Bro: The Network Defense Framework

Comprehensive Visibility & Defense for Every Corner of Your Network

Robin Sommer

International Computer Science Institute, &
Broala, Inc.

robin@icsi.berkeley.edu
robin@broala.com

http://www.icir.org/robin

Outline

Architecture, deployment, history.

Visibility, detection, customization.

Scaling & enterprise deployment

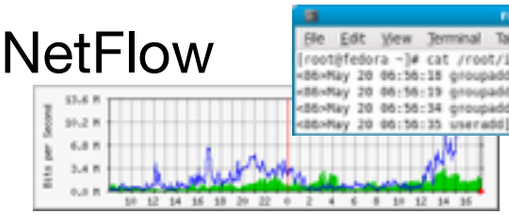
“What Is Bro?”

Packet Capture

Traffic Inspection

Attack Detection

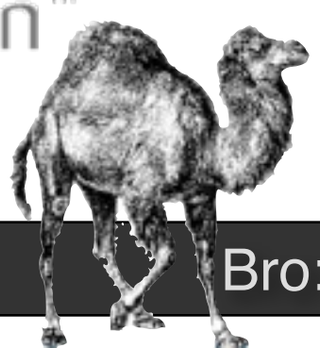
NetFlow



syslog

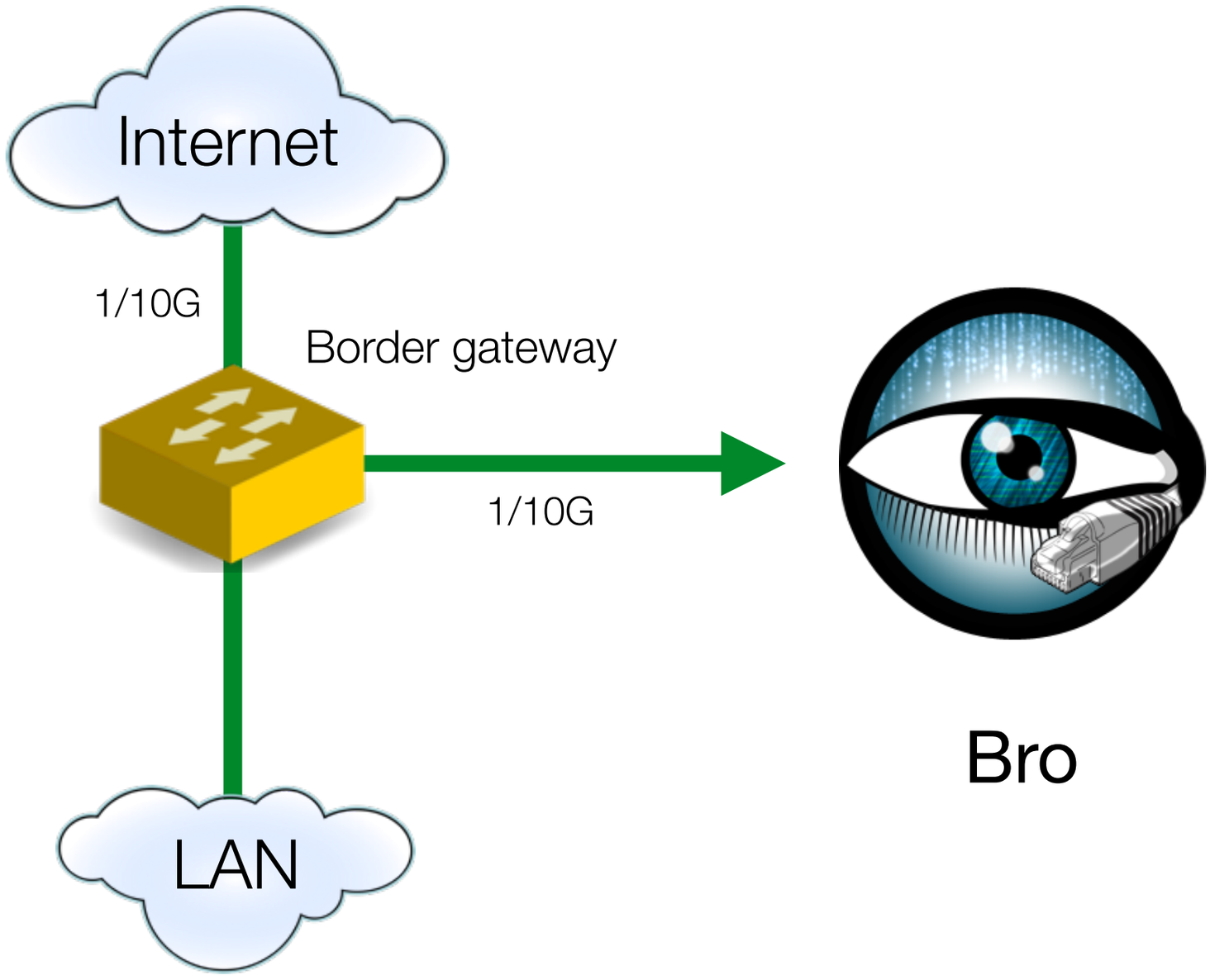
Log Recording

Flexibility
Abstraction
Data Structures



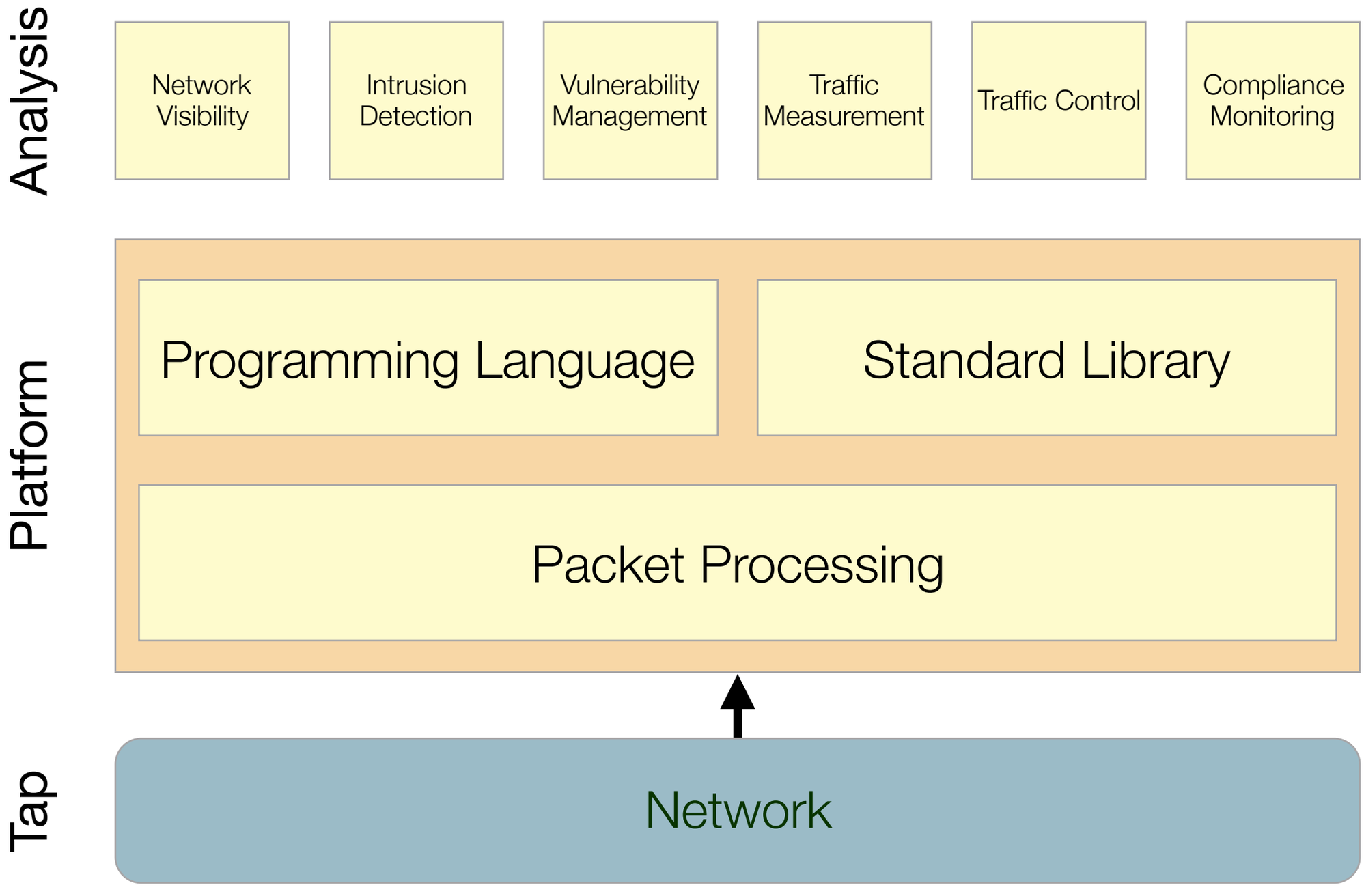
broala

Typical Deployment



Architecture

Open-source
BSD License



“Who’s Using It?”

Installations across the Country

Universities & research Labs
Most DOE National Labs
Supercomputing centers
Government organizations
Fortune 20 enterprises

Community

50/90/150/180 attendees at BroCon ’12/’13/’14/‘15
110 organizations at BroCon ‘15
5,000 Twitter followers
1,000 mailing list subscribers
100 users average on IRC channel
1,400 stars on GitHub
Direct downloads from 150 countries

Fully integrated into Security Onion

Popular security-oriented Linux distribution

Security Onion

ICSI

broala

Bro History

Academic Publications

1995 1996 1997 1998 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016

- 1998: USENIX Paper
- 2000: Backdoors, Stepping Stones
- 2003: Anonymizer, Active Mapping, Context Signat.
- 2004: TRW, State Mgmt., Independ. State
- 2005: Host Context, Time Machine, Enterprise Traffic
- 2006: BinPAC, DPD, 2nd Path
- 2007: Bro Cluster, Shunt
- 2008: Autotuning
- 2009: Parallel Prototype
- 2012: Input Framework
- 2013: SSL Trust, Relationships
- 2014: Summary Stats, HILTI, DPI Concurrency, PLC Modeling
- 2015: NetControl, VAST, Tor Traffic

- 1995: Vern writes 1st line of code
- 1996: LBNL starts using Bro operationally
- 1997: v0.2, 1st CHANGES entry
- 1998: v0.4, HTTP analysis, Scan detector, IP fragments, Linux support
- 1999: v0.6, RegExps, Login analysis
- 2000: v0.7a48, Consistent CHANGES
- 2002: v0.7a90, Profiling, State Mgmt
- 2003: v0.7a175/0.8aX, Signatures, SMTP, IPv6 support, User manual
- 2004: v0.8aX/0.9aX, SSL/SMB, STABLE releases, BroLite
- 2005: 0.8a37, Communication, Persistence, Namespaces, Log Rotation
- 2005: v1.0, BinPAC, IRC/RPC analyzers, 64-bit support, Sane version numbers
- 2006: v1.1/v1.2, *when* Stmt, Resource tuning, Broccoli, DPD
- 2007: v1.3, Ctor expressions, GeoIP, Conn Compressor
- 2008: v1.4, DHCP/BitTorrent, HTTP entities, NetFlow, Bro Lite Deprecated
- 2009: v1.5, BroControl
- 2010: v2.0, User Experience
- 2011: v2.1, IPv6, Input Framew.
- 2012: v2.2, File Analysis, Summary Stats
- 2013: v2.3, Performance, SNMP, Radius, SSL++
- 2014: v2.4, Broker, Plugins, DTLS/KRB

Bro SDCI — NSF

Bro Center — NSF

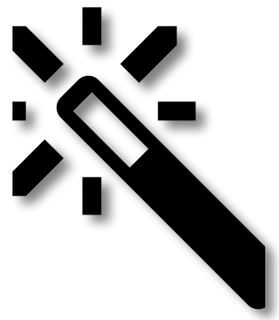
broala

broala

“What Can It Do?”

Visibility

Alerts

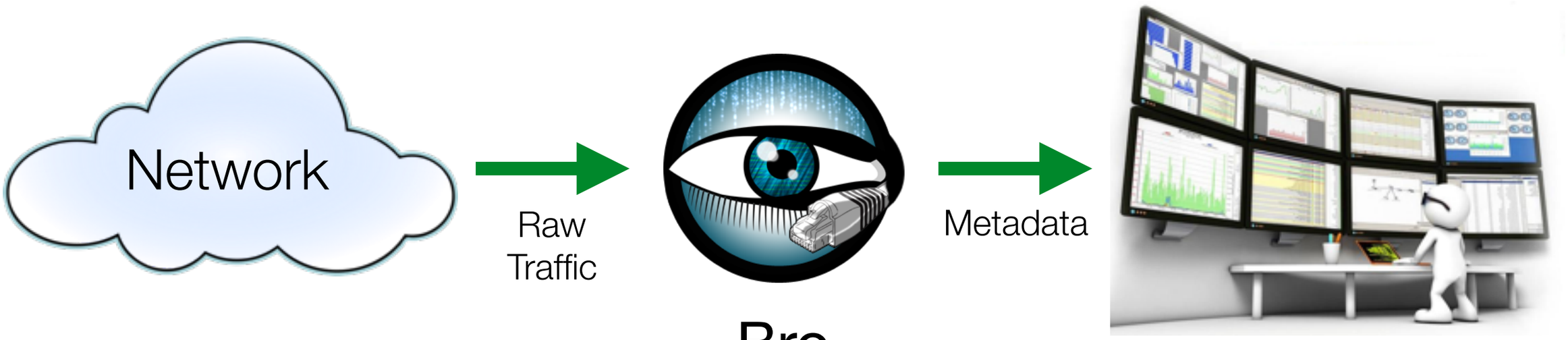


Custom Logic

“Network ground truth”

Bro's Log Files

Rich, structured, real-time metadata streams
for incident response & forensics.



Connection Logs

conn.log

ts	1393099415.790834	Timestamp
uid	CSoqsg12YRTsWjYbZc	Unique ID
id.orig_h	2004:b9e5:6596:9876:[…]	Originator IP
id.orig_p	59258	Originator Port
id.resp_h	2b02:178:2fde:bff:[…]	Responder IP
id.resp_p	80	Responder Port
proto	tcp	IP Protocol
service	http	App-layer Protocol
duration	2.105488	Duration
orig_bytes	416	Bytes by Originator
resp_bytes	858	Bytes by Responder
conn_state	SF	TCP state
local_orig	F	Local Originator?
missed_bytes	0	Gaps
history	ShADafF	State History
tunnel_parents	Cneap78AnVWoA1yml	Outer Tunnel Connection

HTTP

http.log

ts	1393099291.589208
uid	CKFUW73bIADw0r9pl
id.orig_h	2a07:f2c0:90:402:41e:c13:6cb:99c
id.orig_p	54352
id.resp_h	2406:fe60:f47::aaeb:98c
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

Understand Your Network (1)

Top HTTP servers by IP addresses vs host headers.

```
a198-189-255-200.deploy.akamaitechnolgies.com
a198-189-255-216.deploy.akamaitechnolgies.com
a198-189-255-217.deploy.akamaitechnolgies.com
a198-189-255-230.deploy.akamaitechnolgies.com
a198-189-255-225.deploy.akamaitechnolgies.com
a198-189-255-206.deploy.akamaitechnolgies.com
a198-189-255-201.deploy.akamaitechnolgies.com
a198-189-255-223.deploy.akamaitechnolgies.com
                  72.21.91.19
a198-189-255-208.deploy.akamaitechnolgies.com
a198-189-255-207.deploy.akamaitechnolgies.com
          nuq04s07-in-f27.1e100.net
 a184-28-157-55.deploy.akamaitechnologies.com
a198-189-255-224.deploy.akamaitechnolgies.com
a198-189-255-209.deploy.akamaitechnolgies.com
a198-189-255-222.deploy.akamaitechnolgies.com
a198-189-255-214.deploy.akamaitechnolgies.com
          nuq04s06-in-f27.1e100.net
        upload-lb.pmtpa.wikimedia.org
          nuq04s08-in-f27.1e100.net
```

```
          ad.doubleclick.net
          ad.yieldmanager.com
       b.scorecardresearch.com
          clients1.google.com
    googleads.g.doubleclick.net
       graphics8.nytimes.com
             l.yimg.com
liveupdate.symanteclive update.com
          mt0.google.com
       pixel.quantserve.com
       platform.twitter.com
       profile.ak.fbcdn.net
             s0.2mdn.net
  safebrowsing-cache.google.com
       static.ak.fbcdn.net
          swcdn.apple.com
       upload.wikimedia.org
          www.facebook.com
    www.google-analytics.com
          www.google.com
```

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

Internal Protocols

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

radius.log

ts	1392796962.091566
uid	Ci3RM24iF4vIYRGHc3
id.orig_h	10.129.5.11
id.resp_h	10.129.5.1
username	foo@eduroam.mwn.de
mac	f0:34:57:91:11:cd
remote_ip	-
result	success

Bro's Protocol Analyzers

AYIYA	Ident	Rlogin
BitTorrent	Kerberos	Rsh
DCE_RPC	Login	SIP
DHCP	Modbus	SMTP
DNP3	MySQL	SNMP
DNS	NCP	SOCKS
DTLS	NFS	SSH
FTP	NTP	SSL
Finger	NetBIOS	Syslog
GTPv1	PE	Telnet
Gnutella	POP3	Teredo
HTTP	Portmapper	X509
ICMP	Radius	ZIP
IRC	RDP	

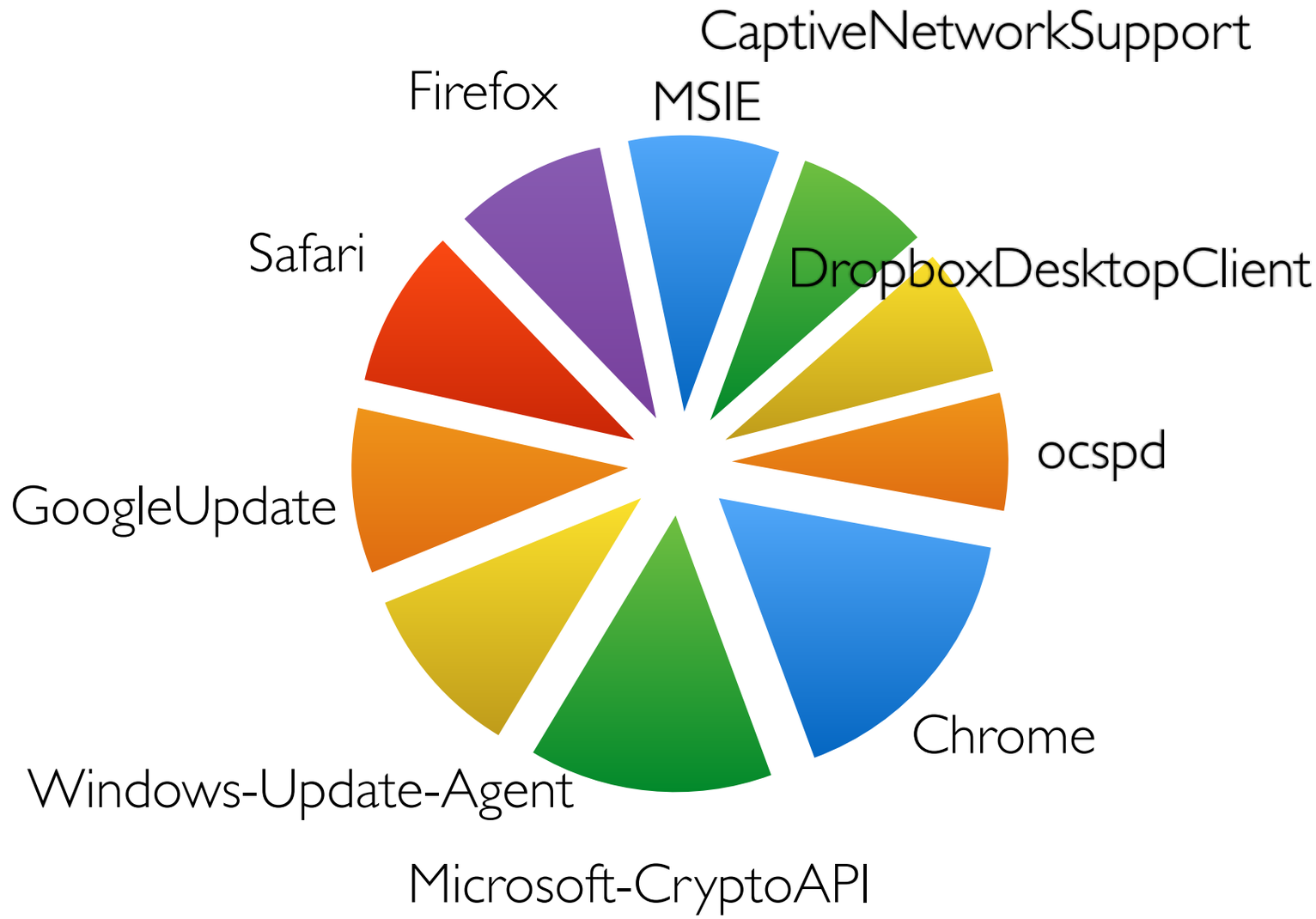
Software

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)

Understand Your Network (2)

Top Software by Number of Hosts



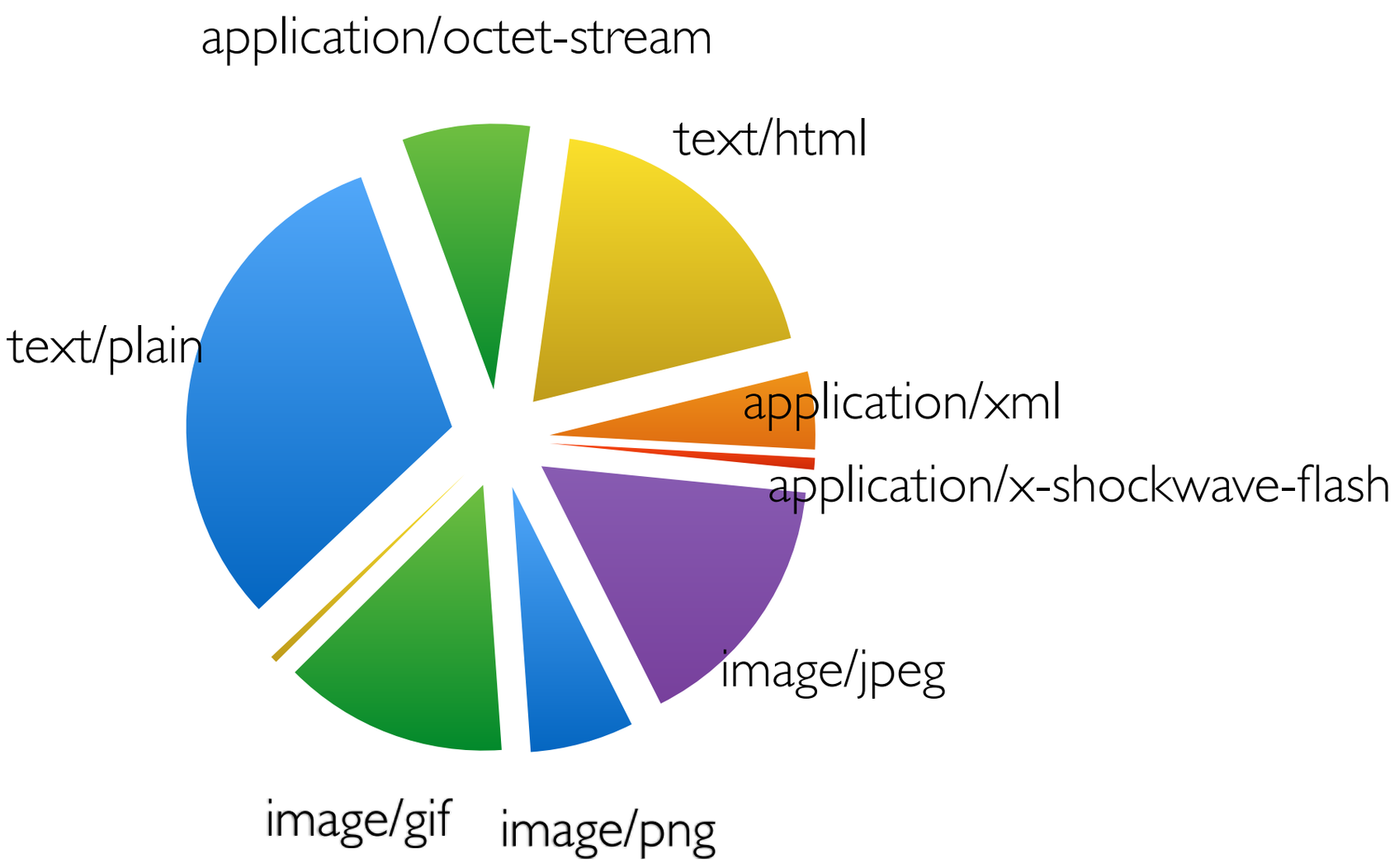
Files

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

Understand Your Network (3)

Top File Types



Volume of Logs & Files

Lawrence Berkeley National Laboratory

About 5,000 users & 15,000 hosts.

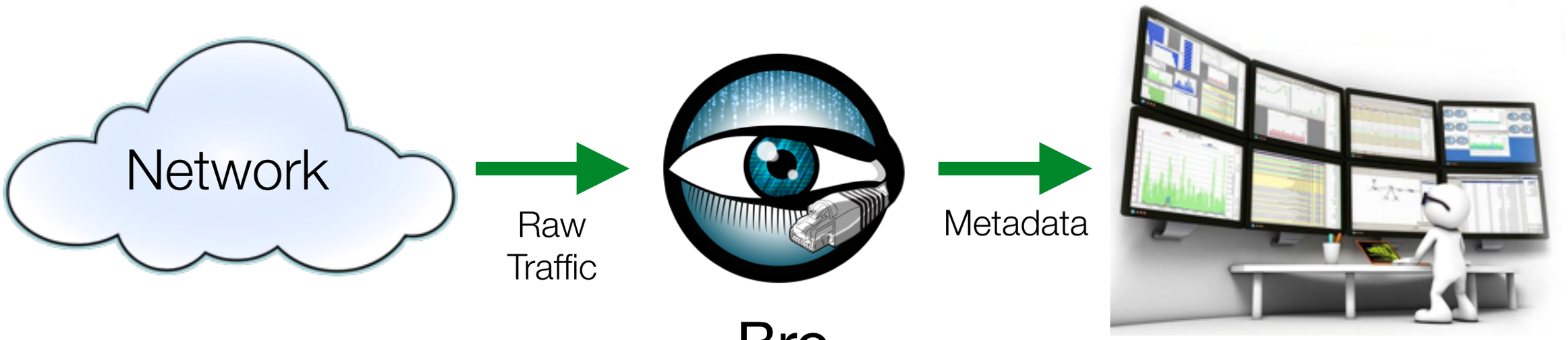
Log entries on a typical weekday in May

`conn.log`	203M
`dns.log`	71M
`http.log`	25M
`x509.log`	5.4M
`files.log`	33M
Extracted files (*)	96K

(*) Includes office docs, executables, PDFs.

Bro's Log Files

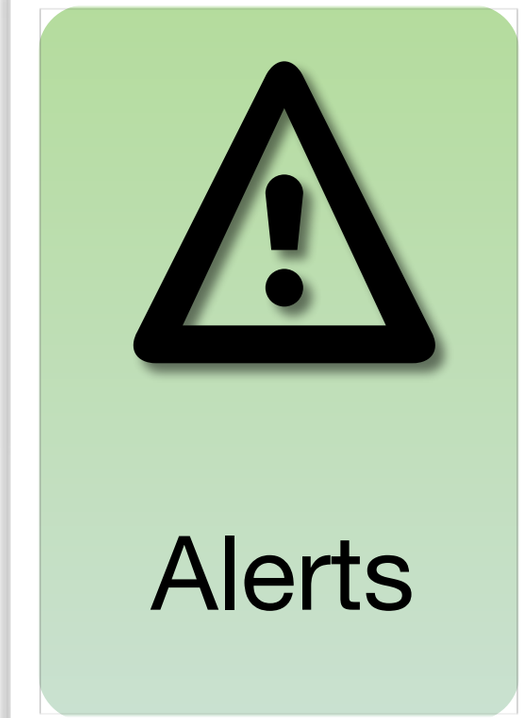
Rich, structured, real-time metadata streams
for incident response & forensics.



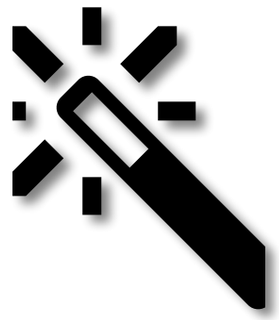
Common use cases: Forensics, hunting, profiling

“What Can It Do?”

Visibility



Alerts



Custom Logic

“Network Ground Truth”

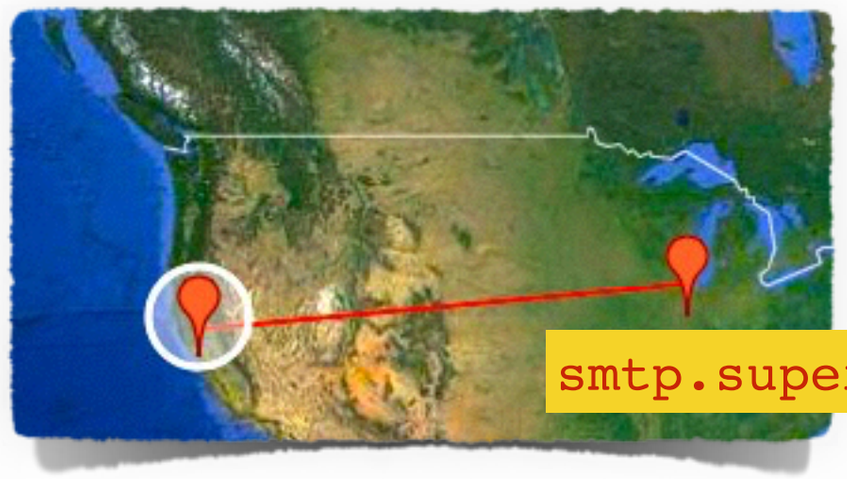
“Watch this!”

Record & trigger actions

Watching for Suspicious Logins

`SSH::Watched_Country_Login`

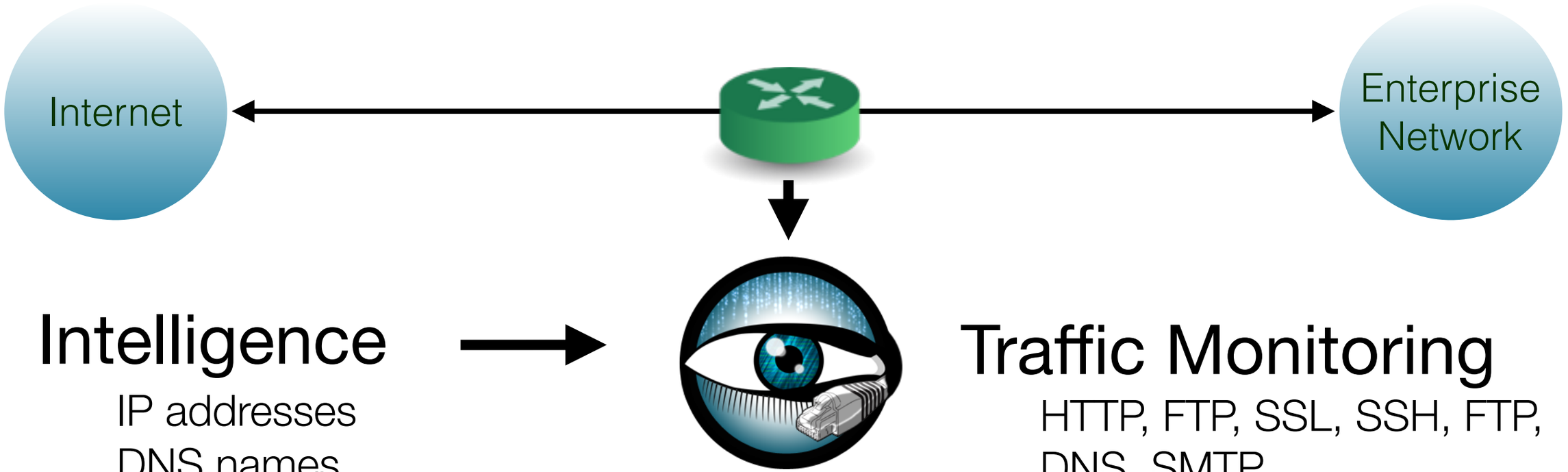
Login from an unexpected country.



`SSH::Interesting_Hostname_Login`

Login from an unusual host name.

Intelligence Integration



Intelligence

IP addresses
DNS names
URLs
File hashes

Feeds

CIF
JC3
Spamhaus
Custom/Proprietary

Traffic Monitoring

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

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

notice.log

Intelligence Integration (Active)

TEAM CYMRU COMMUNITY SERVICES

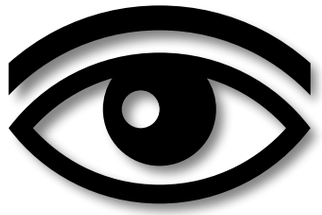
```
# cat files.log | bro-cut mime_type sha1 | awk '$1 ~ /x-dosexec/‘
application/x-dosexec   5fd2f37735953427e2f6c593d6ec7ae882c9ab54
application/x-dosexec   00c69013d34601c2174b72c9249a0063959da93a
application/x-dosexec   0d801726d49377bfe989dcca7753a62549f1ddda
[…]
```

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

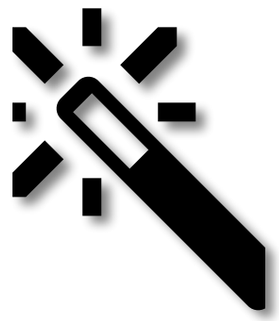
notice.log

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?”



Visibility



Custom Logic

“Watch this!”

Record & trigger actions

*“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 you have seen.

Amendable to extensive customization and extension.

Growing community writing 3rd party scripts.

Mozilla open-sourced >50 Bro scripts on GitHub.

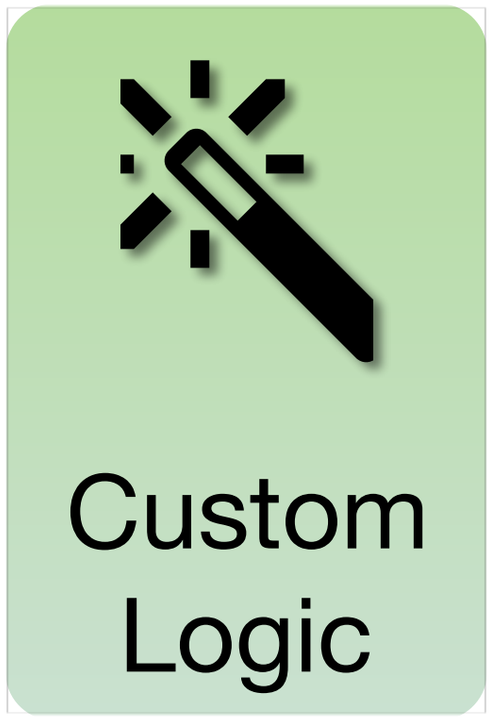
We are developing a community repository.

Like CPAN/PyPI for Bro scripts and plugins, funded by Mozilla.

“What Can It Do?”

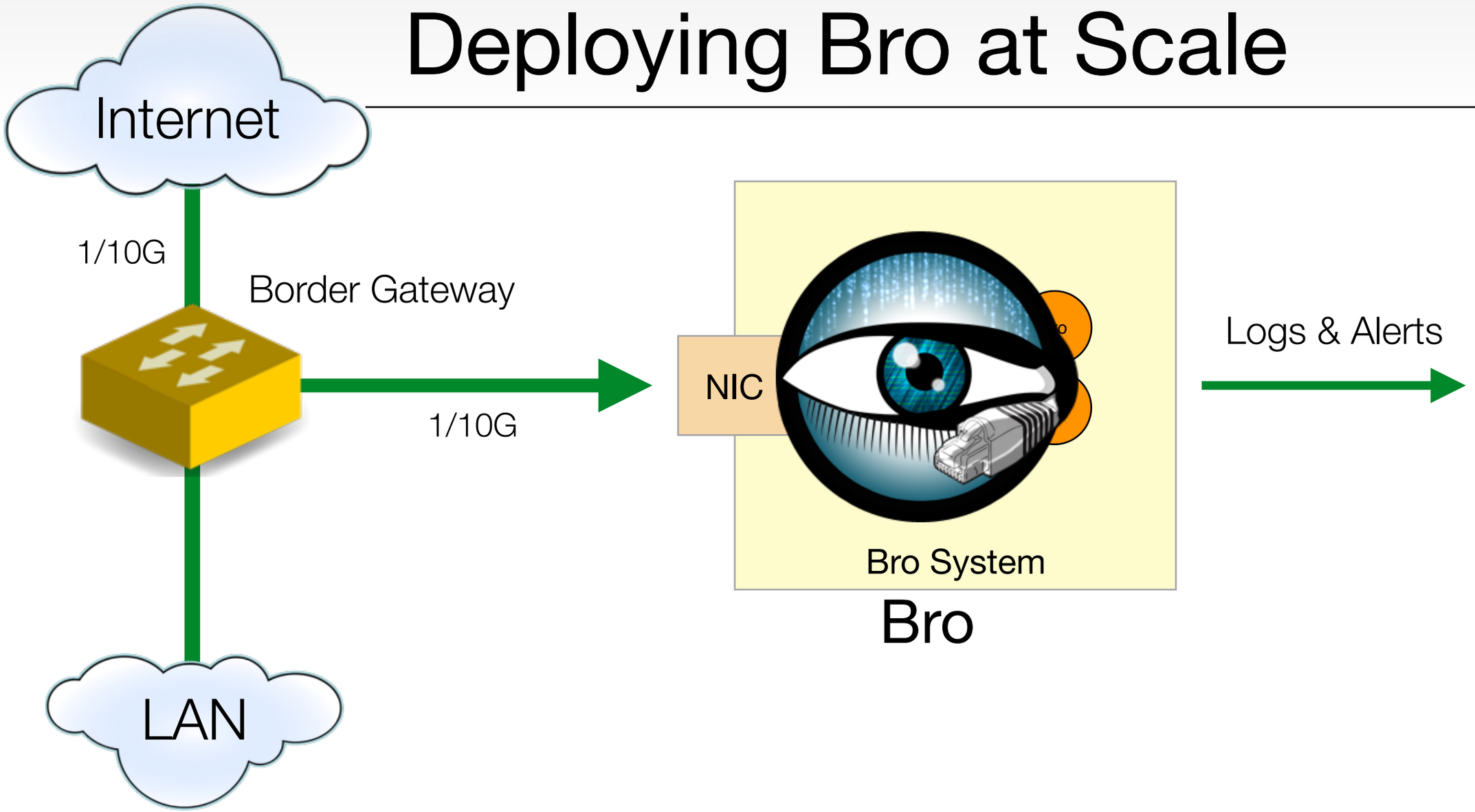
Log Files

Alerts



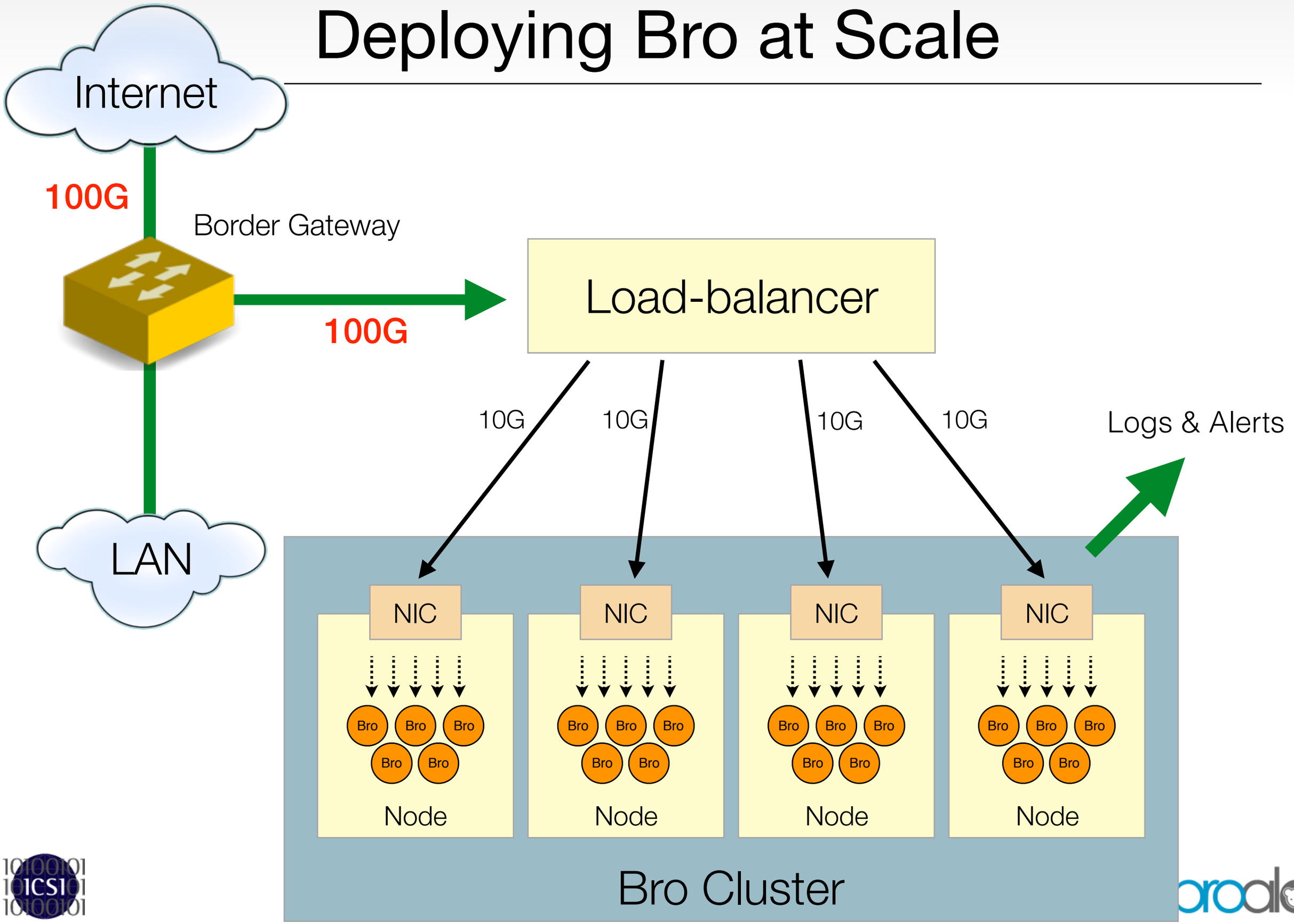
Custom Logic

Deploying Bro at Scale

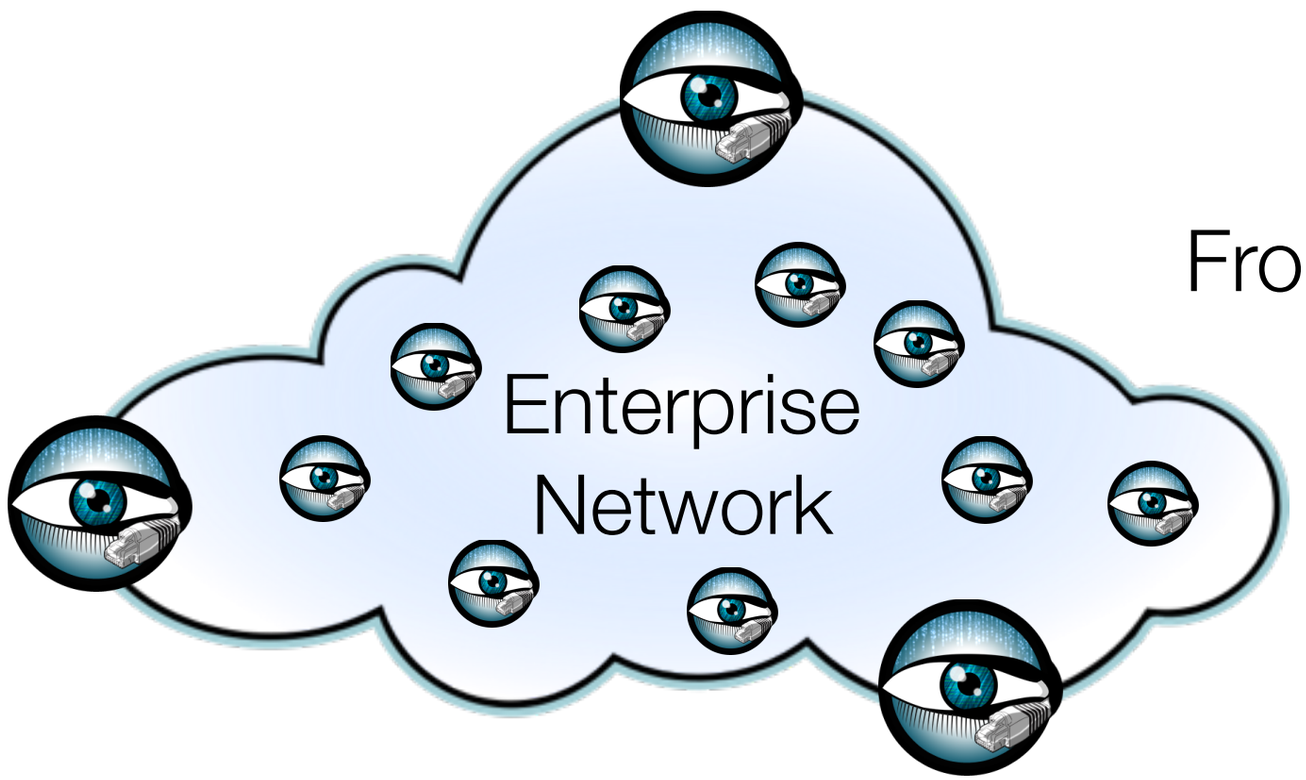


Bro

Deploying Bro at Scale



Monitoring Enterprise Environments

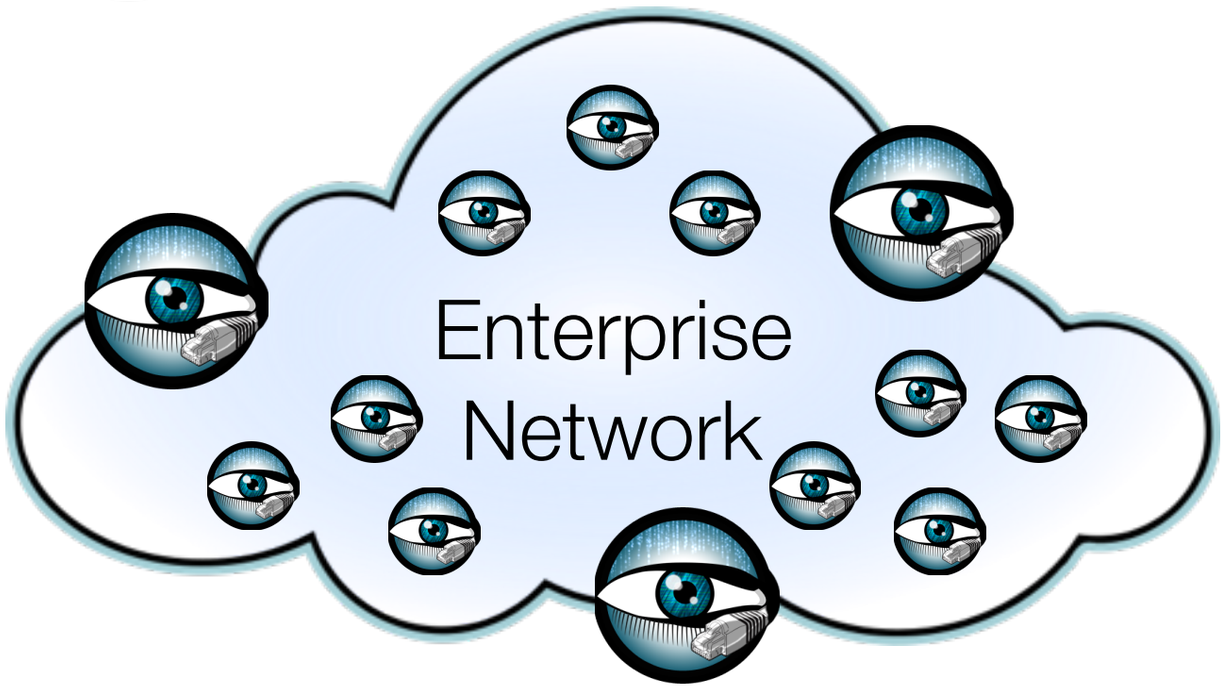


From perimeter to internal.

From standalone to coordinated.

From passive to active.

Bro's open-source roadmap is full of functionality to support all of this.



A Tale of Two Users

Science & Higher Education

Happy to experiment.

Used to open-source software.

Driven by skilled individuals.

Limited funding.

Bro Center of Expertise

Enterprises & Governments

Used to purchasing solutions.

Require reliable point of contact.

Avoid dependence on individuals.

More flexible budgets.

broala

Enterprise-grade Bro solutions, from the creators of Bro.

Commercial Bro support plans.

Fully-supported, turn-key Bro appliances.

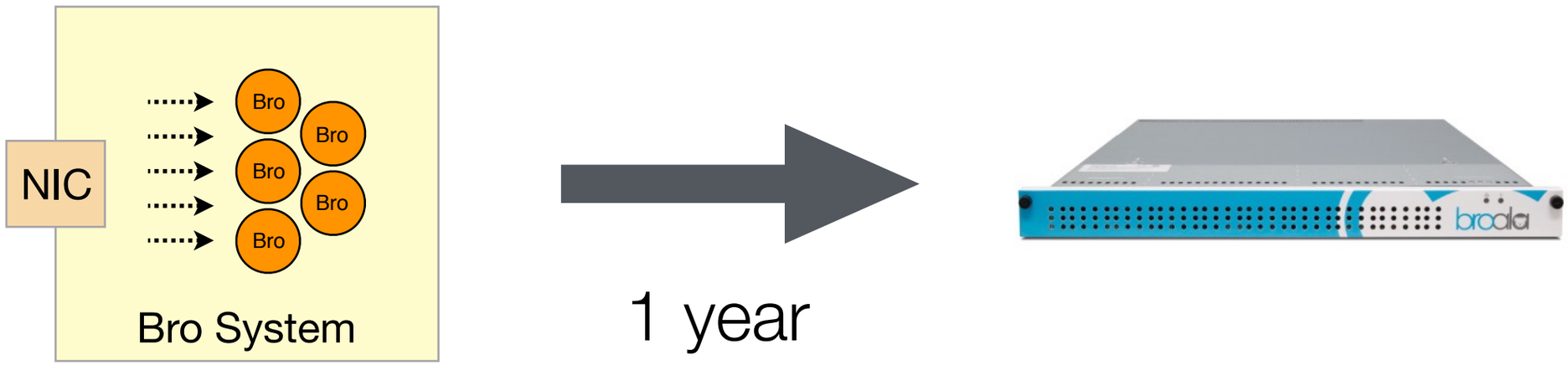
BroBox One

Visibility, made elegantly simple.

- Bro logs and file extraction
- Export data to Kafka, Splunk, Syslog, SFTP
- Engineered for easy of use; setup < 10 mins
- Aggressively tuned for performance & stability
- Custom 4x10G FPGA NIC
- Zero maintenance, ready for the future
- *Soon*: Comprehensive API

Advantage: Integration

With BroBox One we are controlling the full stack.

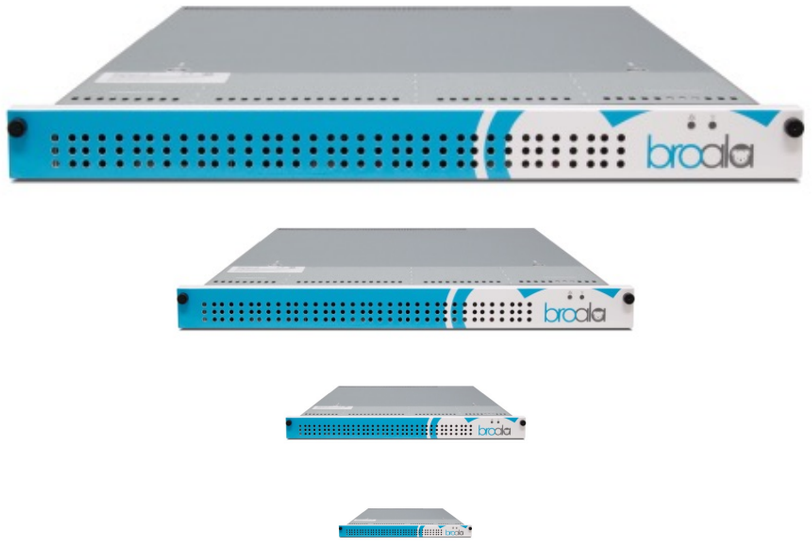


We can take integration much further,
while maintaining the open-source spirit.

Broala's Roadmap

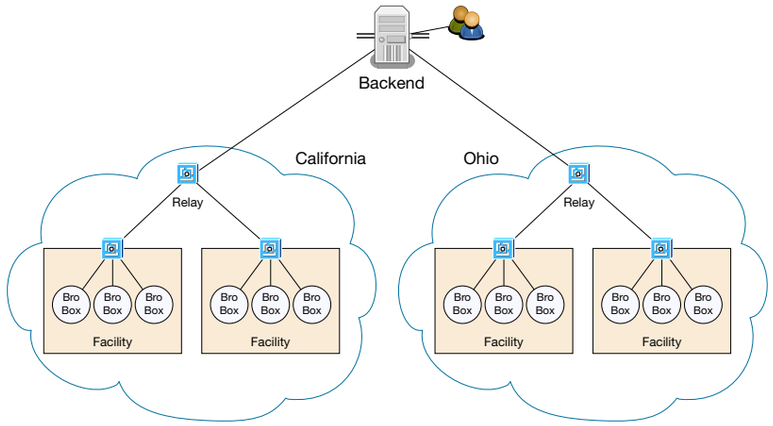
Broala is building a turn-key solution to operate Bro at scale.

Range of BroBox Models



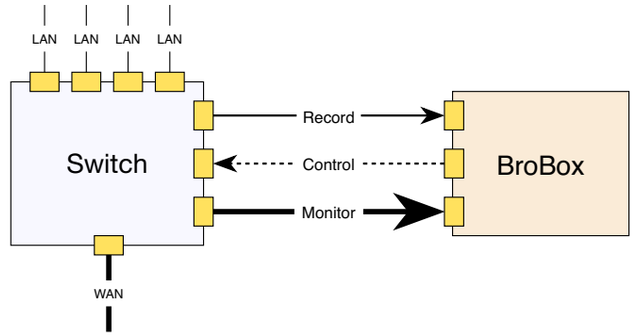
Backbone, data center, offices, factory floor, cloud.

Central Fleet Management



Global aggregation, correlation, & management across 100s of locations.

Active Response



Dynamic firewall.

Join the Bro Community

Broala is just one of many companies leveraging Bro.

Joint goal: A sustainable long-term open-source model.

Software Freedom Conservancy

Fiscal sponsor & neutral 3rd party.

Bro Leadership Team

Steering Committee including community members.

Bro Future Fund

Precious metal sponsorships.

Bro: Open-source Network Monitoring

Versatile

Supports intrusion detection, forensics, vulnerability management, file analysis, traffic measurement, and more.

Efficient

Scales to needs of large networks horizontally and vertically.

Widely adopted

Used by enterprises, cloud providers, universities, financial institutions, government agencies, household brands, national labs, data centers.

Flexible

Customizable & integrates with major enterprise analytics tools.

Out-of-band solution

Passive analysis without performance penalties on production traffic.

Open-source

Very permissive BSD license.

Commercially supported

Broala offers professional Bro solutions by the creators of the system.

The U.S. National Science Foundation has enabled much of Bro.

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

Upcoming Bro Events

August 16 (tentative)	Bro Training at NSF Cybersecurity Summit, VA
Sep 13–15	BroCon 2016, Austin, TX

We are hiring!

The Bro Project
www.bro.org
info@bro.org
@Bro_IDS

Commercial Bro Solutions
www.broala.com
info@broala.com
@Broala_