)  42968( 5.5)    9.0 M( 5.8)
2012-04-04 03:35:42.075 229923.283 any    173.173.88.154     662( 0.5)  24174( 3.1)    7.8 M( 5.0)
2012-04-03 23:55:42.732 243046.744 any    12.190.135.235    8941( 7.1)  44361( 5.7)    4.7 M( 3.0)
2012-04-02 21:52:22.258 336940.332 any    96.255.98.154     3423( 2.7) 134956(17.2)    4.3 M( 2.8)
2012-04-02 23:13:45.952  68474.621 any    69.171.227.72      266( 0.2)   3587( 0.5)    1.5 M( 1.0)
2012-04-03 06:03:18.178 279675.667 any    69.164.192.215   40170(31.8)  40416( 5.2)    1.1 M( 0.7)
2012-04-02 21:52:24.486 336596.889 any    208.67.222.222    2483( 9.9)  12483( 1.6)  710722( 0.5)
2012-04-03 17:23:00.811   2996.191 any    63.233.110.148      15( 0.0)   5283( 0.7)  646464( 0.4)

Summary: total flows: 126373, total bytes: 155278100, total packets: 783326…
Time window: 2012-04-02 21:52:19 - 2012-04-06 19:28:02
Total flows processed: 323982, Blocks skipped: 0, Bytes read: 15578112
Sys: 0.044s flows/second: 7363227.3  Wall: 0.042s flows/second: 7704318.5
```

Many flows, few packets per flow– possible C2 channel

Large data, few flows– likely exfiltration

Aggregate and summarize flow data with customizable parameters

Custom output formatting

Output ordered by first flow start time

```
SIFT$ nfdump -R netflow/ -A srcip,dstip,dstport -O tstart \
            -o "fmt:%ts %sa -> %dap %byt %pkt %fl" 'dst host 199.73.28.114'
Date first seen              Src IP Addr         Dst IP Addr:Port     Bytes  Packets Flows
2012-04-03 01:03:09.877        10.3.58.7 ->    199.73.28.114:80      31.2 M   145160 23927
2012-04-03 16:28:43.187        10.3.58.7 ->    199.73.28.114:8000       252        9     3
2012-04-03 16:30:27.015        10.3.58.7 ->    199.73.28.114:443      17324      806     4
2012-04-03 21:04:27.948        10.3.58.5 ->    199.73.28.114:443     18.0 M    29821    82
2012-04-03 21:45:39.148        10.3.58.5 ->    199.73.28.114:4444      1104       36     4
2012-04-03 22:24:57.820        10.3.58.5 ->    199.73.28.114:80        1771       20     4
2012-04-03 22:25:12.596        10.3.58.5 ->    199.73.28.114:8080       184        6     2
2012-04-03 22:38:31.056        10.3.58.5 ->    199.73.28.114:53         276        9     3
2012-04-05 17:47:46.780        10.3.58.6 ->    199.73.28.114:80       9.9 M    78166 13420
2012-04-06 15:33:54.362        10.3.58.6 ->    199.73.28.114:22         368       12     4
Summary: total flows: 37453, total bytes: 59093636, total packets: 254045…
Time window: 2012-04-02 21:52:19 - 2012-04-06 19:28:02
Total flows processed: 323982, Blocks skipped: 0, Bytes read: 15578112
Sys: 0.040s flows/second: 8099550.0  Wall: 0.042s flows/second: 7699923.9
```

Timestamps show earliest attacker activity on each system, order of compromise

“long” output format shows TCP flags – SYN only means unsuccessful connection attempts

```
SIFT$ nfdump -R netflow/ -O tstart -o long 'dst host 199.73.28.114 and dst port 8000'
Date first seen          Duration Proto      Src IP Addr:Port          Dst IP Addr:Port   Flags
2012-04-03 16:28:43.187     8.979 TCP          10.3.58.7:1132  ->    199.73.28.114:8000  ....S.
2012-04-03 16:28:43.435     9.033 TCP          10.3.58.7:1134  ->    199.73.28.114:8000  ....S.
2012-04-03 16:29:04.440     8.949 TCP          10.3.58.7:1241  ->    199.73.28.114:8000  ....S.
Summary: total flows: 3, total bytes: 252, total packets: 9…
Time window: 2012-04-02 21:52:19 - 2012-04-06 19:28:02
Total flows processed: 323982, Blocks skipped: 0, Bytes read: 15578112
Sys: 0.036s flows/second: 8999500.0  Wall: 0.037s flows/second: 8729844.8
```

Focus on the largest data flows

```
SIFT$ nfdump -R netflow/ -q -A srcip,dstip,dstport -O tstart \
          -o "fmt:%ts %sa -> %dap %byt %pkt %fl" 'dst host 207.58.245.179'
2012-04-03 00:32:51.022        10.3.58.7 ->   207.58.245.179:80        4596      108     6
2012-04-03 00:33:17.118        10.3.58.7 ->   207.58.245.179:443     274874      675     3
2012-04-03 22:41:05.020        10.3.58.5 ->   207.58.245.179:80        3193       52     6
2012-04-06 16:34:11.276        10.3.58.6 ->   207.58.245.179:80      45.0 M    59590     4
2012-04-06 16:35:50.971        10.3.58.6 ->   207.58.245.179:443     734014     7494  1207
SIFT$ nfdump -R netflow -O tstart \
          'src host 10.3.58.6 and dst host 207.58.245.179 and dst port 80'
Date first seen          Duration Proto  Src IP Addr:Port     Dst IP Addr:Port  Packets  Bytes
2012-04-06 16:34:11.276     6.214 TCP     10.3.58.6:61407 -> 207.58.245.179:80      934  35952
2012-04-06 16:44:44.716     3.394 TCP     10.3.58.6:61658 -> 207.58.245.179:80       26   2888
2012-04-06 16:45:34.832   265.102 TCP     10.3.58.6:61684 -> 207.58.245.179:80    28798 22.1 M
2012-04-06 16:50:00.009   270.510 TCP     10.3.58.6:61684 -> 207.58.245.179:80    29832 22.9 M
Summary: total flows: 4, total bytes: 45012572, total packets: 59590…
Time window: 2012-04-02 21:52:19 - 2012-04-06 19:28:02
Total flows processed: 323982, Blocks skipped: 0, Bytes read: 15578112
Sys: 0.036s flows/second: 8999500.0  Wall: 0.043s flows/second: 7415472.6
```

Exfil via 80/tcp in two large transfers

Timestamps useful for correlation with host evidence and PCAPs

Next Steps

PCAP data?

- Extract interesting flows

Host evidence?

- Flow starts as pivot points

SANS

The Most Trusted Source for Information Security Training, Certification, and Research

"The course is a very good introduction to a very complex topic. It balances the technical and theory extremely well."
-Andrew Mayhew, **Alcoa**

CYBER SECURITY TRAINING

Sydney 2019

Grace Hotel Sydney | 4-23 November

Protect Your Organisation Advance Your Career

12 hands-on, immersion-style courses taught by real-world practitioners

Hal Pomeranz – hal@sans.org
http://deer-run.com/~hal/

Courses offered in:

- Cyber Defence
- Penetration Testing
- Digital Forensics
- Ethical Hacking
- Security Management
- Cyber Threat Intelligence
- ICS/SCADA Security

GIAC CERTIFICATIONS

www.sans.org/sydney-2019

anz@sans.org

SANS Community Sessions