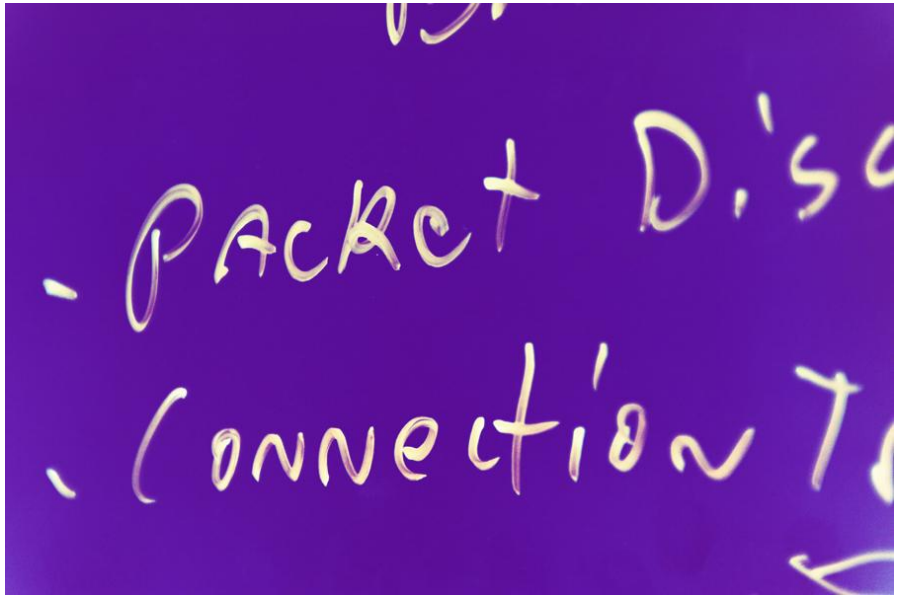
Scalable Protocol-Based Packet Inspection for Advanced Network Threat Detection



Reservoir Labs
632 Broadway, Suite 803
New York, New York 10012
(212) 780-0527
http://www.reservoir.com

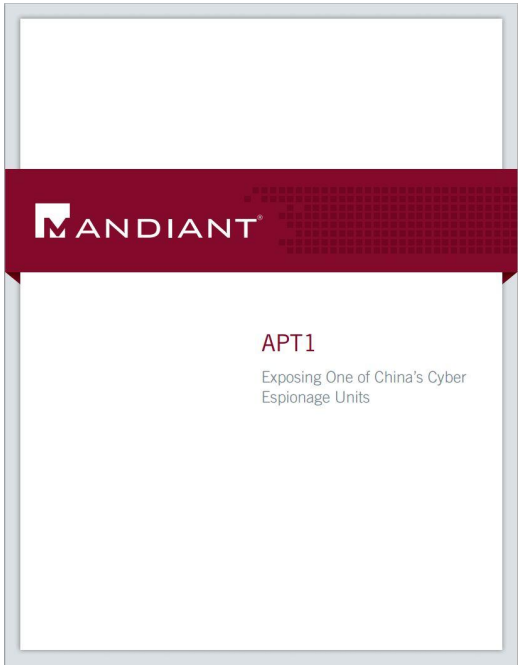
J. Giralt, A. Commike,
R. Rotsted, R. Lethin

giralt@reservoir.com
commike@reservoir.com
rotsted@reservoir.com
lethin@reservoir.com

Abstract

Protocol-based packet inspection systems provide a means for advanced threat detection that can complement traditional string matching IDS. These systems execute analytics written in cybersecurity domain-specific programming languages and in terms of protocol elements, and this allows for agile detection of attack behaviors that cannot be captured with string matching IDS. We will provide a quick tutorial on protocol-based packet inspection systems and their benefits for cyber security, and describe a system called R-Scope(R) that extends the open source Bro network security monitor with new analytics and that can employ advanced network processing electronics. R-Scope allows network security engineers to provide protection from evolving threats and at high network traffic rates. R-Scope is the result of Small Business Innovative Research (SBIR) performed by Reservoir Labs for the US DOE, with current installation and experimentation in DOE.

The Motivation



Office of Science and Technology Policy
Executive Office of the President
New Executive Office Building
Washington, DC 20502

FOR IMMEDIATE RELEASE
March 29, 2012

Contact: Rick Weiss 202 456-6037 rweiss@ostp.eop.gov
Lisa-Joy Zgorski 703 292-8311 lisajoy@nsf.gov

OBAMA ADMINISTRATION UNVEILS "BIG DATA" INITIATIVE: ANNOUNCES $200 MILLION IN NEW R&D INVESTMENTS

Aiming to make the most of the fast-growing volume of digital data, the Obama Administration today announced a "Big Data Research and Development Initiative." By improving our ability to extract knowledge and insights from large and complex collections of digital data, the initiative promises to help solve some the Nation's most pressing challenges.

Cyber threats/defense rapidly growing

- Border threats to inside the network defense
- Persistent threats
- Adaptive defenses

Big Data implies Big Network

- 100 Gbps networks in deployment
- 1 Tbps networks being designed
- Full forensic packet capture infeasible

Needed:
Powerful, High-Speed, Advanced Network Monitoring

Shift to Exploration-Driven Security

Alert-driven	**Exploration-driven**
Incident DETECTION	Incident DISCOVERY
Alert comes in -> you respond	You go out -> you find actionable info -> you act
Like tech support	Like QA
Response	"Hunting"
Alert-centric	Question-centric
Context to decide on the alert	Context to explore wider/deeper
Drill-down	Drill-sideways
Triage THIS entity	Explore in THIS direction
Want to be "done" with the alert	Want to know what is really going on
Operations - alert volume	Research - insight usefulness

Source: Anton Chuvakin, "Alert-driven vs. Exploration-driven Security Analysis, Gartner
http://blogs.gartner.com/anton-chuvakin/2013/05/20/alert-driven-vs-exploration-driven-security-analysis/

http://www.bro.org

http://www.bro.org/

The Bro Network Security ...

Home | Downloads | Documentation | Support | Community | Development | Research | Contact | Site Map

The Bro Network Security Monitor

Bro is a powerful network analysis framework that is much different from the typical IDS you may know.

Adaptable
Bro's domain-specific scripting language enables site-specific monitoring policies.

Efficient
Bro targets high-performance networks and is used operationally at a variety of large sites.

Flexible
Bro is not restricted to any particular detection approach and does not rely on traditional signatures.

Forensics
Bro comprehensively logs what it sees and provides a high-level archive of a network's activity.

In-depth Analysis
Bro comes with analyzers for many protocols, enabling high-level semantic analysis at the application layer.

Highly Stateful
Bro keeps extensive application-layer state about the network it monitors.

Open Interfaces
Bro interfaces with other applications for real-time exchange of information.

Open Source
Bro comes with a BSD license, allowing for free use with virtually no restrictions.

SEARCH

Search

EVENTS

No events scheduled currently.

See past events.

BLOG

Using ICSI's Open-Source Bro Platform to Protect the Blue Waters Supercomputer
Friday, April 26, 2013

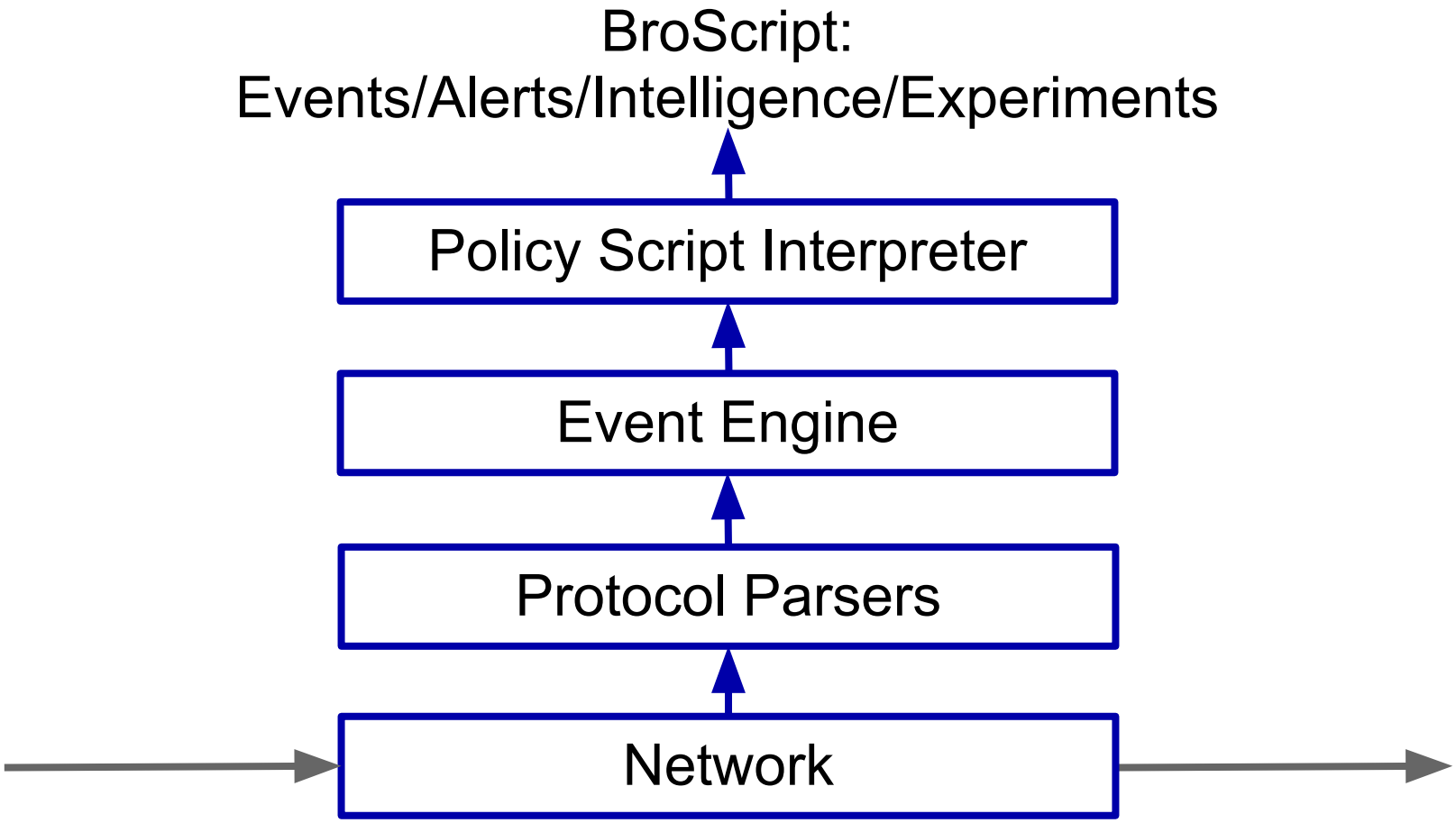
bro.org — A New Home for Bro
Thursday, March 07, 2013

Watching for the APT1 Intelligence
Friday, February 22, 2013

Bro Summer Internship Available
Tuesday, January 22, 2013

Searching the ICSI Notary for Rogue Turktrust Intermediate Certificates
Friday, January 04, 2013

Bro Architecture



Protocol-Based Analytics

RFC 2616: HTTP

```
Network Working Group
Request for Comments: 2616
Obsoletes: 2068
Category: Standards Track

        Hypertext Transfer Protocol -- HTTP/1.1
(...)

5 Request

(...)
    Request =   Request-Line                ; Section 5.1
                *(( general-header          ; Section 4.5
                | request-header            ; Section 5.3
                | entity-header ) CRLF)     ; Section 7.1
                CRLF
                [ message-body ]            ; Section 4.3

5.1 Request-Line

(...)
    Request-Line  = Method SP Request-URI SP HTTP-Version CRLF

5.1.1 Method

(...)
    Method = "OPTIONS"      ; Section 9.2
           | "GET"          ; Section 9.3
           | "HEAD"         ; Section 9.4
           | "POST"         ; Section 9.5
           | "PUT"          ; Section 9.6
           | "DELETE"       ; Section 9.7
           | "TRACE"        ; Section 9.8
           | "CONNECT"      ; Section 9.9
           | extension-method
    extension-method = token
```

Bro Protocol Language

```
(...)

type HTTP_TOKEN = RE/[^()<>@,;:\"\/[\]?={} \t]+/;
type HTTP_METHOD        = RE/(OPTIONS|GET|HEAD|POST|
                          PUT|DELETE|TRACE|CONNECT)/
type HTTP_WS            = RE/[ \t]*/;
type HTTP_URI           = RE/[^ ]+/;

type HTTP_RequestLine = record {
  method:       HTTP_METHOD;
:               HTTP_WS;
  uri:          HTTP_URI;
:               HTTP_WS;
  version: HTTP_Version;
} &oneline;

type HTTP_Version = record {
:               "HTTP/";
  vers_str: RE/[0-9]+\.[0-9]+/;
} &let {
  vers_num: double = bytestring_to_double(vers_str);
};

(...)
```

Bro Script

```
global conn_info: table[conn_id] of http_session_info
        &read_expire=5mins
        &redef;
event http_request(c: connection, method: string,
                   original_URI: string,
                   unescaped_URI: string, version: string)
        {
        if ( c$id !in conn_info )
                {
                local x: http_session_info;
                conn_info[c$id] = x;
                }

        local sess_ext = conn_info[c$id];
        sess_ext$method = method;
        sess_ext$uri = unescaped_URI;

        }
event http_reply(c: connection, version: string,
                 code: count, reason: string)
        {
        local this_timestamp: time;
        local this_sel_cap: double;
        local id = c$id;
        if ( id !in conn_info )
                return;
```

- Semantic Signatures (Protocol & Analytics)
- Stateful Domain Specific Language (DSL)
- Open Source, funded by DOE, active community
- Extensible and flexible
- Agile rapid response to catch immediate threats
- Exploration, apply new filters from intelligence

Signature vs. Protocol-Based

Snort

```
alert tcp any any -> 192.168.1.0/24 111
(content:"|00 01 86 a5|"; msg: "mountd
access";)
```

Bro

```
event http_all_headers(
  c: connection,
  is_orig: bool,
  hlist: mime_header_list)
{
  /* A highly simplified version of
     Bro's sidejacking analytic */
  cookie = c$http$cookie;
  local ctx = cookies[cookie];
  if (client != ctx$client)
     report_sidejacking(c, ctx);
}
```

Signature vs. Protocol-Based

Snort

```
alert tcp any any -> 192.168.1.0/24 111
(content:"|00 01 86 a5|"; msg: "mountd
access";)
```

matching regex

Bro

```
event http_all_headers(
  c: connection,
  is_orig: bool,
  hlist: mime_header_list)
{
  /* A highly simplified version of
     Bro's sidejacking analytic */
  cookie = c$http$cookie;
  local ctx = cookies[cookie];
  if (client != ctx$client)
     report_sidejacking(c, ctx);
}
```

Signature vs. Protocol-Based

Snort

```
alert tcp any any -> 192.168.1.0/24 111
(content:"|00 01 86 a5|"; msg: "mountd
access";)
```

Bro

event triggered natively

```
event http_all_headers(
  c: connection,
  is_orig: bool,
  hlist: mime_header_list)
{
  /* A highly simplified version of
     Bro's sidejacking analytic */
  cookie = c$http$cookie;
  local ctx = cookies[cookie];
  if (client != ctx$client)
     report_sidejacking(c, ctx);
}
```

network object semantics

full state; event correlation algorithms are possible

Some Bro Users

Labs

US DOE, Lawrence Berkeley National Labs
National Energy Research Scientific Computing Center (NERSC)
National Center for Supercomputer Applications (NCSA, Blue Waters)
Texas Advanced Computing Center (TACC), ...

Government

Boulder County
...

Commercial

BBN
Ultra Electronics 3eTI
XeniMax Media, ...

Universities

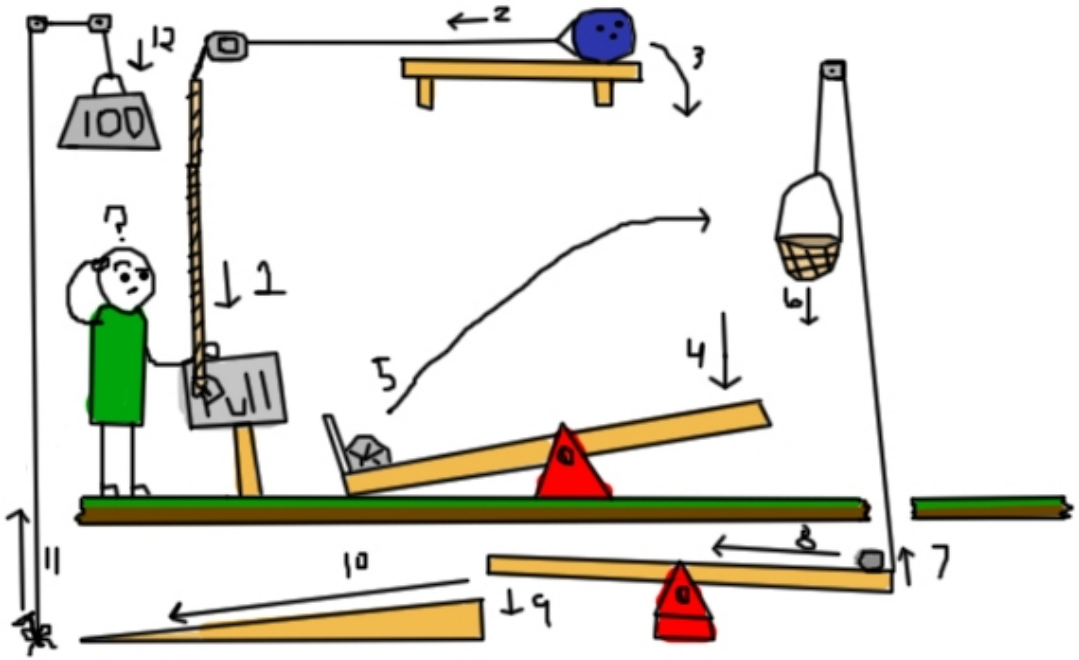
SUNY Albany, CMU, UT Dallas
University Wisconsin, UC Boulder
Medical University of South Carolina
University Utah,...

Source: Bro mailing list

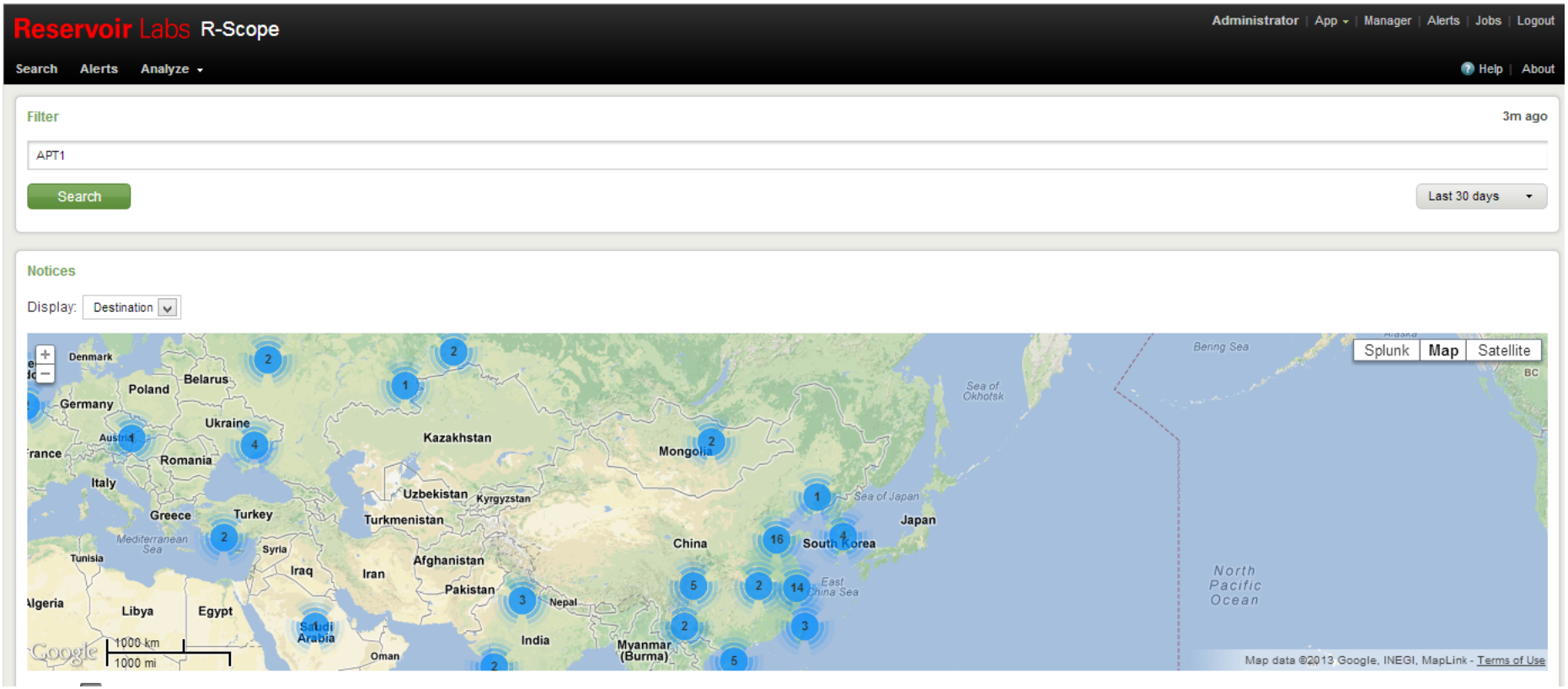
Bro Network Security Monitor

Open Source Software

1. Git Download
2. Compile
3. Choose HW
4. Choose NIC
5. Configure
6. Tune
7. Goto 1

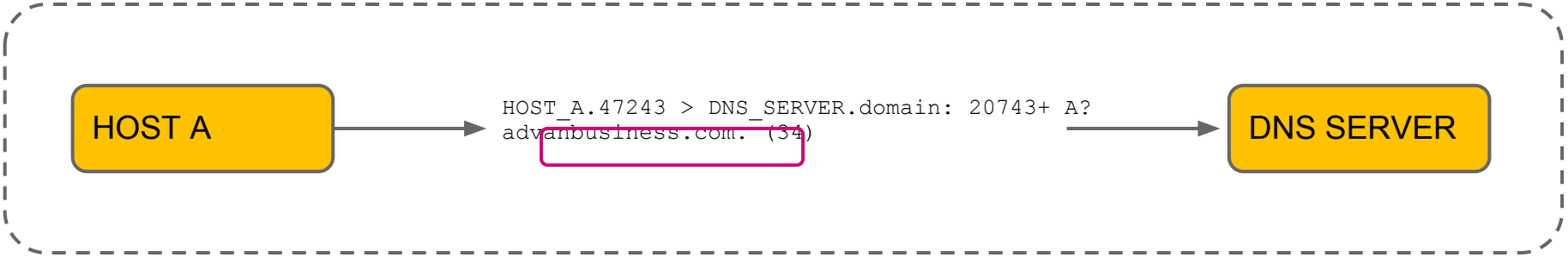


APT1 Intelligence Detection



APT1 Intelligence Detection

Network Monitored by Bro



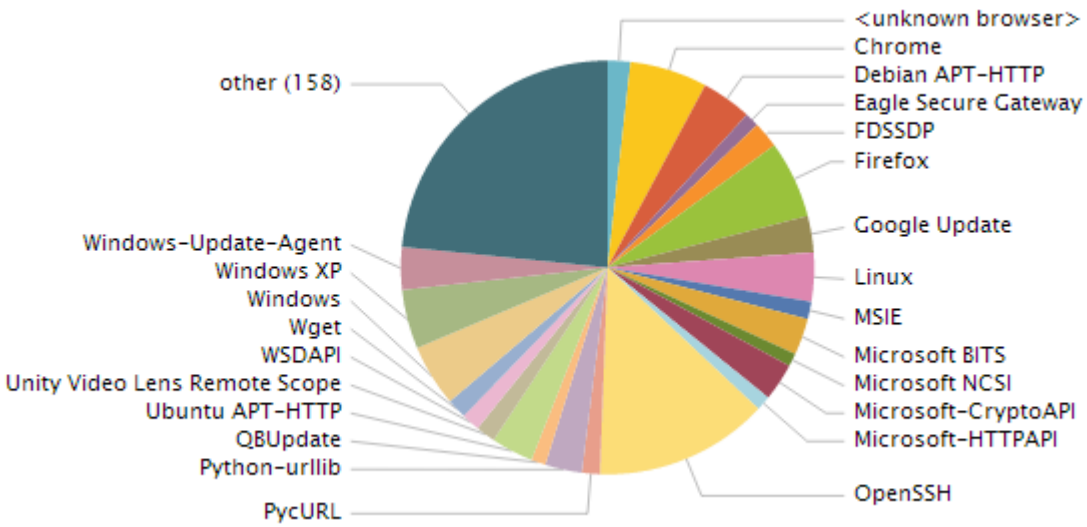
Bro Policy Script

```
event dns_request(c: connection, msg: dns_msg, query: string, qtype: count, qclass:
count)
        {
        if (query in APT1::domains)
                {
                NOTICE([$note=APT1::Domain_Hit,
                        $conn=c,
                        $msg=fmt("A domain from the APT1 report seen: %s", query),
                        $identifier=cat(query)]);
                }
        }
```

```
const apt1_domains: set[string] = {
        "advanbusiness.com",
        "aoldaily.com",
        "aolon1ine.com",
        "applesoftupdate.com",
        "arrowservice.net",
        "attnpower.com",
        "aunewsonline.com",
        "avvmail.com",
        "bigdepression.net",
}
```

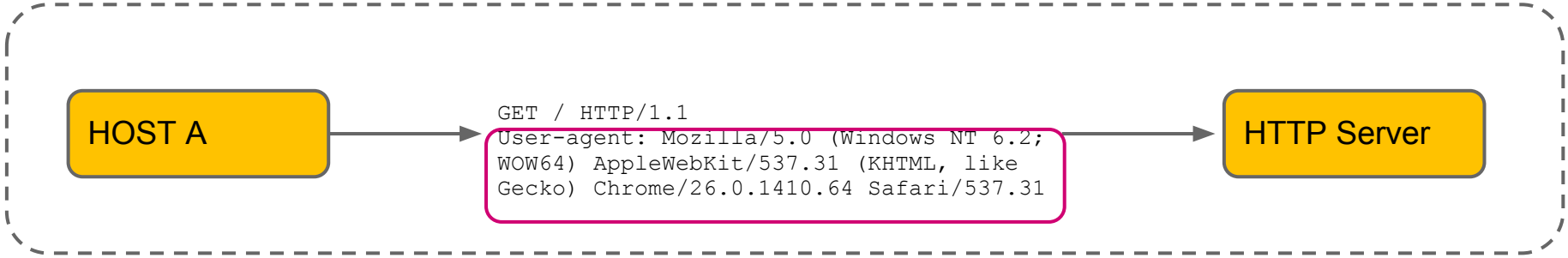
Software Detection

- Software often leaks information that identifies its name and version:
  - User-agent Strings :
    `Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.31 (KHTML, like Gecko) Chrome/26.0.1410.64 Safari/537.31`
  - Protocol Banners :
    `SSH-2.0-OpenSSH_5.9p1 Debian-5ubuntu1.1`



Software Detection

Network Monitored by Bro



"HTTP Software" Bro Policy Script

```
event http_header(c: connection, is_orig: bool, name: string, value: string) &priority=2
        {
        if ( is_orig )
                {
                if ( name == "USER-AGENT" && ignored_user_agents !in value )
                        Software::found(c$id, [$unparsed_version=value, $host=c$id$orig_h, $software_type=BROWSER]);
                }
        }
```

R-Scope App: Software Detection

Filter

java

Search

Last 30 days

Hosts/Ports

Source Address

« prev 1 2 next »

	src	count	percent
1	10.1.1.211	10	40.000000
2	10.1.1.210	3	12.000000
3	10.1.1.245	2	8.000000

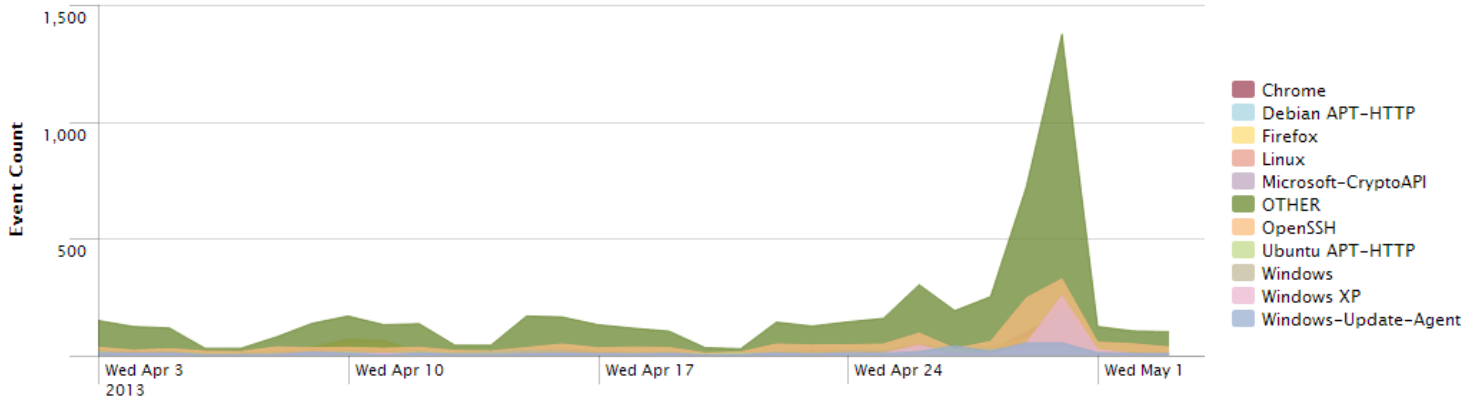
Protocol Attributes

unparsed_version

	unparsed_version	count	percent
1	JNLP/1.7.0 javaws/10.17.2.02 (<internal>) Java/1.7.0_17	10	40.000000
2	JNLP/1.7.0 javaws/10.21.2.11 (<internal>) Java/1.7.0_21	8	32.000000
3	Java/1.6.0_19	2	8.000000
4	Java/Java 7 Update 11 Sparkle/313	1	4.000000

Timecharts

Sessions by name



R-Scope App: Software Detection

10.1.1.60:8000/en-US/app/rscope-apps-2.0/software

Reservoir Labs R-Scope

Administrator | App | Manager | Alerts | Jobs | Logout

Search Alerts Analyze

Help | About

Filter

Search

Last 30 days

Hosts/Ports

Source Address

« prev 1 2 3 4 5 6 7 8 9 10 next »

	src	count	percent
1	10.1.1.211	923	7.697440
2	10.1.1.222	912	7.605704
3	10.1.1.251	889	7.413894
4	10.1.1.210	533	4.445000
5	10.1.1.60	417	3.477608
6	10.1.1.47	413	3.444250
7	10.1.1.3	404	3.369194
8	10.1.1.23	399	3.327496
9	10.1.1.205	371	3.093987
10	10.1.1.22	349	2.910516

Protocol Attributes

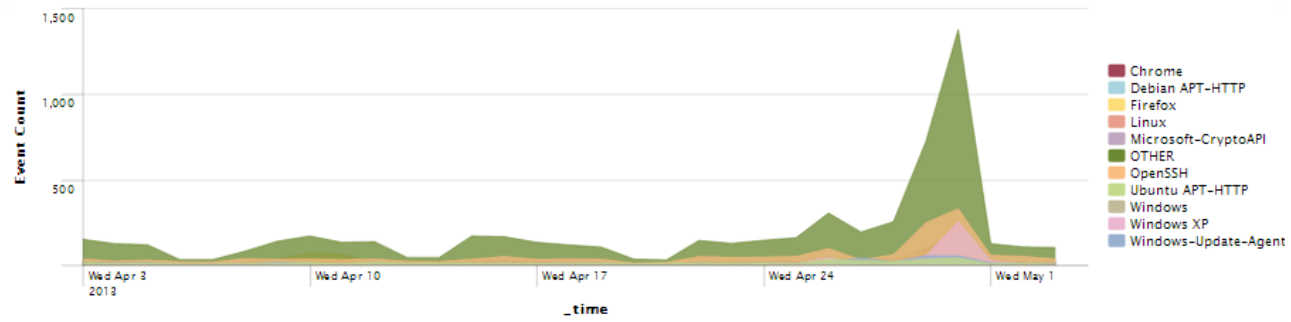
name

« prev 1 2 3 4 5 6 7 8 9 10 next »

	name	count	percent
1	OpenSSH	1638	13.660245
2	Chrome	730	6.087899
3	Firefox	726	6.054541
4	Windows	579	4.828621
5	Windows XP	554	4.620132
6	Debian APT-HTTP	470	3.919606
7	Linux	460	3.836210
8	Windows-Update-Agent	397	3.310816
9	Ubuntu APT-HTTP	394	3.285798
10	Microsoft-CryptoAPI	352	2.935535

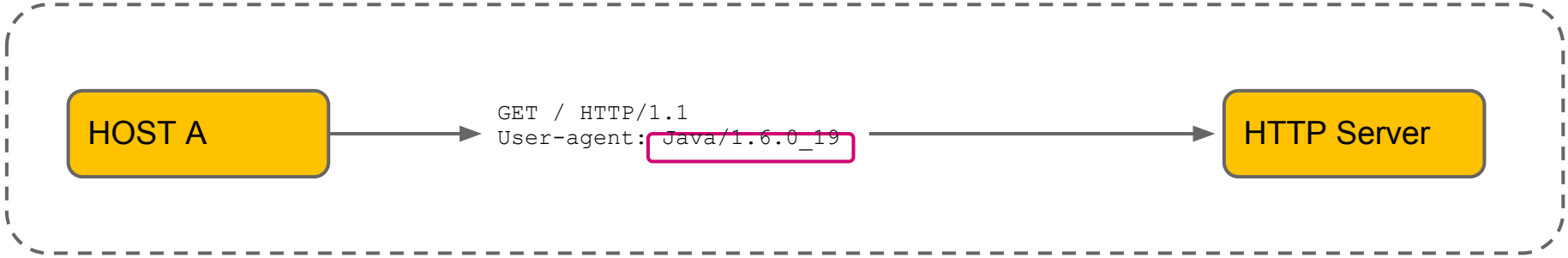
Timecharts

Sessions by name



Vulnerable Software Detection

Network Monitored by Bro



"Vulnerable Versions"
Bro Policy Script

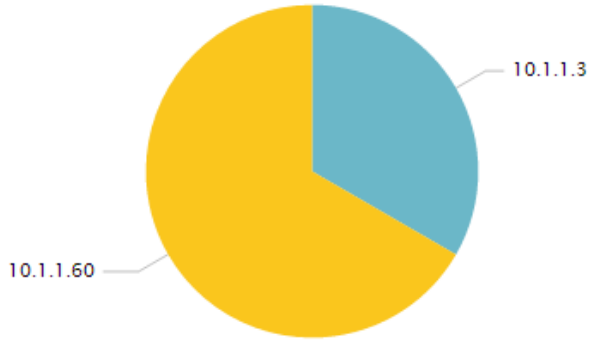
```
event log_software(rec: Info)
{
  if ( rec$name in vulnerable_versions &&
          cmp_versions(rec$version, vulnerable_versions[rec$name]) <= 0 )
              {
              NOTICE([$note=Vulnerable_Version, $src=rec$host,
                  $msg=fmt("A vulnerable version of software was detected: %s",
software_fmt(rec))]);
              }
        }
```

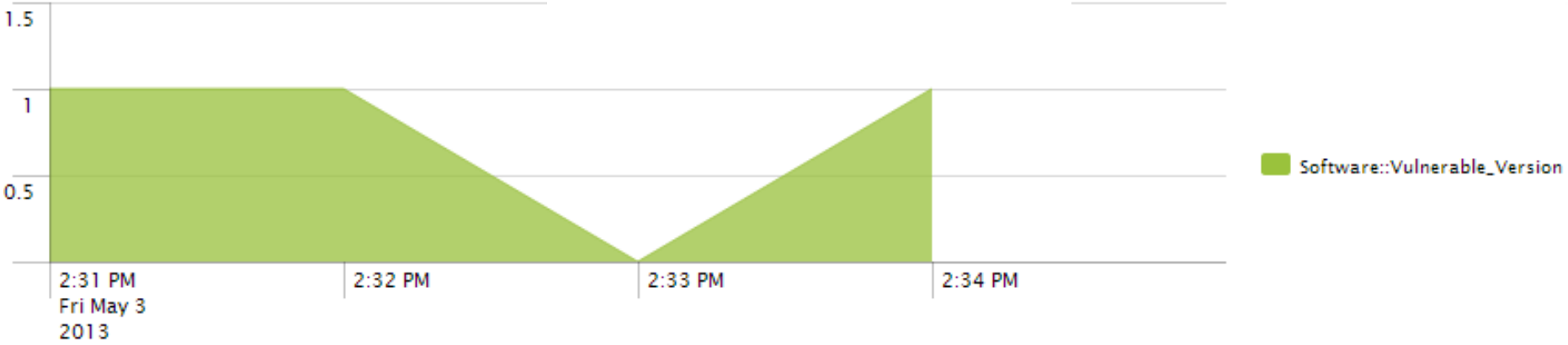
"Vulnerable Versions" Table
(Mined from NIST's NVD)

```
redef Software::vulnerable_versions += {

["Java"] =
[$major=1,$minor=6,$minor2=0,$addl="22"],

};
```

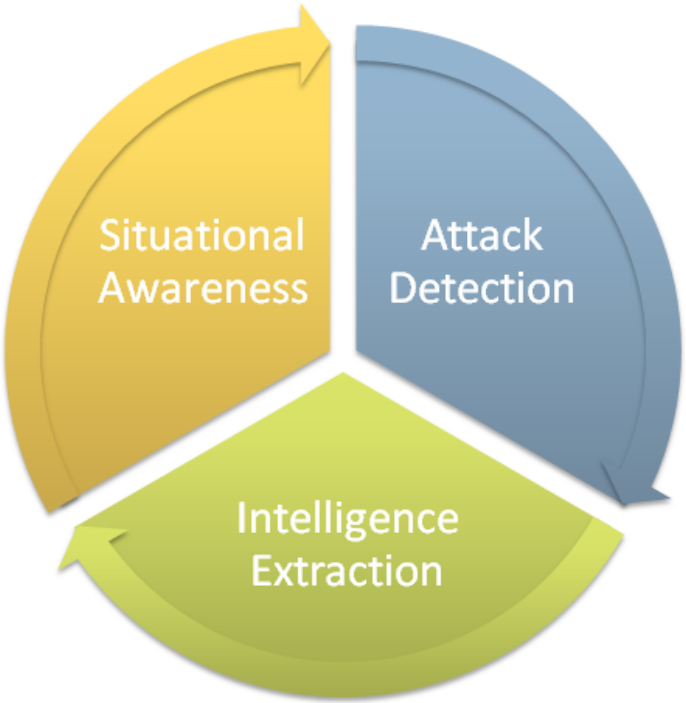
Vulnerable Software Detection Powered by NIST

	_time	id_orig_h	id_resp_h	note	msg
1	5/3/13 2:34:53.162 PM	10.1.1.3	NULL	Software::Vulnerable_Version	A vulnerable version of software was detected: Firefox 9.1.0
2	5/3/13 2:32:23.503 PM	10.1.1.60	NULL	Software::Vulnerable_Version	A vulnerable version of software was detected: Firefox 3.0.0
3	5/3/13 2:31:56.045 PM	10.1.1.60	NULL	Software::Vulnerable_Version	A vulnerable version of software was detected: Java 1.6.0-19





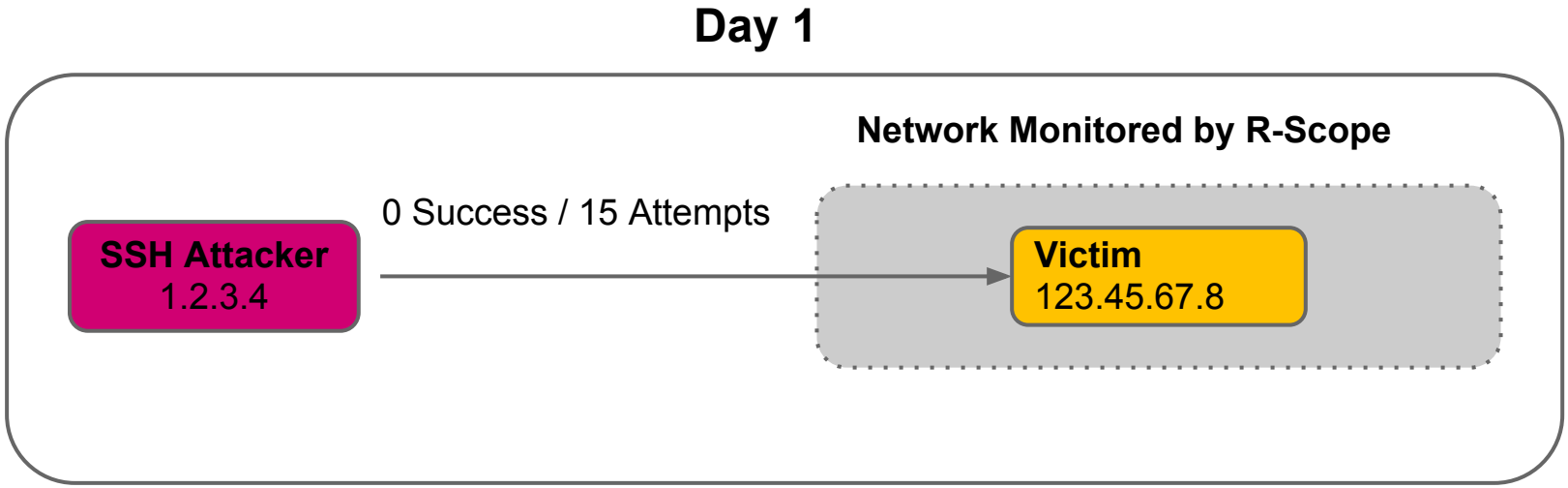
Adaptive Defense



Threat Intelligence Workflow

Apply filters derived from intelligence

Example Analytic: Persistent SSH Attacker Detection

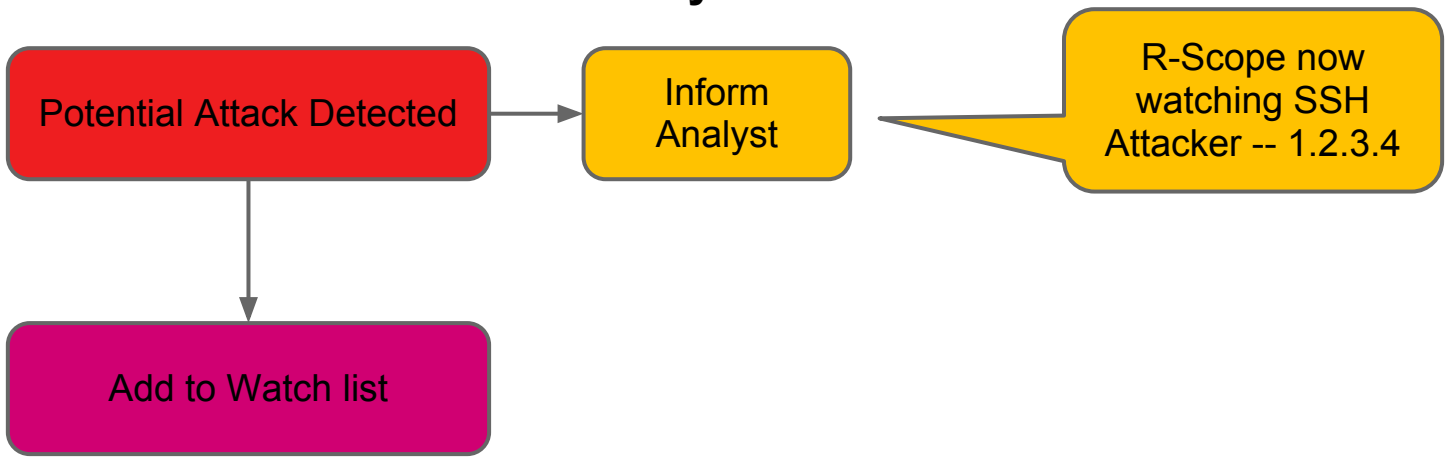


The Persistent Attacker analytic detects SSH attackers who attack over a series of days. This method of detection highlights:

- Attackers targeting your organization
- Attackers attempting to evade traditional detection techniques (attempts / day thresholds)

Example Analytic: Persistent SSH Attacker Detection

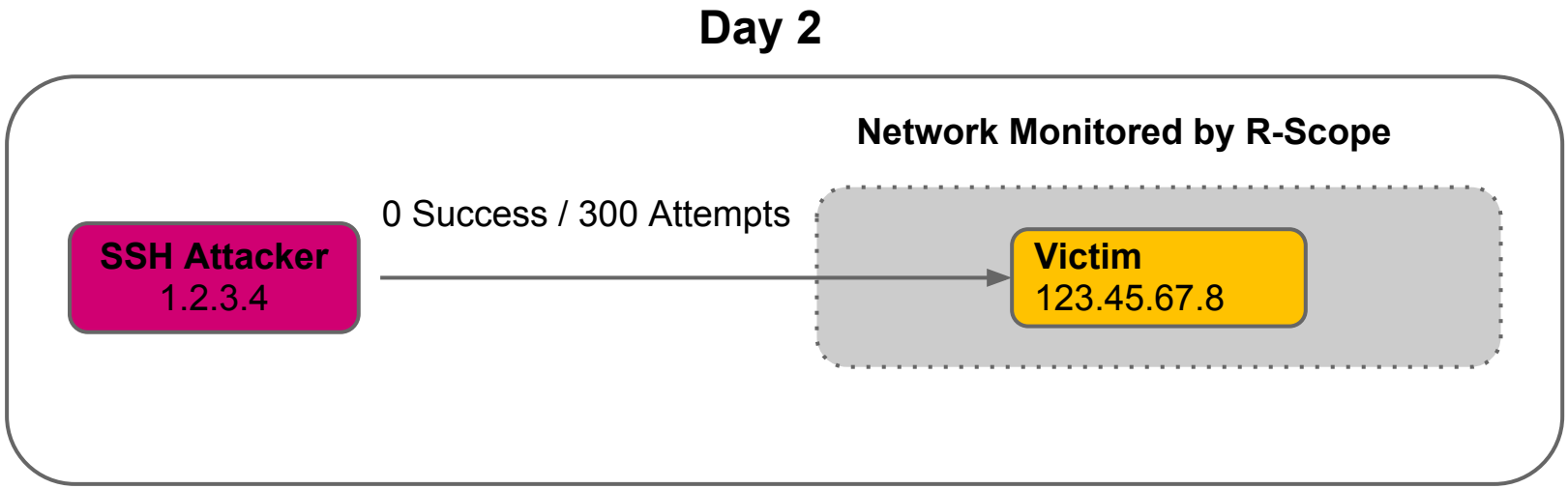
Day 1



Watched Hosts	Failed Logins / Login Attempt	Days Attacking
1.2.3.4	0.0%	1

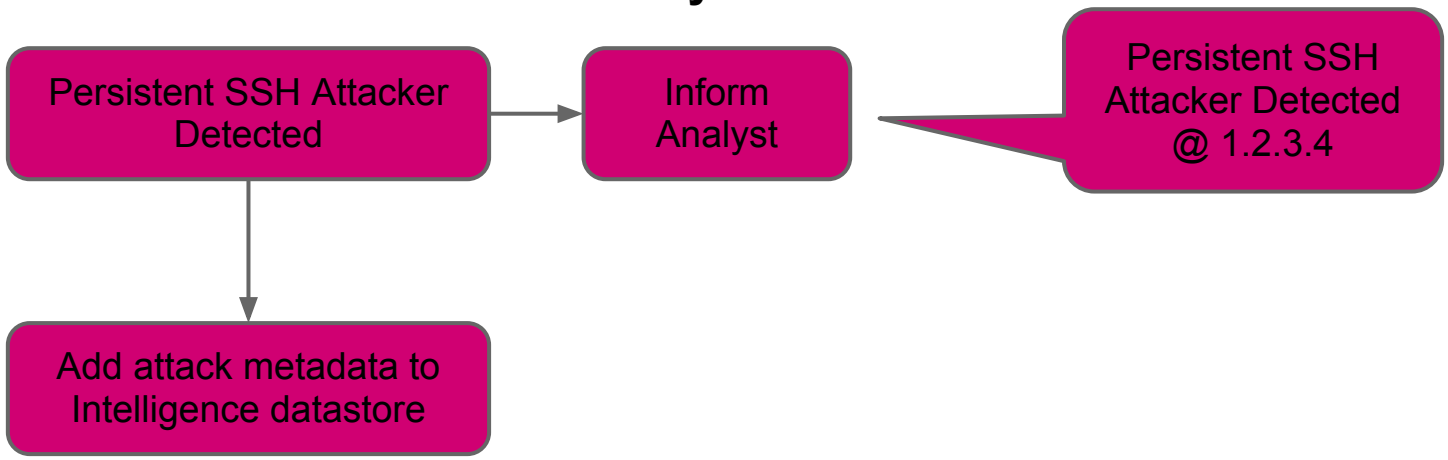
Attacking Days Threshold = 2 days **Successful Login Threshold** = 30 %

Example Analytic: Persistent SSH Attacker Detection



Example Analytic: Persistent SSH Attacker Detection

Day 2



Watched Hosts	Failed Logins / Login Attempt	Days Attacking
1.2.3.4	0.0%	2

Attacking Days Threshold = 2 days **Successful Login Threshold** = 30 %

Bro Use Cases

APT reconnaissance

Exfiltration detection

Adaptive defense

Hunting / experimentation/ exploration

Continuous control monitoring

Integration with external threat intelligence sources

Defenses against polymorphic attacks

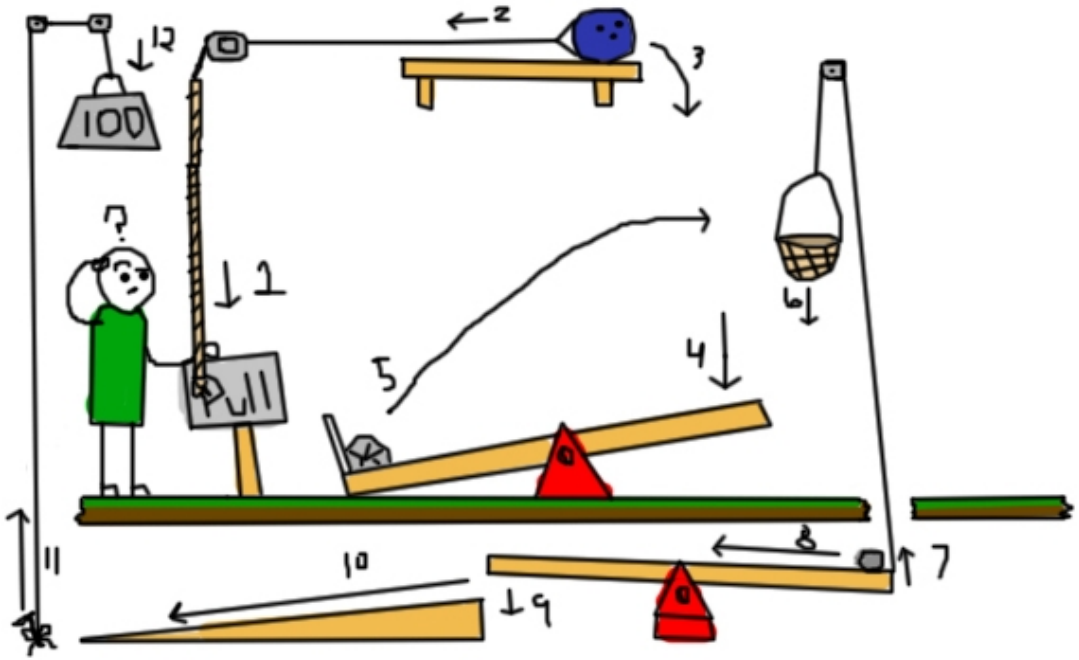
Internal policy validation

...

Bro Network Security Monitor

Open Source Software

1. Git Download
2. Compile
3. Choose HW
4. Choose NIC
5. Configure
6. Tune
7. Goto 1



Raw Bro Output

```
#separator \x09
#set_separator      ,
#empty_field        (empty)
#unset_field        -
#path     ssl
#open     2013-05-03-09-00-03
#fields   ts        uid       id.orig_h id.orig_p id.resp_h id.resp_p version   cipher    server_name         session_id          subject   issuer_subject      not_valid_before
          not_valid_after     last_alert          client_subject      client_issuer_subject         cert_hash validation_status
#types    time      string    addr      port      addr      port      string    string    string    string    string    string    time      time      string    string    string
          string    string
1367586002.795279   hyEvFOj2Ua6         10.1.1.60 36150     82.165.47.254       443       TLSv10    TLS_DHE_RSA_WITH_AES_256_CBC_SHA        -         -         CN=*.abuse.ch,
OU=Domain Control Validated - RapidSSL(R),OU=See www.rapidssl.com/resources/cps (c)12,OU=GT44325223,O=*.abuse.ch,C=CH,serialNumber=izuFPyAiIcGvI/2tiMCVPxF8ZU6lBH/1
CN=RapidSSL CA,O=GeoTrust\, Inc.,C=US   1329215636.000000   1395107894.000000   -         -         -         f175fd6358c8cf7feb342b0ead09a22a        ok
1367586003.532457   1JeJbfHoth          10.1.1.60 48483     64.12.249.115       443       TLSv10    TLS_RSA_WITH_RC4_128_MD5      -         -         CN=*.abuse.ch,OU=Domain
Control Validated - RapidSSL(R),OU=See www.rapidssl.com/resources/cps (c)12,OU=GT44325223,O=*.abuse.ch,C=CH,serialNumber=izuFPyAiIcGvI/2tiMCVPxF8ZU6lBH/1       CN=RapidSSL CA,
O=GeoTrust\, Inc.,C=US        1329215636.000000   1395107894.000000   -         -         -         f175fd6358c8cf7feb342b0ead09a22a        ok
1367586006.757908   lR9kdHCST7f         10.1.1.211          54897     74.125.226.200      443       TLSv10    TLS_ECDHE_ECDSA_WITH_RC4_128_SHA        plus.google.com
4c33f04310b5c84c784b81bb33b88c4907fadccdc579d70ceb4f4ec3cd17f44b      -         -         -         -         -         -         -         -
1367586007.672865   sFhlV1tWsBc         10.1.1.222          58107     74.125.226.213      443       TLSv11    TLS_ECDHE_RSA_WITH_RC4_128_SHA          -         -
CN=mail.google.com,O=Google Inc,L=Mountain View,ST=California,C=US    CN=Google Internet Authority,O=Google Inc,C=US    1366830166.000000   1388433766.000000   -         -
          -         a35f3844bcbd346dd3866601c674496a        ok
1367586012.837338   vvHVSUkB4Bl         10.1.1.211          54898     63.245.217.44       443       TLSv10    TLS_RSA_WITH_RC4_128_SHA      aus3.mozilla.org
6d60fa2859d01a0858dcd99168ee54a58d50029686dfbfd910c8158592c955d2      CN=aus3.mozilla.org,OU=Automatic Update System,O=Mozilla Corporation,L=Mountain View,ST=California,C=US,
serialNumber=2NFmS7A4iNpW/tc9S7-5whOeGhHQgLKx     OU=Equifax Secure Certificate Authority,O=Equifax,C=US      1307952403.000000   1379202050.000000   -         -         -
          3824ba933bc67a98bc0e3df256e6b4e3        ok
1367586014.988107   bE0Eufn5Izj         10.1.1.211          54904     208.75.122.30       443       TLSv10    TLS_RSA_WITH_RC4_128_MD5      origin.ih.constantcontact.com
bf1efa4974b51e6f8863242a86694170de72206bf93d0a67c8b105897ce7f3aa      -         -         -         -         -         -         -         -
1367586014.988731   A0RDITIo6f6         10.1.1.211          54909     208.75.122.30       443       TLSv10    TLS_RSA_WITH_RC4_128_MD5      origin.ih.constantcontact.com
bf1efa4974b51e6f8863242a86694170de72206bf93d0a67c8b105897ce7f3aa      -         -         -         -         -         -         -         -
1367586015.375897   5z6fEs78ovd         10.1.1.24 52047     74.125.226.204      443       TLSv11    TLS_ECDHE_RSA_WITH_RC4_128_SHA          static.googleusercontent.com  -
          CN=*.googleusercontent.com,O=Google Inc,L=Mountain View,ST=California,C=US      CN=Google Internet Authority,O=Google Inc,C=US    1366830296.000000
1388433896.000000   -         -         -         69256954ae1499d60d6d748ec4db925e        ok
1367586015.398027   7U6K20Gi7Q6         10.1.1.24 42708     74.125.226.221      443       TLSv11    TLS_ECDHE_RSA_WITH_RC4_128_SHA          chatenabled.mail.google.com
9d7bd35c4199c03e9877c8c057f6023013d8070790537a0c710b3805de64e0ad      -         -         -         -         -         -         -         -
1367586015.376003   JYUWtlG1i8j         10.1.1.24 47159     74.125.226.203      443       TLSv11    TLS_ECDHE_RSA_WITH_RC4_128_SHA          mail-attachment.googleusercontent.
com       -         CN=*.googleusercontent.com,O=Google Inc,L=Mountain View,ST=California,C=US      CN=Google Internet Authority,O=Google Inc,C=US    1366830296.000000
1388433896.000000   -         -         -         69256954ae1499d60d6d748ec4db925e        ok
1367586014.849758   U6QvtVD4X72         10.1.1.211          54899     74.125.226.207      443       TLSv10    TLS_ECDHE_ECDSA_WITH_RC4_128_SHA        ssl.gstatic.com
6cd013e239a6113926bd3659179edca3acd39dde969bbac42058753f5c0af82e      -         -         -         -         -         -         -         -
1367586015.397866   Bb5xU034z7g         10.1.1.24 52049     74.125.226.204      443       TLSv11    TLS_ECDHE_RSA_WITH_RC4_128_SHA          lh4.googleusercontent.com     -
          CN=*.googleusercontent.com,O=Google Inc,L=Mountain View,ST=California,C=US      CN=Google Internet Authority,O=Google Inc,C=US    1366830296.000000
1388433896.000000   -         -         -         69256954ae1499d60d6d748ec4db925e        ok
1367586018.211678   GcyUHv4HzB6         10.1.1.24 47163     74.125.226.203      443       TLSv11    TLS_ECDHE_RSA_WITH_RC4_128_SHA          mail-attachment.googleusercontent.
com       -         CN=*.googleusercontent.com,O=Google Inc,L=Mountain View,ST=California,C=US      CN=Google Internet Authority,O=Google Inc,C=US    1366830296.000000
1388433896.000000   -         -         -         69256954ae1499d60d6d748ec4db925e        ok
1367586018.302481   E7HpO7keONk         10.1.1.47 57622     75.126.58.197       443       TLSv11    TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA      api.mixpanel.com    -         CN=*.
mixpanel.com,OU=Domain Control Validated - RapidSSL(R),OU=See www.rapidssl.com/resources/cps (c)12,OU=GT67152415,O=*.mixpanel.com,C=US,
serialNumber=kGpbhl3LwgG8PlxPXAjrnN1cUz4idoRK     CN=RapidSSL CA,O=GeoTrust\, Inc.,C=US   1331127738.000000   1394456284.000000   -         -         -
d574556612be9d8e570f3209cbb80782        ok
```

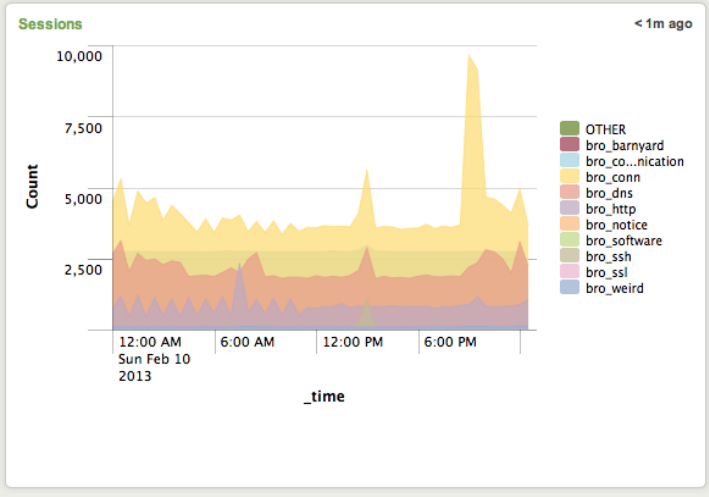
R-Scope Network Security Appliance

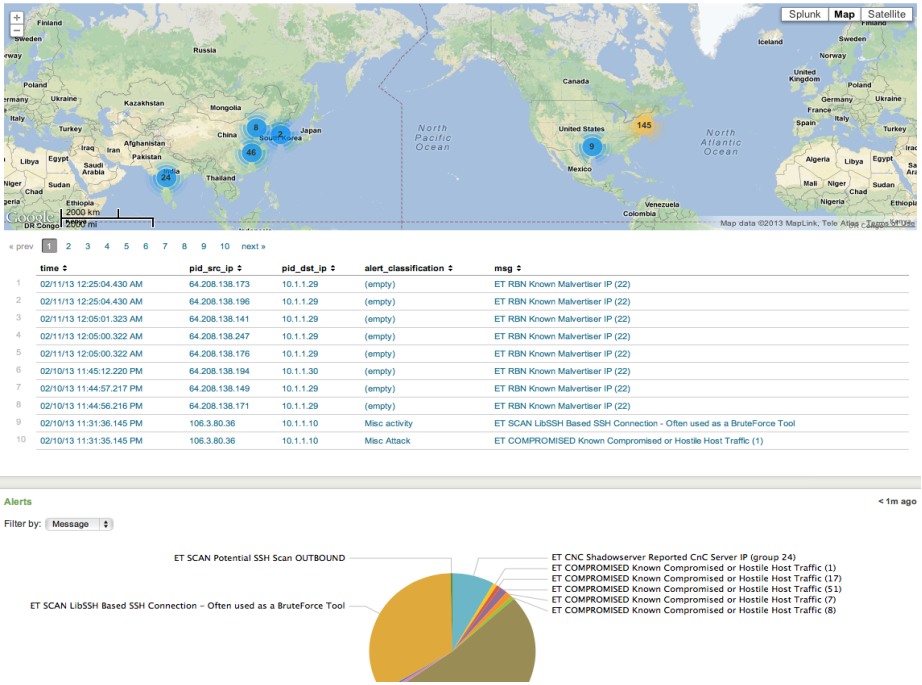
Agile, Scalable, Advanced Network Monitoring

Analytics/Detection Engine

Advanced Analytics Provided

Turnkey solution





Reservoir Labs

R-Scope Network Security Appliance

R-Scope DOMINATE-T
R-Scope PACE-X
Bro open source software base
SIEM integration
Perimeter and insider protection
Configurable to 100 Gbps and beyond

TILERA
SUPERMICRO

Bro

splunk>
Reservoir Labs

10.1.1.60:8000/en-US/app/rscope-apps-2.0/threat_dashboard

Reservoir Labs R-Scope

Administrator | App | Manager | Alerts | Jobs | Logout

Search Alerts Analyze

Help | About

Filter

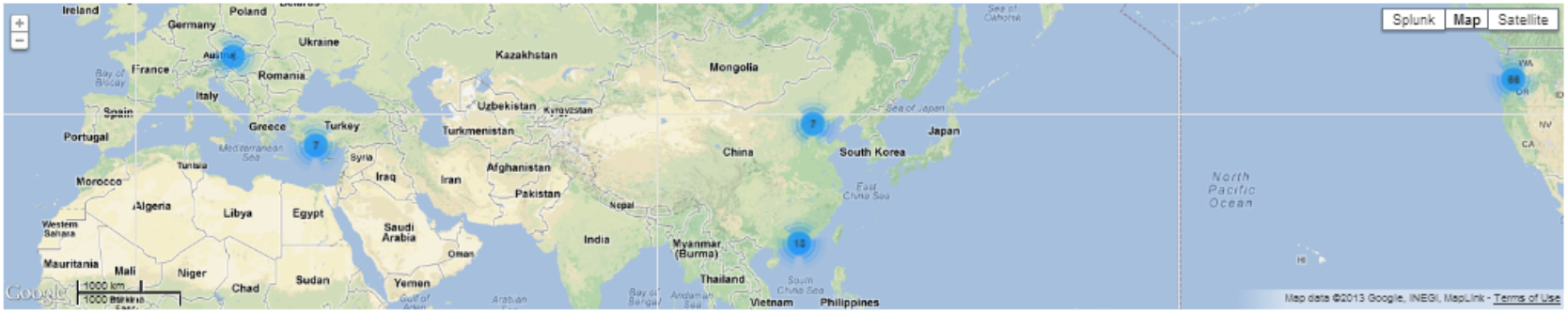
2m ago

Search

Last 30 days

Notices

Display: Source



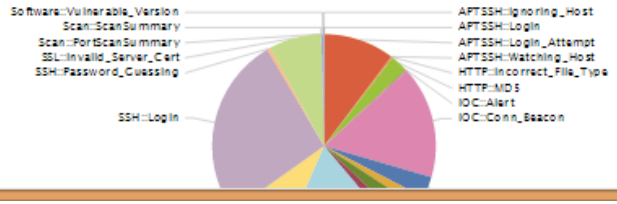
« prev 1 2 3 4 5 6 7 8 next »

	_time	id_orig_h	id_resp_h	note	msg
1	4/30/13 7:43:51.830 PM	221.176.53.74	10.1.1.10	SSH::Login	Heuristically detected successful SSH login.
2	4/30/13 7:43:51.830 PM	221.176.53.74	10.1.1.10	SSH::Login	Heuristically detected successful SSH login.
3	4/30/13 7:43:51.830 PM	221.176.53.74	10.1.1.10	SSH::Login	Heuristically detected successful SSH login.
4	4/30/13 7:43:51.830 PM	221.176.53.74	10.1.1.10	SSH::Login	Heuristically detected successful SSH login.
5	4/30/13 7:43:51.830 PM	221.176.53.74	10.1.1.10	SSH::Login	Heuristically detected successful SSH login.
6	4/30/13 7:43:51.830 PM	221.176.53.74	10.1.1.10	SSH::Login	Heuristically detected successful SSH login.
7	4/30/13 7:39:26.049 PM	221.176.53.74	NULL	SSH::Password_Guessing	Threshold crossed by metric_index(host=221.176.53.74) 18/10
8	4/27/13 6:34:51.395 AM	223.5.3.200	NULL	SSH::Password_Guessing	Threshold crossed by metric_index(host=223.5.3.200) 1476/10
9	4/27/13 5:32:28.191 AM	223.5.3.200	NULL	SSH::Password_Guessing	Threshold crossed by metric_index(host=223.5.3.200) 18/10
10	4/19/13 2:38:15.656 PM	222.128.198.6	NULL	SSH::Password_Guessing	Threshold crossed by metric_index(host=222.128.198.6) 14/10

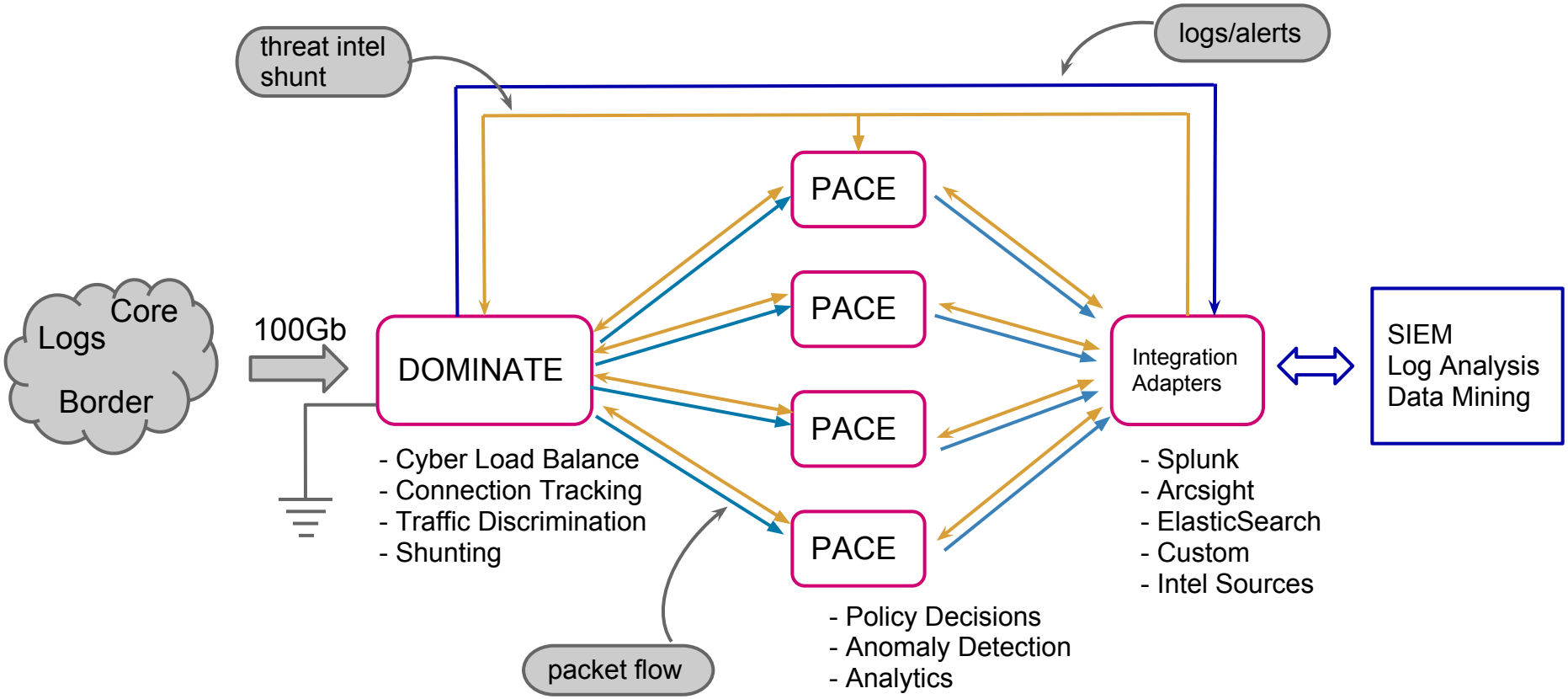
Notices

< 1m ago

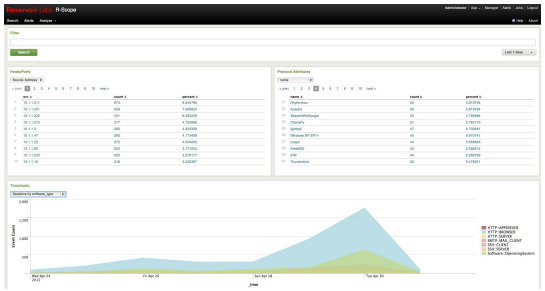
Filter by: Note

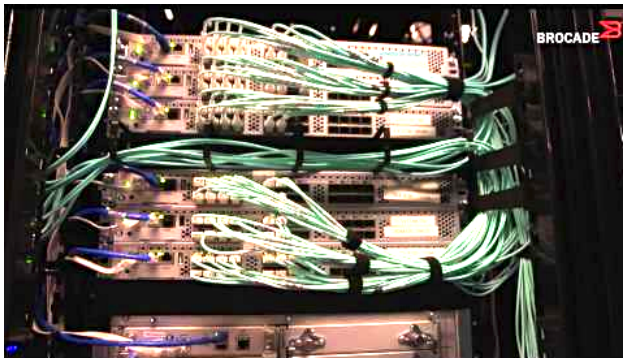


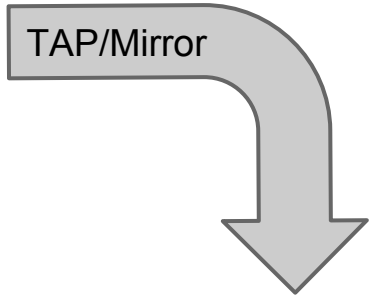
R-Scope: System Integration



R-Scope DOMINATE-T







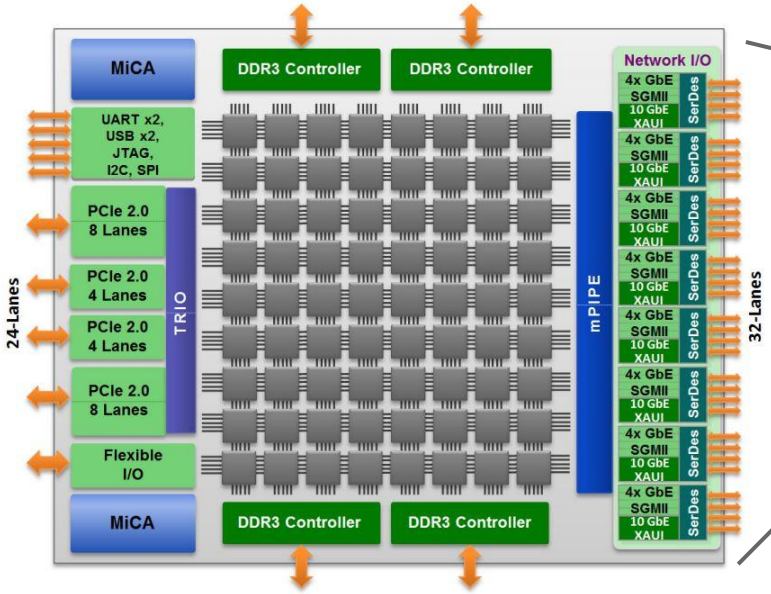
100Gbps

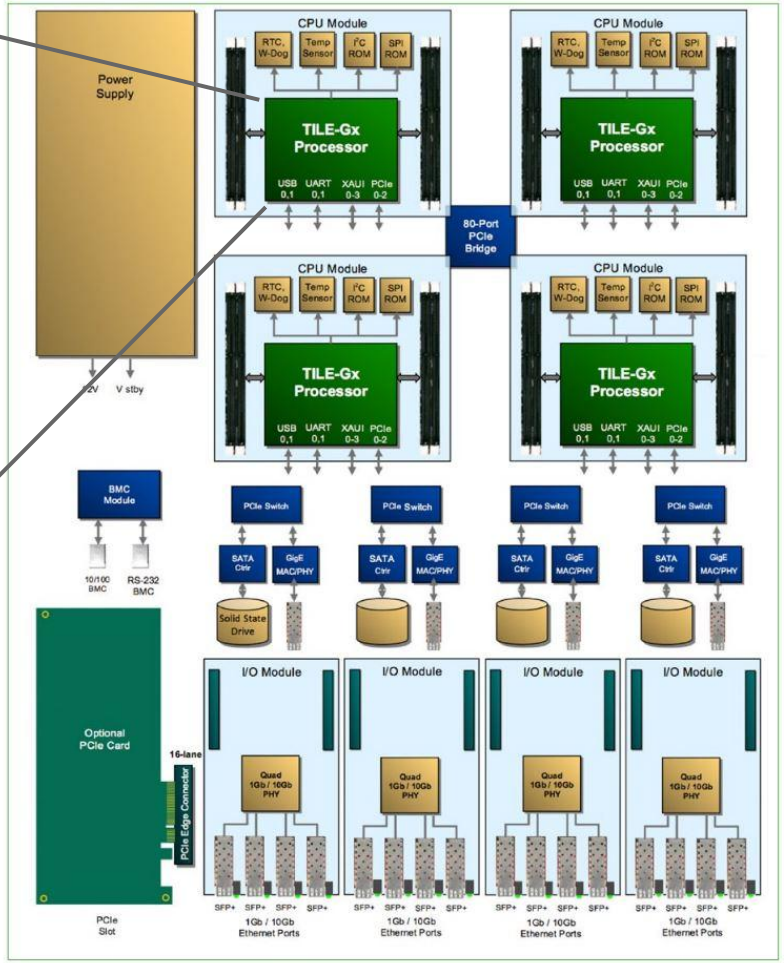
DOMINATE-T

20 - 40Gbps

- 4 – 8 Processor Systems
- 160Gbps – 320Gbps Raw Throughput
- 32 Core Processors
- R-Scope Software Tightly Coupled
- Front-end Load Balancing
- First Pass Analytics

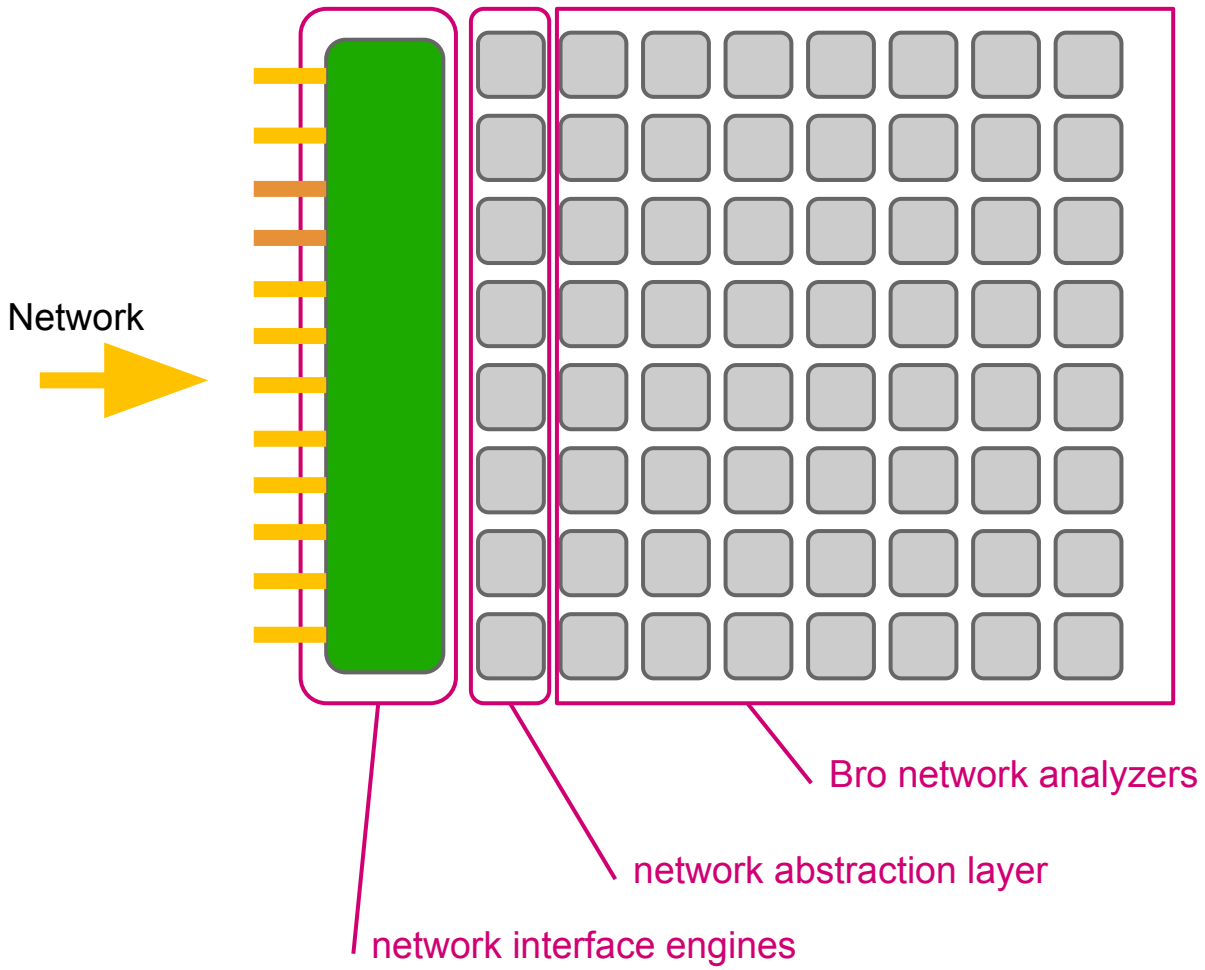
Tilera-TILExtreme-Gx



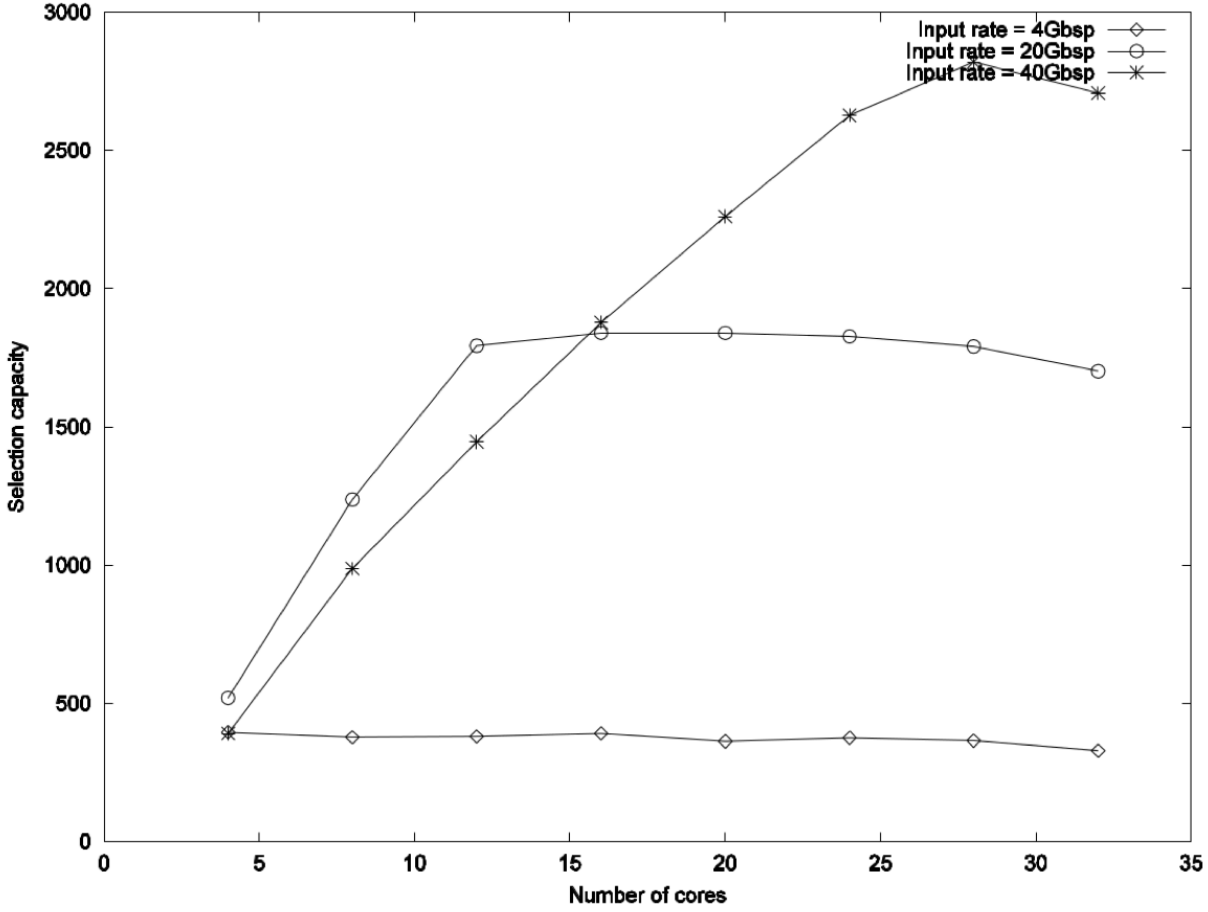


TILExtreme-Gx™ Block Diagram

DOMINATE-T leverages advanced Tilera hardware for throughput



R-Scope DOMINATE-T events / sec



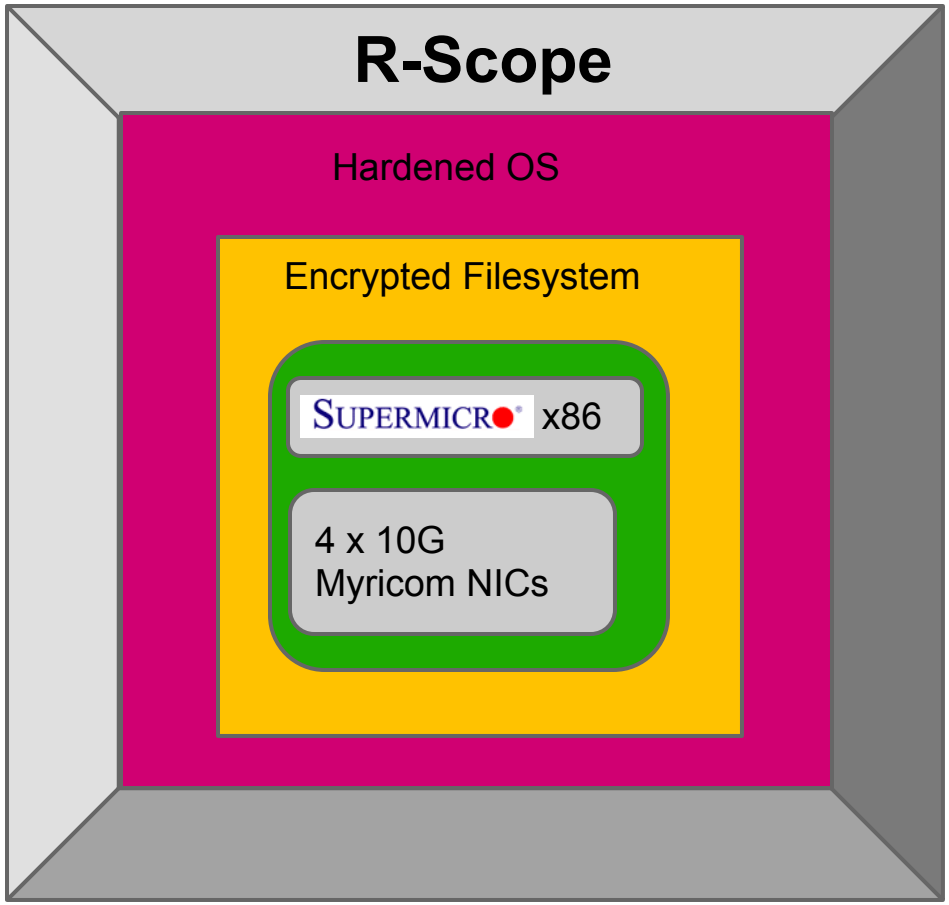
Single Tilera-Gx36
Synthetic traffic
Selection capacity events/sec

Indicates that a single Gx36 processor (36 cores) can handle 40 Gbps traffic at 2800 events/sec

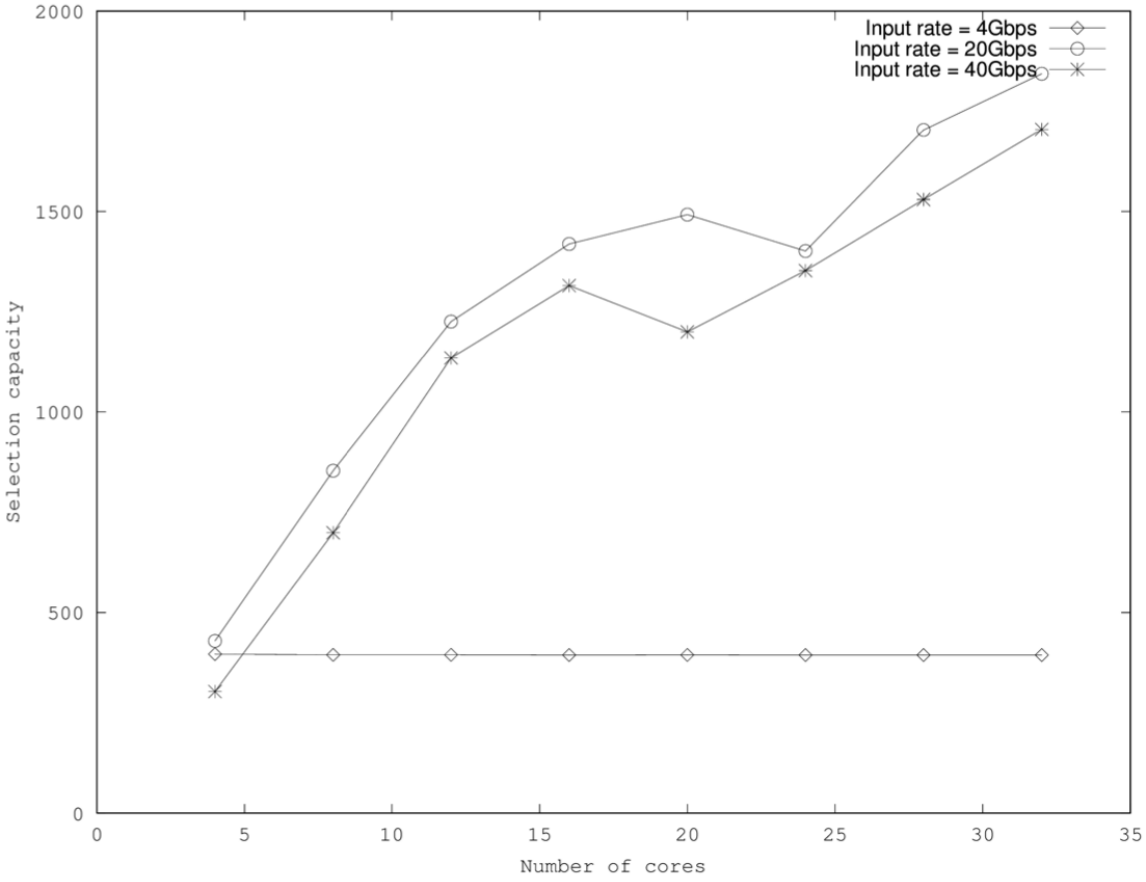
R-Scope-PACE-X

Security Appliance

- Validated HW/SW
- Signed updates
- CLI + GUI Management
- Splunk Integration
- Shunting Control



R-Scope PACE-X (events/sec)



2 sockets
Xeon(R) CPU E5-2670
@ 2.60GHz
(each 8 cores / 16 threads)
20M Cache,
8.00 GT/s Intel QPI

Indicates processing rate peaks at 20 Gbps/s ingest, at 1800 events/sec.

New models with Myricom even faster.

DOMINATE-T at DOE

ESnet Research Testbeds

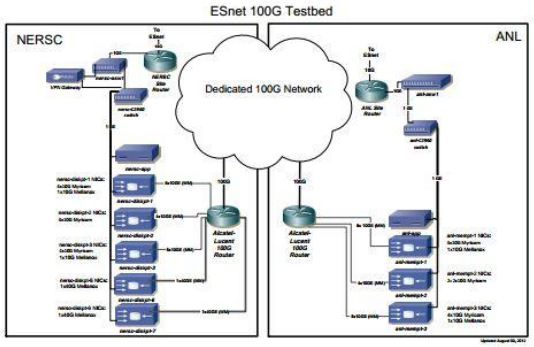
R-Scope DOMINATE-T
installed and in testing now at DOE Lab

100G Testbed

- High-speed protocol research
- Routed network from Argonne to NERSC (dedicated 100G)
- See recent HPCwire

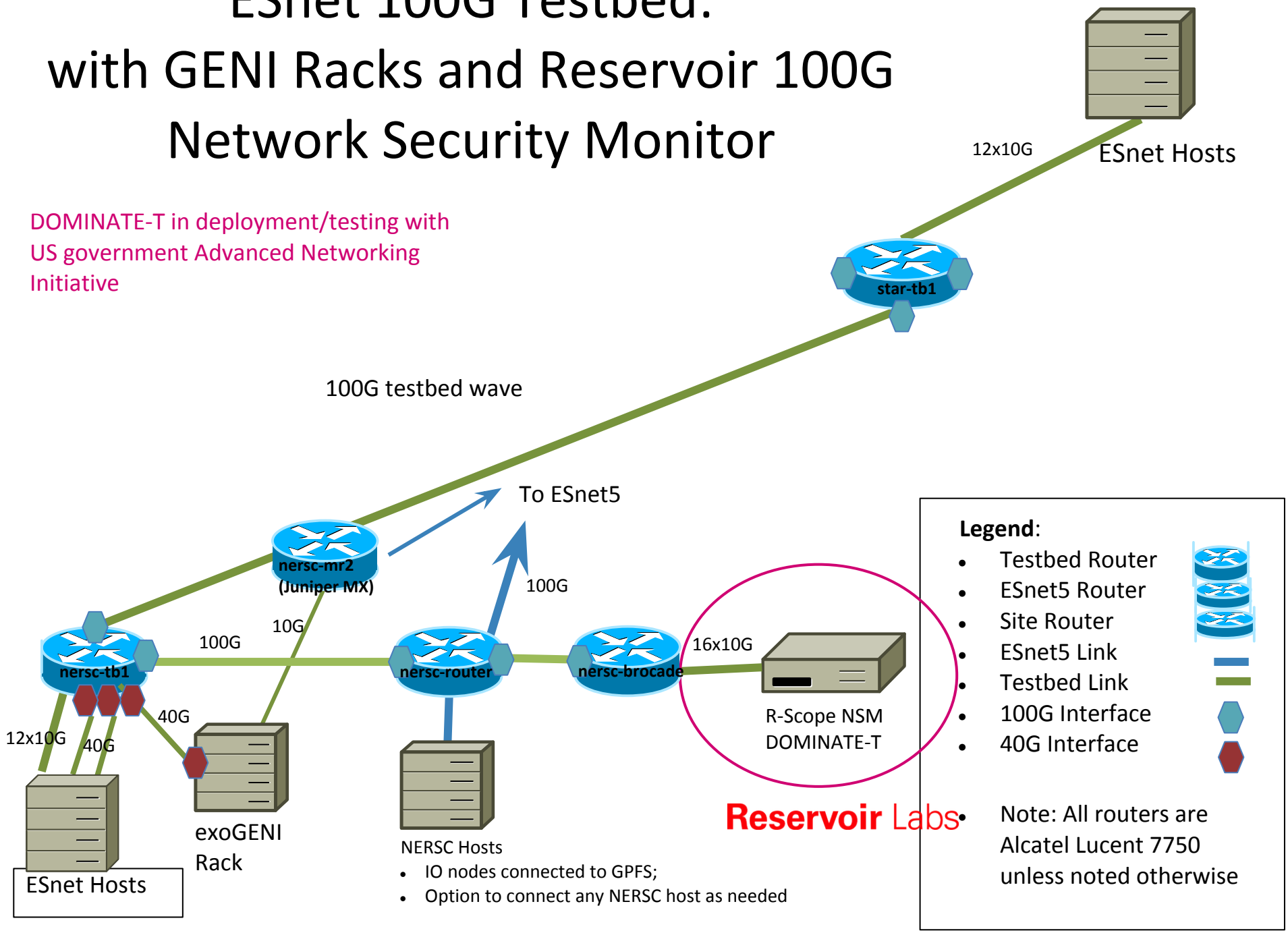
Dark Fiber Testbed

- Continental-scale fiber footprint for disruptive research



ESnet 100G Testbed: with GENI Racks and Reservoir 100G Network Security Monitor

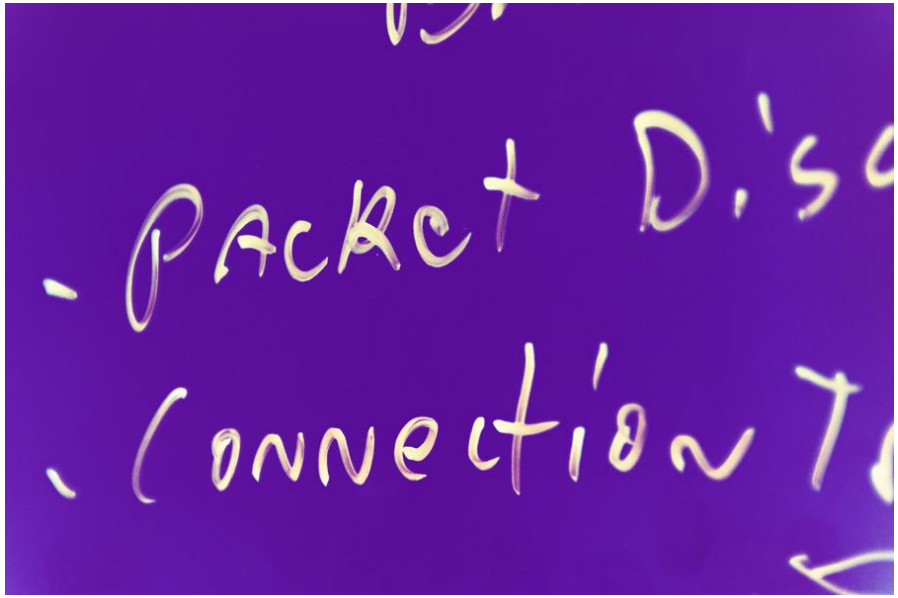
DOMINATE-T in deployment/testing with US government Advanced Networking Initiative



Acknowledgements

CYBER NY Alliance
Department of Energy SBIR Program
Department of Defense
The Bro Community
ESnet Advanced Networking Initiative
NERSC
Tilera Corporation
Super Micro Computer, Inc.
Reservoir R-Scope team

Thank you!



Reservoir Labs
632 Broadway, Suite 803
New York, New York 10012
(212) 780-0527
http://www.reservoir.com

lethin@reservoir.com