The Bro Monitoring Platform

Adam Slagell

National Center for Supercomputing Applications

Borrowed from Robin Sommer
International Computer Science Institute

"What Is Bro?"

TCPDUMP

WIRESHARK

SNORT

NetFlow

syslog

python

Packet Capture

Traffic Inspection

Attack Detection

Log Recording
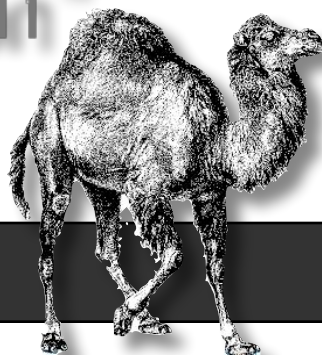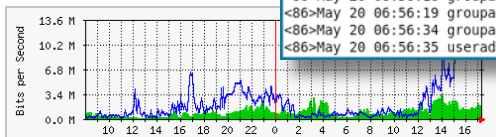
Flexibility
Abstraction
Data Structures

BRO NETWORK SECURITY MONITOR

"Domain-specific Python"

Bro History

Bro IDS

BRO NETWORK SECURITY MONITOR

Academic
Publications

Host Context
Time Machine
Enterprise Traffic

TRW
State Mgmt.
Independ. State

Bro Cluster
Shunt

Anonymizer
Active Mapping
Context Signat.

Parallel Prototype

Input Framework

BinPAC
DPD
2nd Path

Stepping Stone
Detector

USENIX Paper

Autotuning

1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013

Vern writes 1st
line of code

BERKELEY LAB

v0.2
1st CHANGES
entry

v0.6
RegExps
Login analysis

v0.7a90
Profiling
State Mgmt

v0.8aX/0.9aX
SSL/SMB
STABLE releases
BroLite

v1.1/v1.2
when Stmt
Resource
tuning
Broccoli
DPD

v1.5
BroControl

v2.0
New Scripts

v2.2
File Analysis
Summary Stat.

v2.1
IPv6
Input Framew.

LBNL starts
using Bro
operationally

v0.4
HTTP analysis
Scan detector
IP fragments
Linux support

v0.7a175/0.8aX
Signatures
SMTP
IPv6 support
User manual

v1.0
BinPAC
IRC/RPC analyzers
64-bit support
Sane version
numbers

v1.4
DHCP/BitTorrent
HTTP entities
NetFlow
Bro Lite Deprecated

Bro SDCI

NSF

Bro Center

NSF

v0.7a48
Consistent
CHANGES

0.8a37
Communication
Persistence
Namespaces
Log Rotation

v1.3
Ctor expressions
GeoIP
Conn Compressor

broala

"Who's Using It?"

Installations across the US

Universities
Research Labs
Supercomputing Centers
Government Organizations
Fortune 50 Enterprises

Examples

Lawrence Berkeley National Lab
National Center for Supercomputing Applications
Indiana University
General Electric
Mozilla Corporation
... and many more sites I can't talk about.

Fully integrated into *Security Onion*
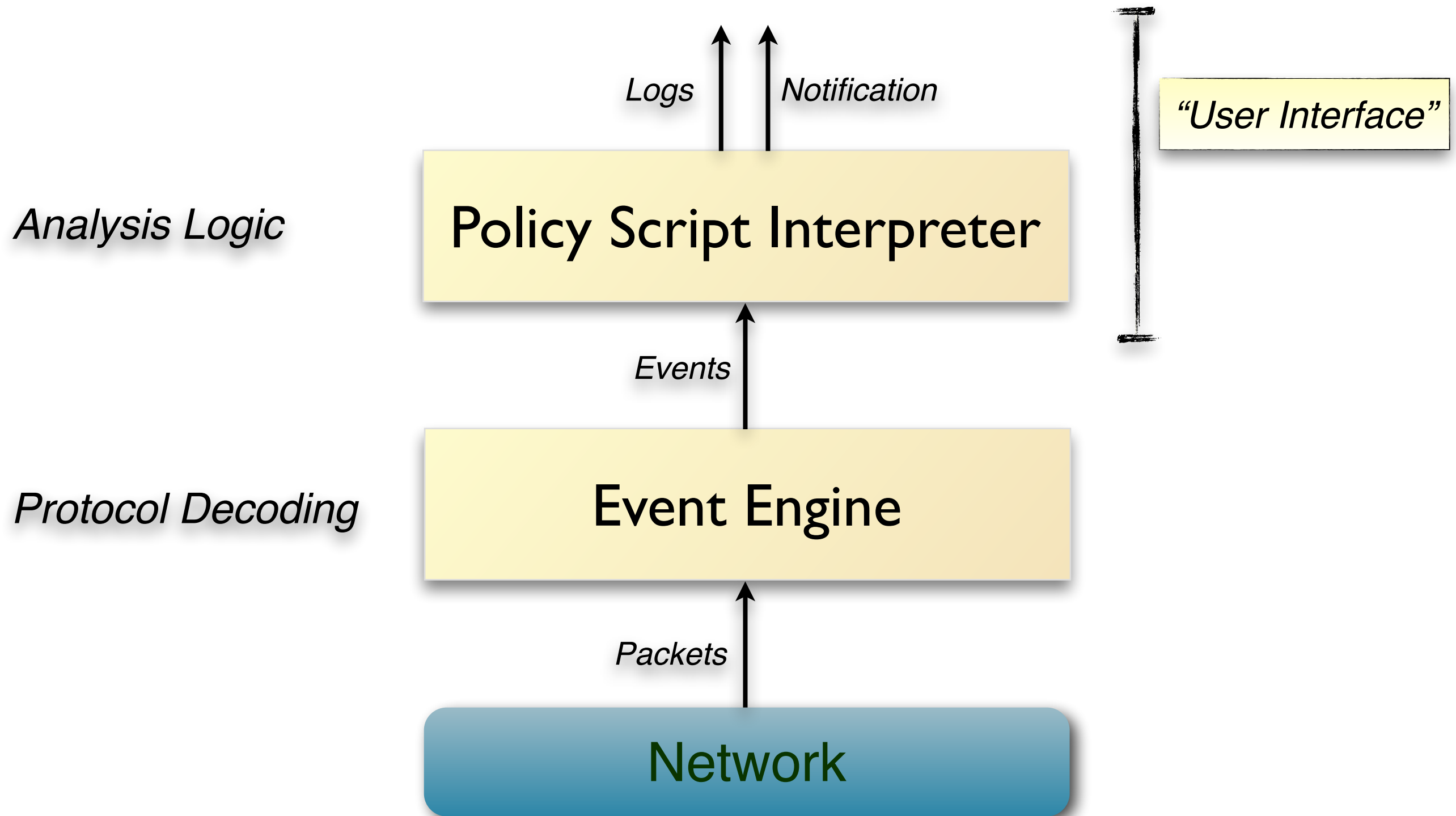
Popular security-oriented Linux distribution

BroCon 2014, Urbana, IL

Community

50/90/150/185 attendees at BroCon
'12/'13/'14/'15
110 organizations at BroCon '14
~4,000 Twitter followers
~1000 mailing list subscribers
~100 users average on IRC channel
10,000+ downloads / version
from 150 countries

Architecture

Analysis Logic

Policy Script Interpreter

Logs *Notification*

"User Interface"

Events

Protocol Decoding

Event Engine

Packets

Network

The Bro Platform

Apps

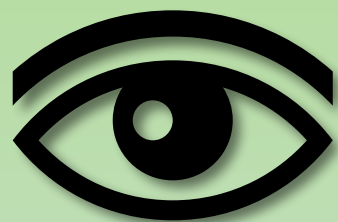| Intrusion Detection | Vulnerabilit. Mgmt | File Analysis | Traffic Measure-ment | Traffic Control | Compliance Monitoring |

Platform

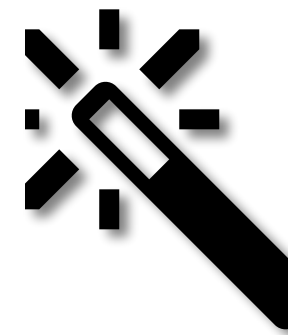| Programming Language | Standard Library |

Packet Processing

Tap

Network

"What Can It Do?"

Log Files

"Network Ground Truth"

Alerts

Custom Logic

Bro Logs

```
> bro -i eth0

[ … wait … ]

> cat conn.log
> ls *.log
```

```
#separator \x09
#set_separator ,
#empty_field   (empty)
#unset_field   -
#path    conn
#open    2013-04-28-23-47-26
#fields  ts       uid        id.orig_h      id.orig_p
#types   time     string     addr           port      [...]
1258531221.486539   arKYeMETxOg   192.168.1.102   68         192.168.1.1    […]
1258531680.237254   nQcgTWjvg4c   192.168.1.103   37         192.168.1.255  […]
1258531693.816224   j4u32Pc5bif   192.168.1.102   37         192.168.1.255  […]
1258531635.800933   k6kgXLOoSKl   192.168.1.103   138        192.168.1.255  […]
1258531693.825212   TEfuqmmG4bh   192.168.1.102   138        192.168.1.255  […]
1258531803.872834   5OKnoww6xl4   192.168.1.104   137        192.168.1.255  […]
1258531747.077012   FrJExwHcSal   192.168.1.104   138        192.168.1.255  […]
1258531924.321413   3PKsZ2Uye21   192.168.1.103   68         192.168.1.1    […]
[…]
```

NCSA

Connections Logs
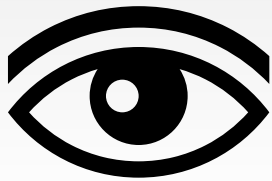
conn.log

`ts`	`1393099191.817686`	Timestamp
`uid`	`Cy3S2U2sbarorQgmw6a`	Unique ID
`id.orig_h`	`177.22.211.144`	Originator IP
`id.orig_p`	`43618`	Originator Port
`id.resp_h`	`115.25.19.26`	Responder IP
`id.resp_p`	`25`	Responder Port
`proto`	`tcp`	IP Protocol
`service`	`smtp`	App-layer Protocol
`duration`	`1.414936`	Duration
`orig_bytes`	`9068`	Bytes by Originator
`resp_bytes`	`4450`	Bytes by Responder
`conn_state`	`SF`	TCP state
`local_orig`	`T`	Local Originator?
`missed_bytes`	`0`	Gaps
`history`	`ShAdDaFf`	State History
`tunnel_parents`	`(empty)`	Outer Tunnels

HTTP

http.log

ts	1393099291.589208
uid	CKFUW73bIADw0r9pl
id.orig_h	17.22.7.4
id.orig_p	54352
id.resp_h	24.26.13.36
id.resp_p	80
method	POST
host	com-services.pandonetworks.com
uri	/soapservices/services/SessionStart
referrer	–
user_agent	Mozilla/4.0 (Windows; U) Pando/2.6.0.8
status_code	200
username	anonymous
password	–
orig_mime_types	application/xml
resp_mime_types	application/xml

SSL
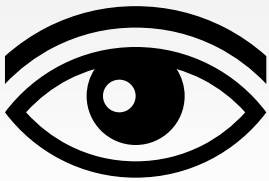
ssl.log		
ts	1392805957.927087	
uid	CEA05l2D7k0BD9Dda2	
id.orig_h	2a07:f2c0:90:402:41e:c13:6cb:99c	
id.orig_p	40475	
id.resp_h	2406:fe60:f47::aaeb:98c	
id.resp_p	443	
version	TLSv10	
cipher	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	
server_name	www.netflix.com	
subject	CN=www.netflix.com,OU=Operations, O=Netflix, Inc.,L=Los Gatos, ST=CALIFORNIA,C=US	
issuer_subject	CN=VeriSign Class 3 Secure Server CA, OU=VeriSign Trust Network,O=VeriSign, C=US	
not_valid_before	1389859200.000000	
not_valid_after	1452931199.000000	
client_subject	-	
client_issuer_subject	-	
cert_hash	197cab7c6c92a0b9ac5f37cfb0699268	
validation_status	ok	

Syslog & DHCP

ts	1392796803.311801
uid	CnYivt3ZONHOuBALR8
id.orig_h	12.3.8.161
id.orig_p	514
id.resp_h	16.74.12.24
id.resp_p	514
proto	udp
facility	AUTHPRIV
severity	INFO
message	sshd[13825]: Accepted publickey for harvest from xxx.xxx.xxx.xxx

dhcp.log

ts	1392796962.091566
uid	Ci3RM24iF4vIYRGHc3
id.orig_h	10.129.5.11
id.resp_h	10.129.5.1
mac	04:12:38:65:fa:68
assigned_ip	10.129.5.11
lease_time	14400.000000

Files

files.log

ts	1392797643.447056
fuid	FnungQ3TI19GahPJP2
tx_hosts	191.168.187.33
rx_hosts	10.1.29.110
conn_uids	CbDgik2fjeKL5qzn55
source	SMTP
analyzers	SHA1,MD5
mime_type	application/x-dosexec
filename	Letter.exe
duration	5.320822
local_orig	T
seen_bytes	39508
md5	93f7f5e7a2096927e06e[…]1085bfcfb
sha1	daed94a5662a920041be[…]a433e501646ef6a03
extracted	-

Software

software.log

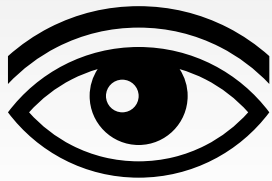|	
ts	1392796839.675867
host	10.209.100.2
host_p	-
software_type	HTTP::BROWSER
name	DropboxDesktopClient
version.major	2
version.minor	4
version.minor2	11
version.minor3	-
version.addl	Windows
unparsed_version	DropboxDesktopClient/2.4.11 (Windows; 8; i32; en_US; Trooper 5694-2047-1832-6291-8315)

Help Understand Your Network
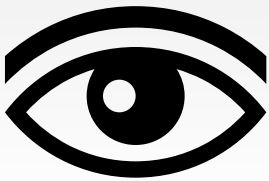
Top File Types
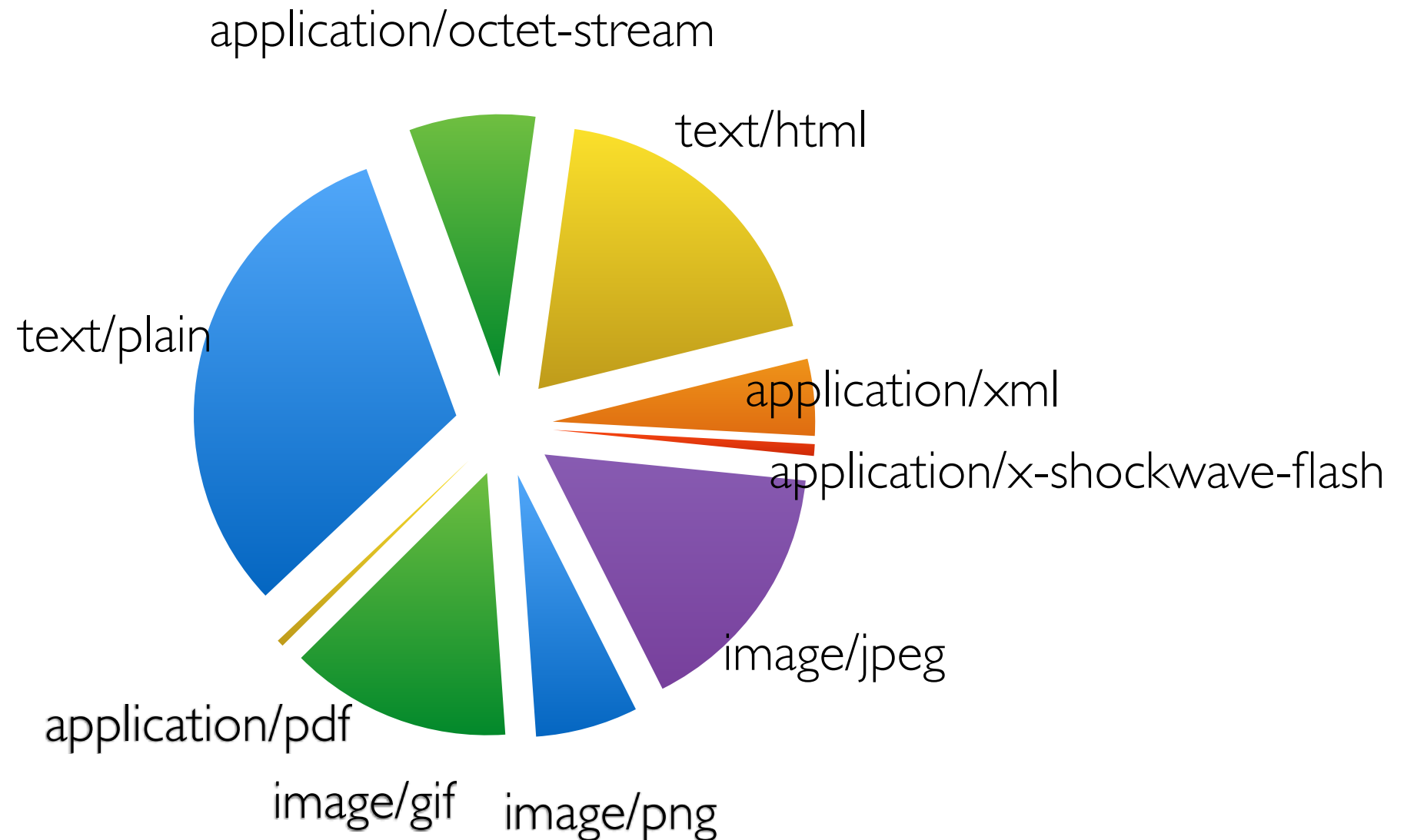

```
cat files.log | bro-cut mime_type | sort | uniq -c | sort -rn
```

Top Software by Number of Hosts
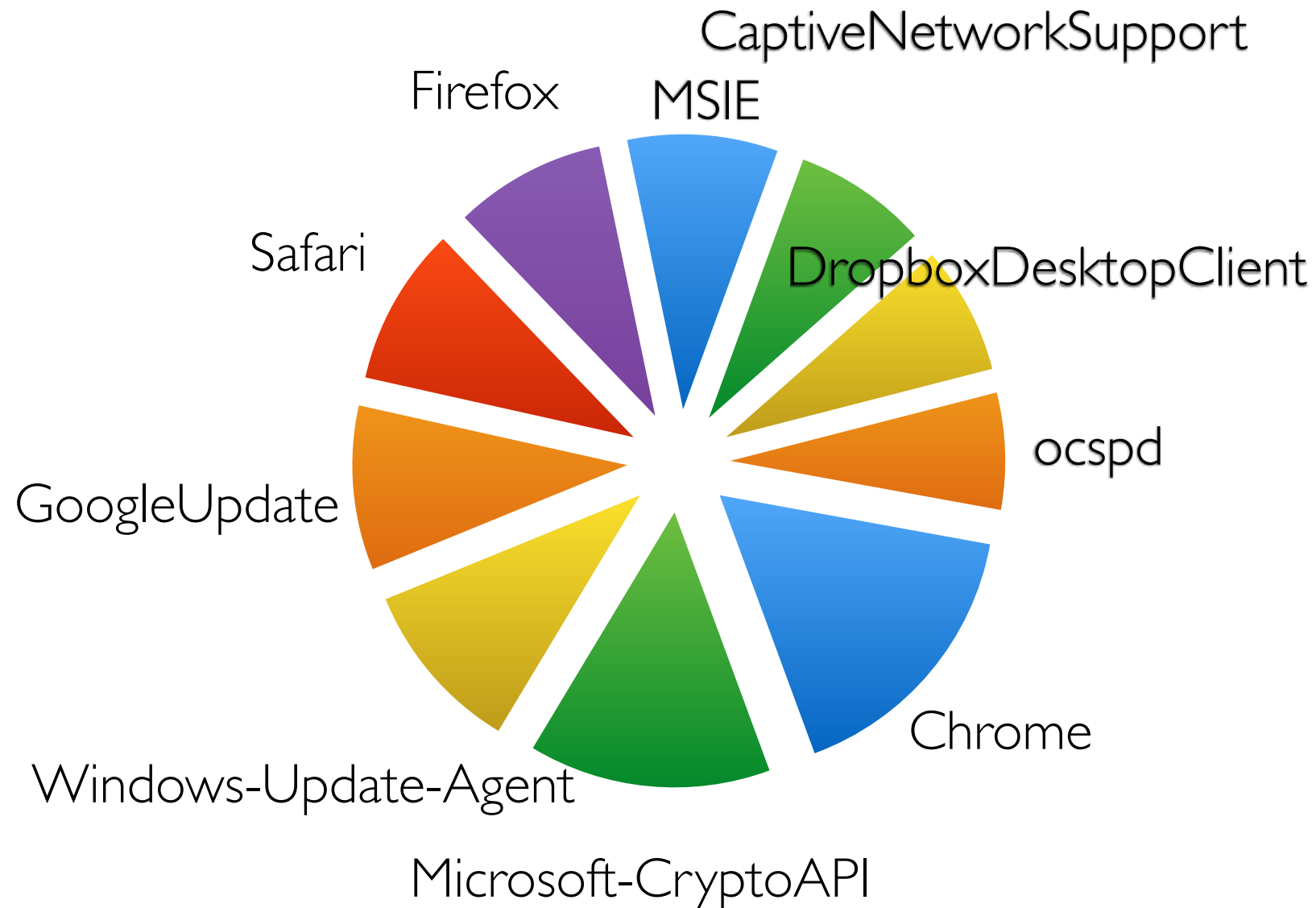

```
cat software.log  | bro-cut host name | sort | uniq |
awk -F '\t' '{print $2}' | sort | uniq -c | sort -rn
```
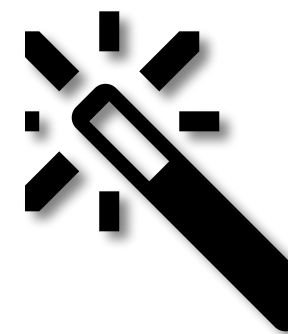
"What Can It Do?"

Log Files

Alerts

Custom Logic

"Watch this!"

Recorded in notice.log.
Can trigger actions.

Alerts in Bro 2.2

```
CaptureLoss::Too_Much_Loss          SSH::Password_Guessing
Conn::Ack_Above_Hole                SSH::Watched_Country_Login
Conn::Content_Gap                   SSL::Certificate_Expired
Conn::Retransmission_Inconsistency  SSL::Certificate_Expires_Soon
DNS::External_Name                  SSL::Certificate_Not_Valid_Yet
FTP::Bruteforcing                   SSL::Invalid_Server_Cert
FTP::Site_Exec_Success              Scan::Address_Scan
HTTP::SQL_Injection_Attacker        Scan::Port_Scan
HTTP::SQL_Injection_Victim          Signatures::Count_Signature
Intel::Notice                       Signatures::Multiple_Sig_Responders
PacketFilter::Dropped_Packets       Signatures::Multiple_Signatures
ProtocolDetector::Protocol_Found    Signatures::Sensitive_Signature
ProtocolDetector::Server_Found      Software::Software_Version_Change
SMTP::Blocklist_Blocked_Host        Software::Vulnerable_Version
SMTP::Blocklist_Error_Message       TeamCymruMalwareHashRegistry::Match
SMTP::Suspicious_Origination        Traceroute::Detected
SSH::Interesting_Hostname_Login     Weird::Activity
SSH::Login_By_Password_Guesser
```

Watching for Suspicious Logins

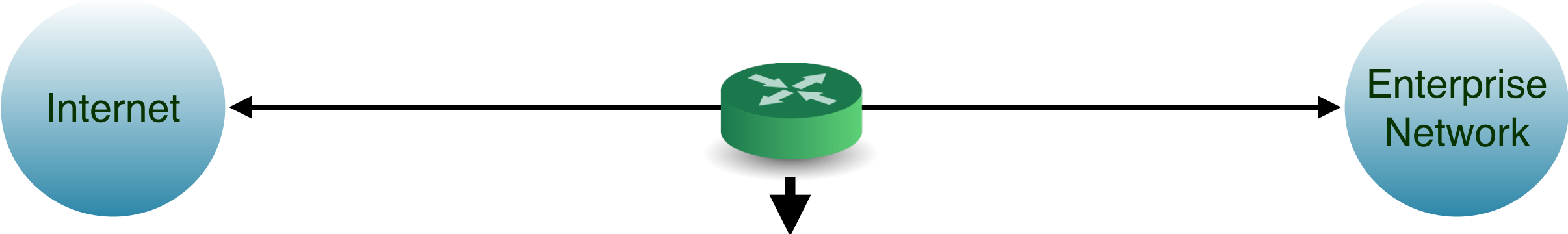
SSH::Watched_Country_Login

Login from an unexpected country.

SSH::Interesting_Hostname_Login

Login from an unusual host name.

smtp.supercomputer.edu

Intelligence Integration (Passive)

Internet ←→ Enterprise Network

Traffic Monitoring

HTTP, FTP, SSL, SSH, FTP, DNS, SMTP, …

```
Conn::IN_ORIG
Conn::IN_RESP
Files::IN_HASH
Files::IN_NAME
DNS::IN_REQUEST
DNS::IN_RESPONSE
HTTP::IN_HOST_HEADER
HTTP::IN_REFERRER_HEADER
HTTP::IN_USER_AGENT_HEADER
HTTP::IN_X_FORWARDED_FOR_HEADER
HTTP::IN_URL
SMTP::IN_MAIL_FROM
SMTP::IN_RCPT_TO
SMTP::IN_FROM
SMTP::IN_TO
SMTP::IN_RECEIVED_HEADER
SMTP::IN_REPLY_TO
SMTP::IN_X_ORIGINATING_IP_HEADER
SMTP::IN_MESSAGE
SSL::IN_SERVER_CERT
SSL::IN_CLIENT_CERT
SSL::IN_SERVER_NAME
SMTP::IN_HEADER
```

ts	1258565309.806483
uid	CAK677xaOmi66X4Th
id.orig_h	192.168.1.103
id.resp_h	192.168.1.1
note	Intel::Notice
indicator	baddomain.com
indicator_type	Intel::DOMAIN
where	HTTP::IN_HOST_HEADER
source	My-Private-Feed

notice.log

Intelligence Integration (Active)

```
# cat files.log | bro-cut mime_type sha1 | awk '$1 ~ /x-dosexec/'
application/x-dosexec    5fd2f37735953427e2f6c593d6ec7ae882c9ab54
application/x-dosexec    00c69013d34601c2174b72c9249a0063959da93a
application/x-dosexec    0d801726d49377bfe989dcca7753a62549f1ddda
[…]
```

```
# dig +short 733a48a9cb4[…]2a91e8d00.malware.hash.cymru.com TXT
"1221154281 53"
```

notice.log

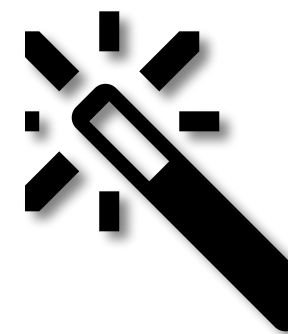|		
ts	**1392423980.736470**	Timestamp
uid	**CjKeSB45xaOmiIo4Th**	Connection ID
id.orig_h	**10.2.55.3**	Originator IP
id.resp_h	**192.168.34.12**	Responder IP
fuid	**FEGVbAgcArRQ49347**	File ID
mime_type	**application/jar**	MIME type
description	**http://app.looking3g.com/[…]**	Source URL Bro saw
note	**TeamCymruMalwareHashRegistry::Match**	Notice Type
msg	**2013-09-14 22:06:51 / 20%**	MHR reply
sub	**https://www.virustotal.com/[…]**	VirusTotal URL

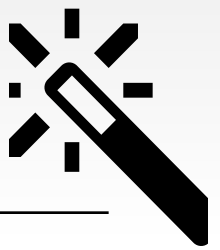# "What Can It Do?"
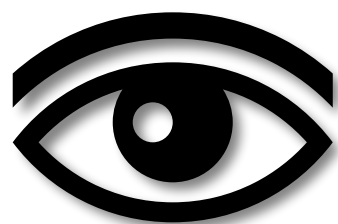
Log Files

Alerts

Custom Logic

*"Don't ask what Bro can do. Ask what **you want** it to do."*

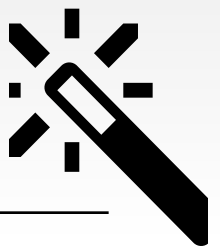# Script Example: Matching URLs

Task: Report all Web requests for files called "passwd".

```
event http_request(c: connection,           # Connection.
                    method: string,         # HTTP method.
                    original_URI: string,   # Requested URL.
                    unescaped_URI: string,  # Decoded URL.
                    version: string)        # HTTP version.
{
    if ( method == "GET" && unescaped_URI == /.*passwd/ )
        NOTICE(...); # Alarm.
}
```

Script Example: Scan Detector

Task: Count failed connection attempts per source address.
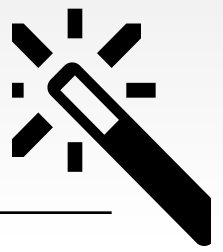
```
global attempts: table[addr] of count &default=0;

event connection_rejected(c: connection)
{
    local source = c$id$orig_h;       # Get source address.

    local n = ++attempts[source];     # Increase counter.

    if ( n == SOME_THRESHOLD )         # Check for threshold.
        NOTICE(...);                   # Alarm.
}
```

Scripts are Bro's "Magic Ingredient"

Bro comes with >10,000 lines of script code.
   Prewritten functionality that's just loaded.

Scripts generate everything we have seen.
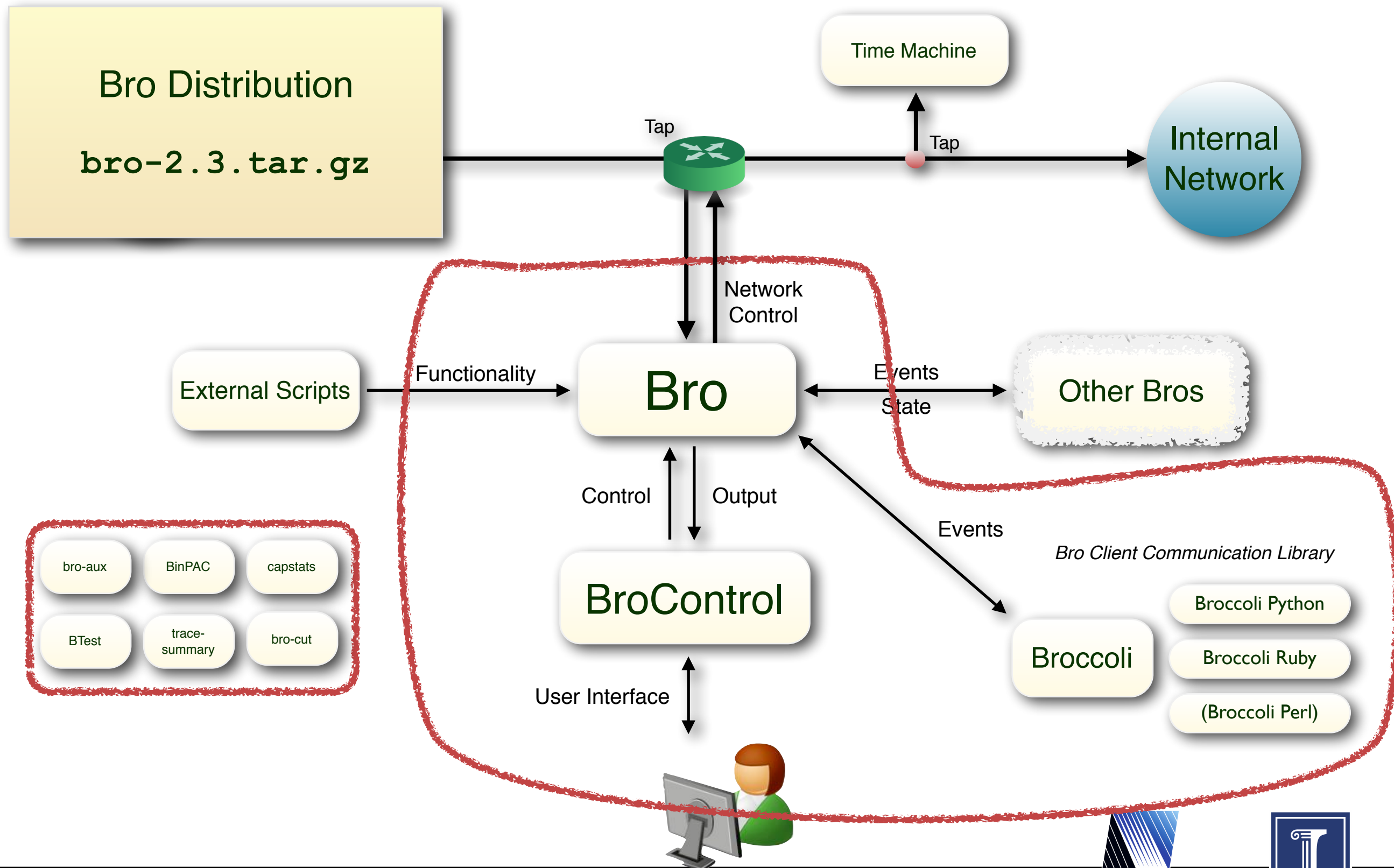   Amendable to extensive customization and extension.

Growing community writing 3rd party scripts.
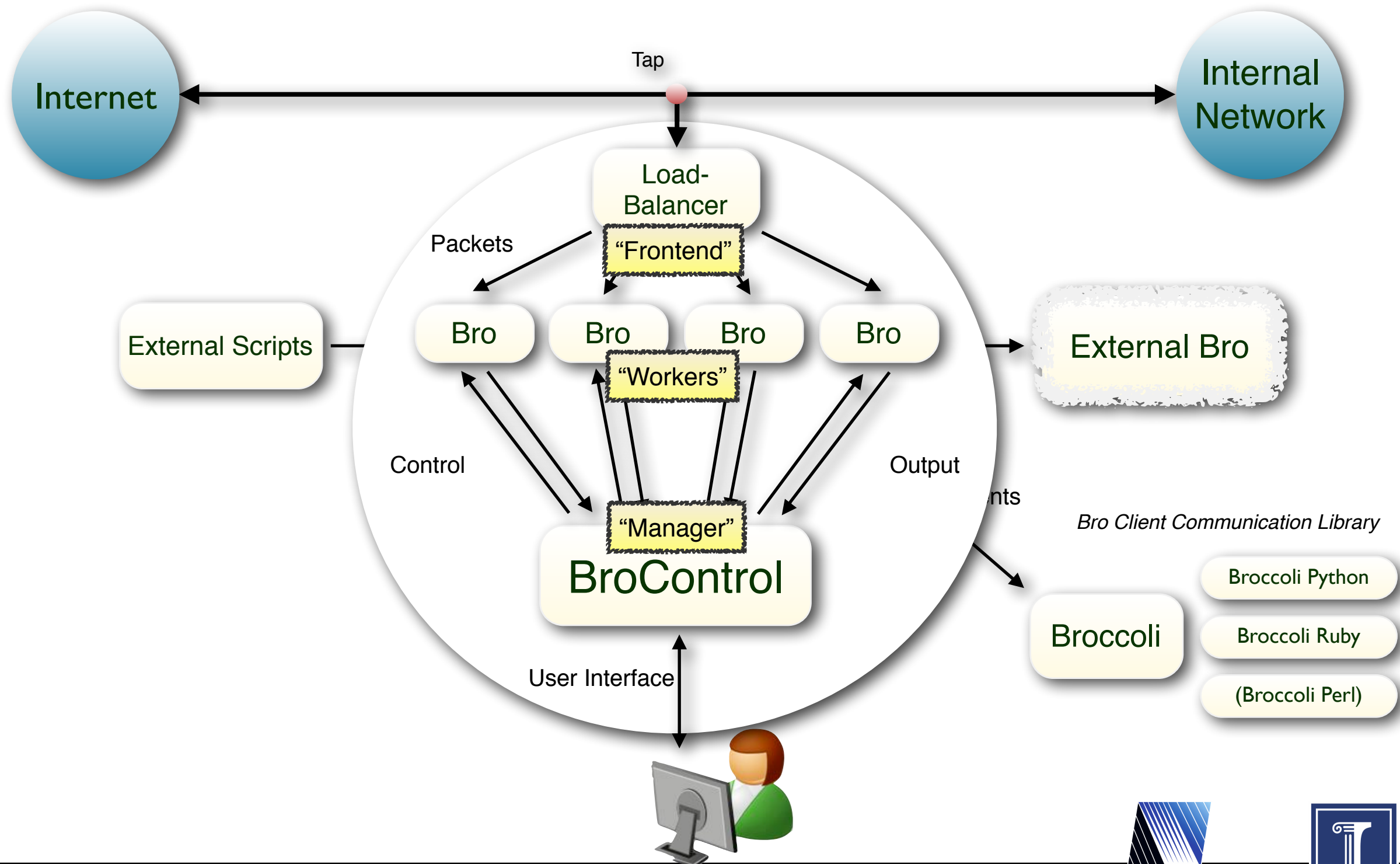   Bro could report Mandiant's APT1 indicators within a day.
   Same for Heartbleed

Bro Ecosystem

Bro Ecosystem

Bro *Cluster* Ecosystem

Installing Bro

Here: We'll use ISLET.
Comes with everything preinstalled.

Normally: Follow instructions on bro.org.
`http://www.bro.org/sphinx/install`

Building from source is pretty straight-forward:

```
> yum install cmake flex bison swig libpcap-devel […]

> wget http://www.bro.org/downloads/release/bro-2.2.tar.gz
> tar xzvf bro-2.2.tar.gz
> cd bro

> ./configure -—prefix=/usr/local && make && make install
```

Configuring Bro

In many cases, just two files to edit.

`<prefix>/etc/node.cfg`

```
# If you have a small network and only one interface to monitor,
# this will do it. We'll talk about cluster mode later.
[bro]
type=standalone
host=localhost
interface=eth0
```

`<prefix>/etc/networks.cfg`

```
# List of local networks in CIDR notation, optionally followed by a
# descriptive tag.
# For example, "10.0.0.0/8" or "fe80::/64" are valid prefixes.

10.0.0.0/8              Private IP space
192.168.0.0/16          Private IP space
```

(There's also `<prefix>/etc/broctl.cfg` with more options you can tweak.)

Using BroControl

Use "broctl" to start & stop.

```
# broctl install
# broctl start
starting bro ...
# broctl status
Name         Type        Host        Status    Pid      Started
bro          standalone  localhost   running   16737    15 May 15:57:35
# ls <prefix>/logs/current/
conn.log http.log […]
```

Reinstall after changing Bro's configuration.

```
# broctl check
bro is ok
# broctl install
# broctl restart
```

Using Bro from the Command Line

We'll use the Bro binary directly.

```
# bro -r trace.pcap
# ls *.log
conn.log http.log […]
```

"bro-cut" is a handy tool to work with logs.

```
# cat http.log | bro-cut -d ts id.orig_h host
2009-11-21T02:19:34-0800 192.168.1.105 download.windowsupdate.com
2009-11-21T02:19:37-0800 192.168.1.105 www.update.microsoft.com
[…]
```

Generally, use your standard Unix tools.
grep, awk, head/tail, sed, etc.

So much more …

Bro is … a Platform

Intrusion Detection	Vulnerabilit. Mgmt	File Analysis	Traffic Measure-ment	Traffic Control	Compliance Monitoring

There's much more we can talk about …

Host-level integration
Data import and export
Automatic Reaction
Monitoring Internal Networks
Measurements
SDN integration
Industrial Control Systems
Embedded Devices
Current Research

More File Analysis
More Protocols
More File Analysis
100Gb/s Networks
Enterprise Protocols
Summary Statistics
Science DMZs
ICSL SSL Notary
Cluster Deployment

Using ISLET & Try.Bro

- ISLET Server

  - Full Linux environment
  - ssh demo@54.149.11.154
  - Password is "CTSC"
    - Then create your own account
  - exercises are in /exercises

- Try.Bro

  - Point web browser to try.bro.org
  - Good for playing with language, seeing logs

The U.S. National Science Foundation has enabled much of our work.

Bro is coming out of almost two decades of academic research, along with extensive transition to practice efforts. NSF has supported much of that, and is currently funding a Bro Center of Expertise at the *International Computer Science Institute* and the *National Center for Supercomputing Applications*.

The Bro Project

www.bro.org

info@bro.org

@Bro_IDS

Commercial Support

www.broala.com

info@broala.com

@Broala_