IBM Security

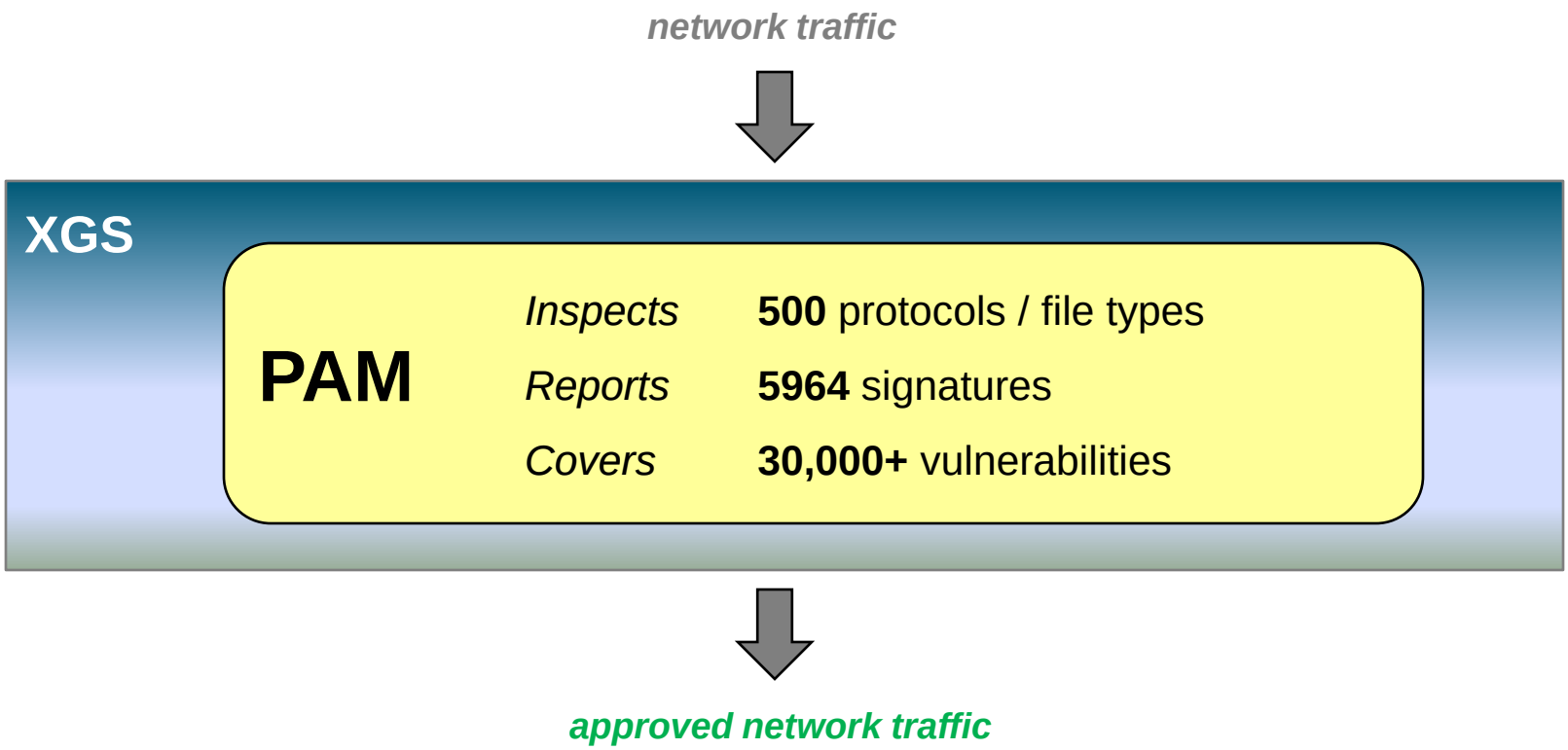
IBM X-Force如何抵御未知威胁

李承达 IBM全球首席资讯安全架构师

IBM

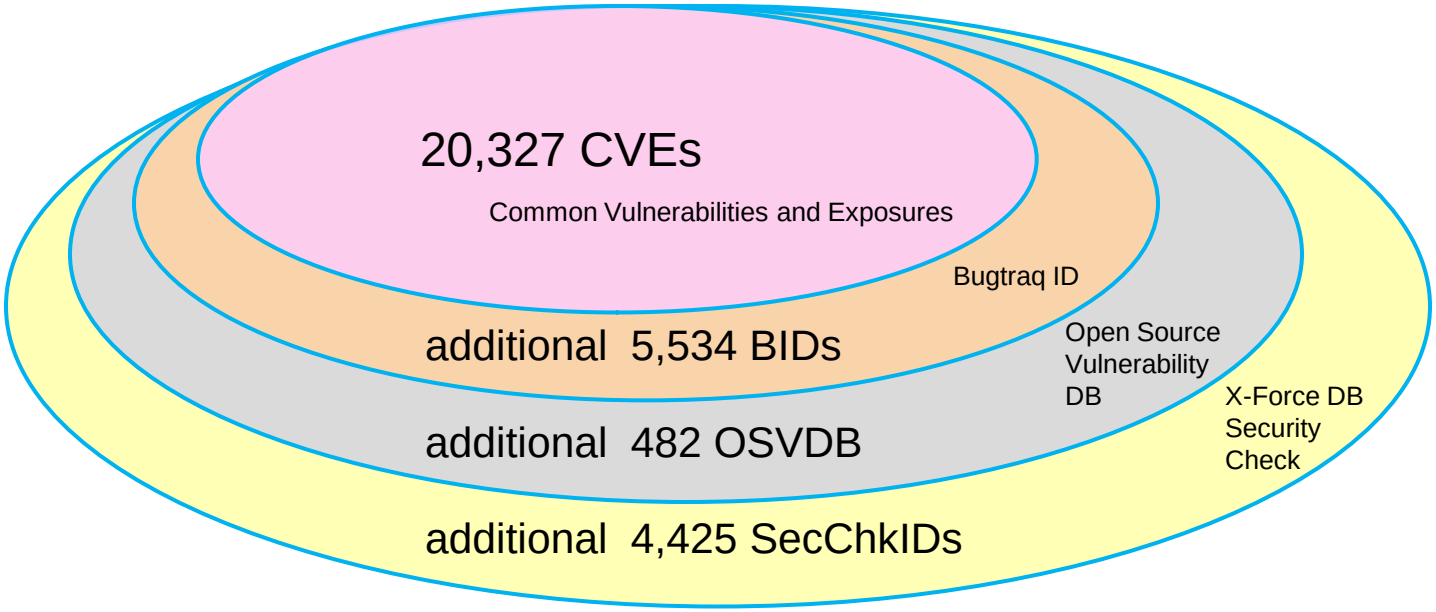
What is PAM?

- The Protocol Analysis Module (PAM) is at the core of many IBM security products
  - XGS next-generation intrusion prevention system (IPS)
- PAM uses Deep Packet Inspection (DPI) to thoroughly inspect packets at wire speed
  - processes up to 25 Gbps on the XGS 7100 appliance.



PAM does more with less

5,459 attack signatures cover 30,000+ vulnerabilities as of March 2016*



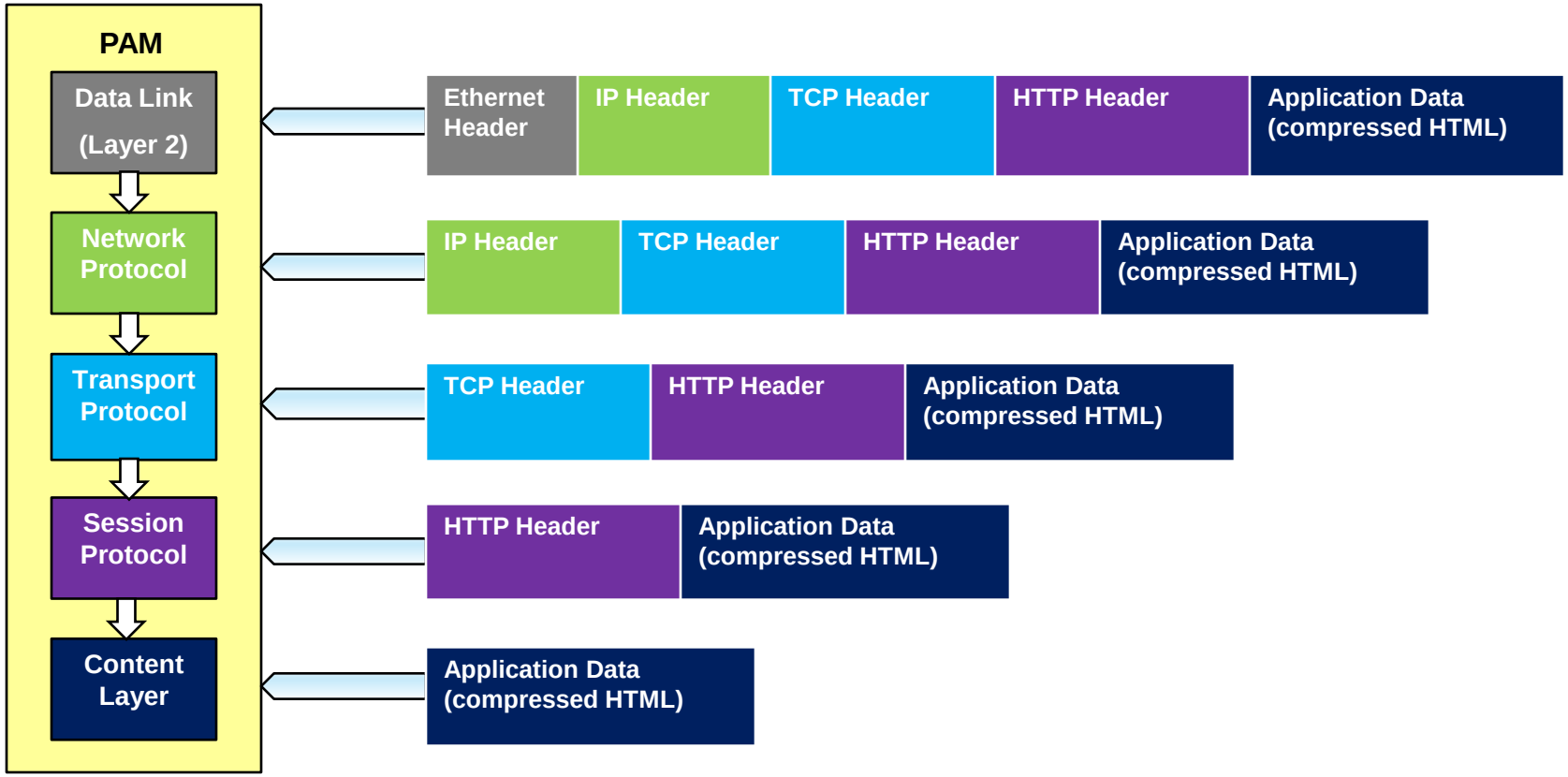
** PAM also contains 497 audit signatures and 8 status signatures*

Leading industry analysts recently commented:

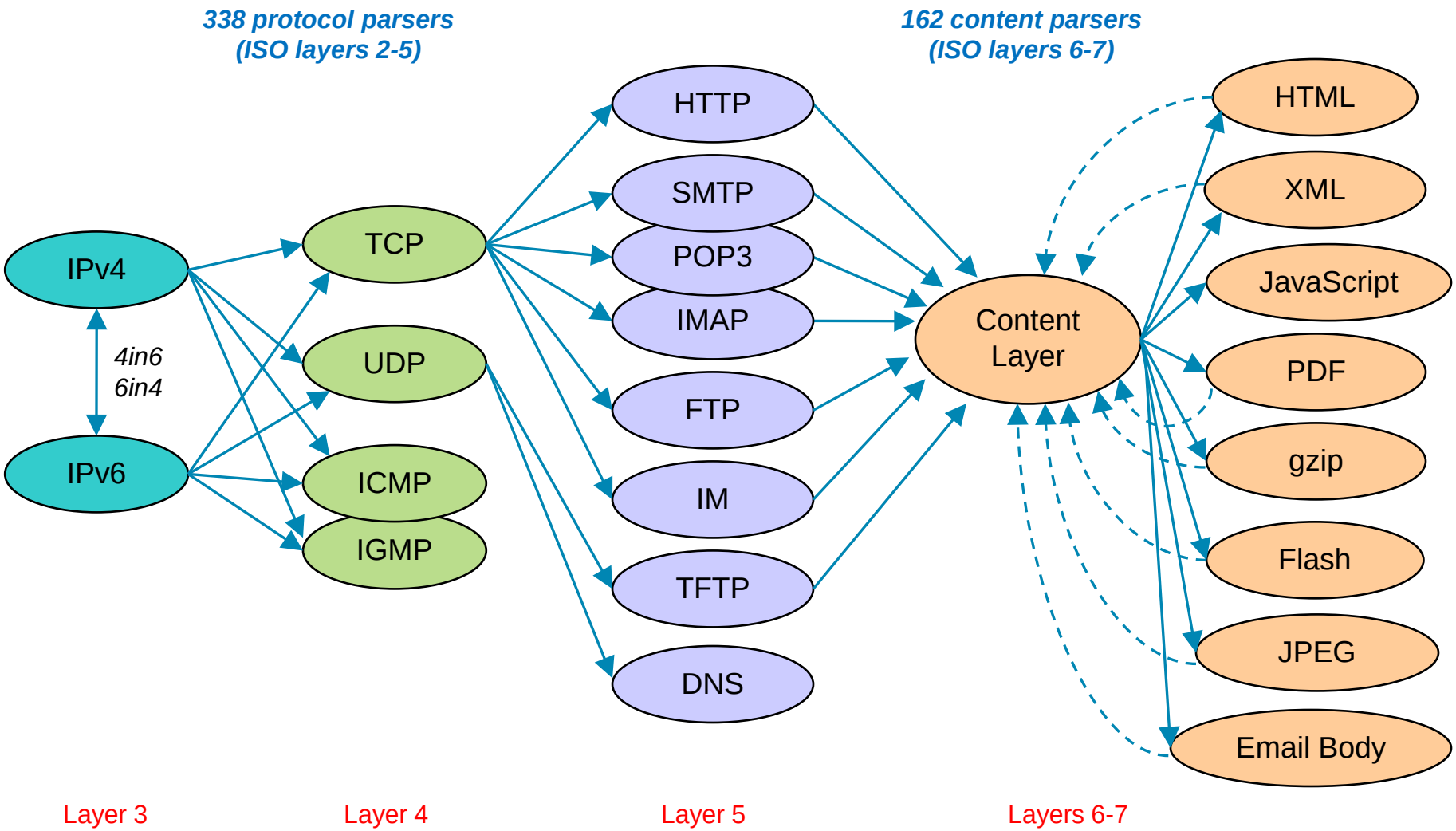
IBM's Protocol Analysis Module (PAM) is still leading the market in its ability to provide low false positives and protection for entire classes of vulnerabilities, with the smallest number of signatures on the market.

PAM parses each frame, layer by layer

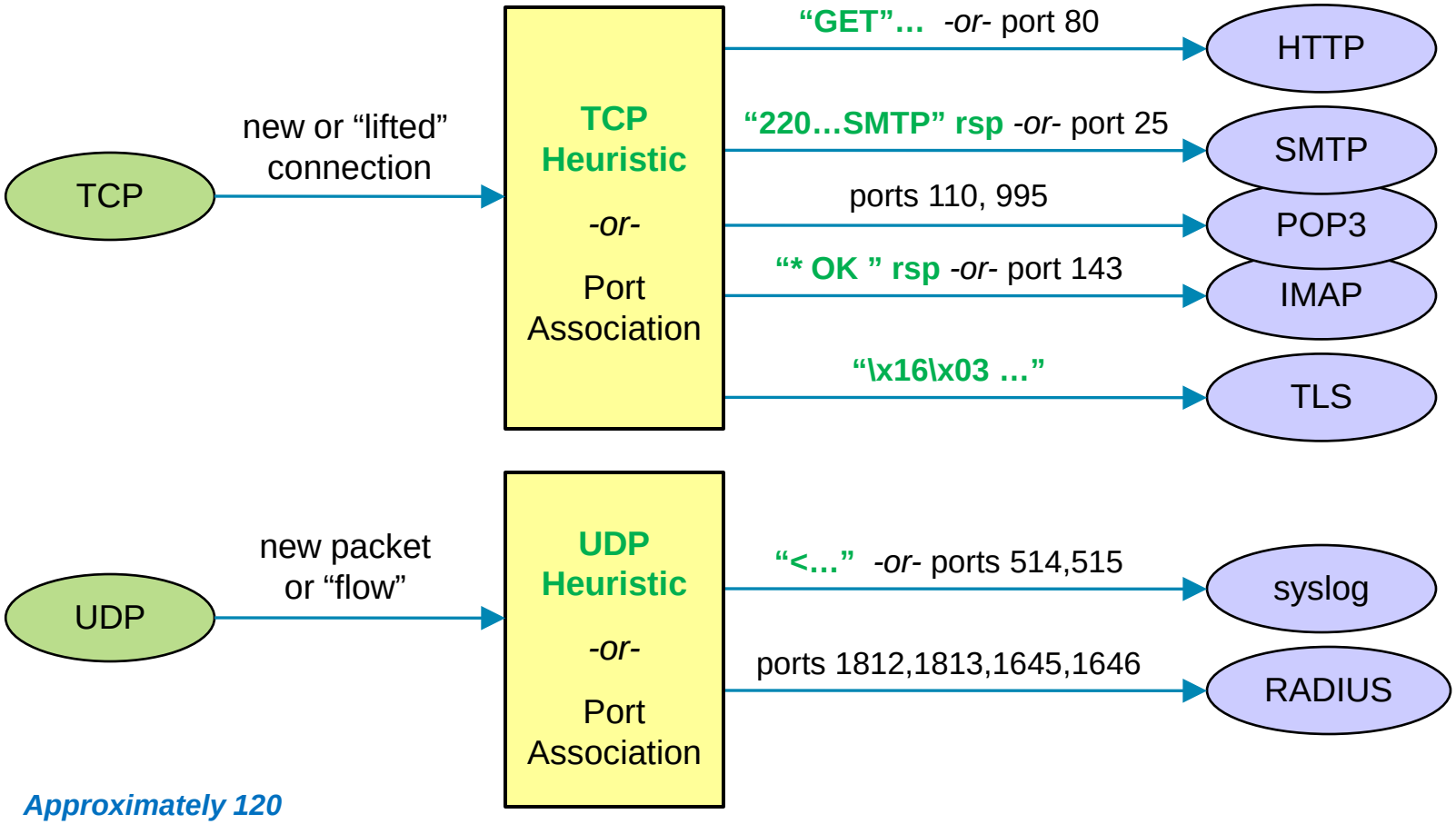
- Deep Packet Inspection continues to the end of the packet in a stateful manner
- PAM signatures may trigger while parsing any layer (2-7)
- Multiple signatures may trigger on the same packet



PAM Parser Overview

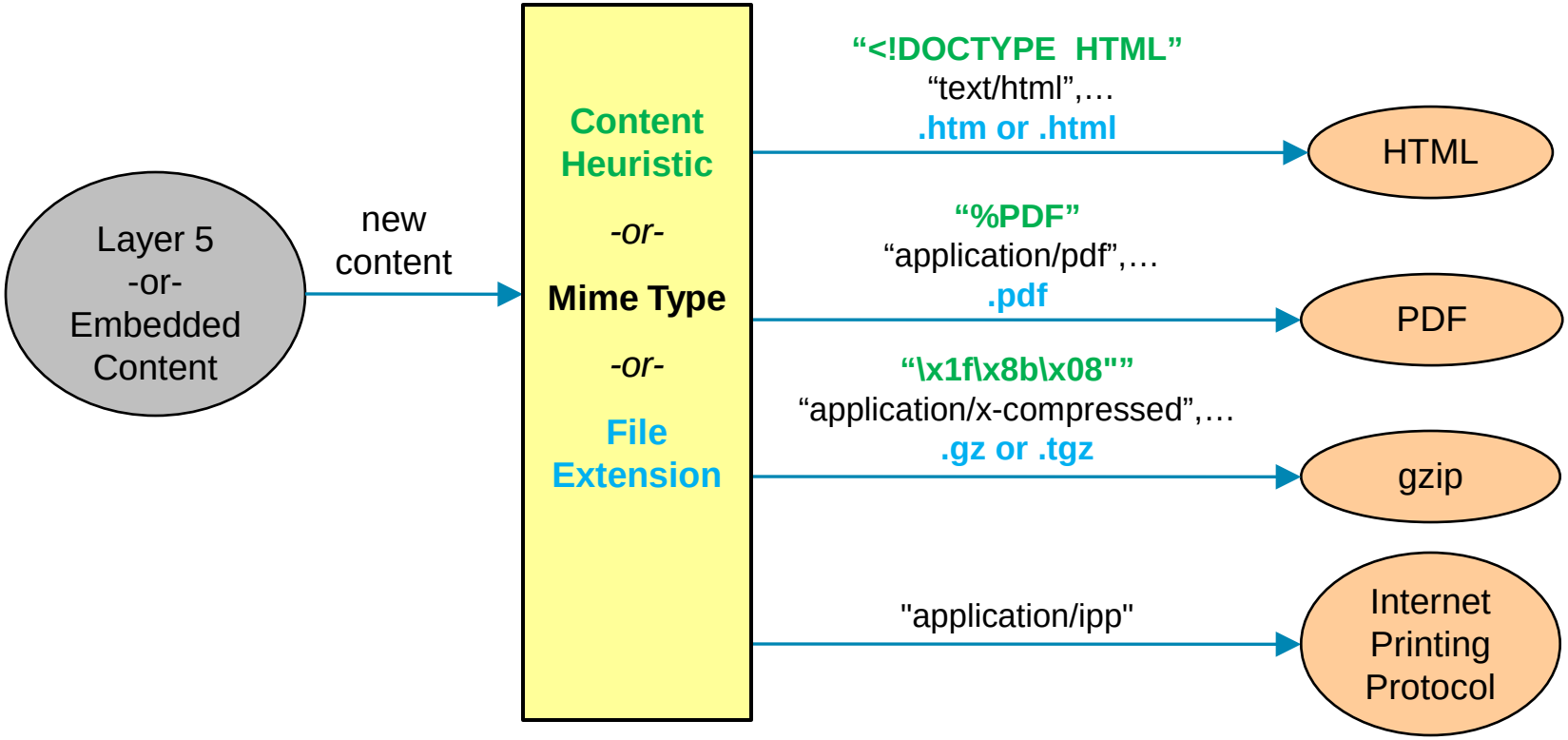


PAM Protocol Heuristics (layer 5)



Approximately 120 protocol parsers identified heuristically

PAM Content Heuristics (layer 6-7)



Approximately 130 content parsers identified heuristically

Example of Deep Packet Inspection (1 of 5)

HTTP 200 response transmitted in 99 TCP segments (packets) over IPv4

```
⊞ Frame 268: 749 bytes on wire (5992 bits), 749 bytes captured (5992 bits)
⊞ Ethernet II, Src: MarvellS 00:6f:52 (00:50:43:00:6f:52), Dst: BuffaloI 3f:88:a7 (4c:e6:76:3f:88:a7)
⊞ Internet Protocol Version 4, Src: 10.1.1.2, Dst: 46.246.42.9
⊞ Transmission Control Protocol, Src Port: http (80), Dst Port: 49825 (49825), Seq: 2719545807, Ack: 3626752787, Len: 695
⊞ [99 Reassembled TCP Segments (398538 bytes): #6(8112), #7(355), #8(4056), #11(8112), #14(8112), #17(8112), #20(8112), #23(8112), #2…
⊟ Hypertext Transfer Protocol
  ⊞ HTTP/1.1 200 OK\r\n
    Date: Thu, 26 Sep 2013 02:24:54 GMT\r\n
    <Date: Thu, 26 Sep 2013 02:24:54 GMT\r\n>
    Server: Apache/2.4.6 (Debian)\r\n
    Transfer-Encoding: chunked\r\n
    <Transfer-Encoding: chunked\r\n>
    Content-Type: application/pdf\r\n
    <Content-Type: application/pdf\r\n>
    \r\n
    <Response: True>
    [HTTP response 1/1]
    [Time since request: 9.320314000 seconds]
    [Request in frame: 4]
  ⊞ HTTP chunked response
    Content-encoded entity body (gzip): 397812 bytes -> 91012590 bytes
⊟ Media Type
    Media type: application/pdf (91012590 bytes)
```

Example of Deep Packet Inspection (2 of 5)

The HTTP response uses Chunked Encoding dividing the payload into 46 chunks.

```
Transfer-Encoding: chunked\r\n
<Transfer-Encoding: chunked\r\n>
Content-Type: application/pdf\r\n
<Content-Type: application/pdf\r\n>
\r\n
<Response: True>
[HTTP response 1/1]
[Time since request: 9.320314000 seconds]
[Request in frame: 4]
HTTP chunked response
  Data chunk (8106 octets)
  Data chunk (8096 octets)
  Data chunk (8096 octets)
  Data chunk (8096 octets)
  Data chunk (8096 octets)
  Data chunk (8096 octets)
  Data chunk (8096 octets)
  Data chunk (8096 octets)
  Data chunk (8096 octets)
  Data chunk (8096 octets)
  Data chunk (8096 octets)
  Data chunk (8096 octets)
  Data chunk (8096 octets)
  Data chunk (8096 octets)
  Data chunk (8096 octets)
```

Example of Deep Packet Inspection (3 of 5)

The HTTP “chunked” payload is compressed in gzip format!

```
⊞ Frame 268: 749 bytes on wire (5992 bits), 749 bytes captured (5992 bits)
⊞ Ethernet II, Src: MarvellS_00:6f:52 (00:50:43:00:6f:52), Dst: BuffaloI_3f:88:a7 (4c:e6:76:3f:88:a7)
⊞ Internet Protocol Version 4, Src: 10.1.1.2, Dst: 46.246.42.9
⊞ Transmission Control Protocol, Src Port: http (80), Dst Port: 49825 (49825), Seq: 2719545807, Ack: 3626752787, Len: 695
⊞ [99 Reassembled TCP Segments (398538 bytes): #6(8112), #7(355), #8(4056), #11(8112), #14(8112), #17(8112), #20(8112), #23(8112), #2…
⊟ Hypertext Transfer Protocol
  ⊞ HTTP/1.1 200 OK\r\n
    Date: Thu, 26 Sep 2013 02:24:54 GMT\r\n
    <Date: Thu, 26 Sep 2013 02:24:54 GMT\r\n>
    Server: Apache/2.4.6 (Debian)\r\n
    Transfer-Encoding: chunked\r\n
    <Transfer-Encoding: chunked\r\n>
    Content-Type: application/pdf\r\n
    <Content-Type: application/pdf\r\n>
    \r\n
    <Response: True>
    [HTTP response 1/1]
    [Time since request: 9.320314000 seconds]
    [Request in frame: 4]
  ⊞ HTTP chunked response
    Content-encoded entity body (gzip): 397812 bytes -> 91012590 bytes
⊟ Media Type
    Media type: application/pdf (91012590 bytes)
```

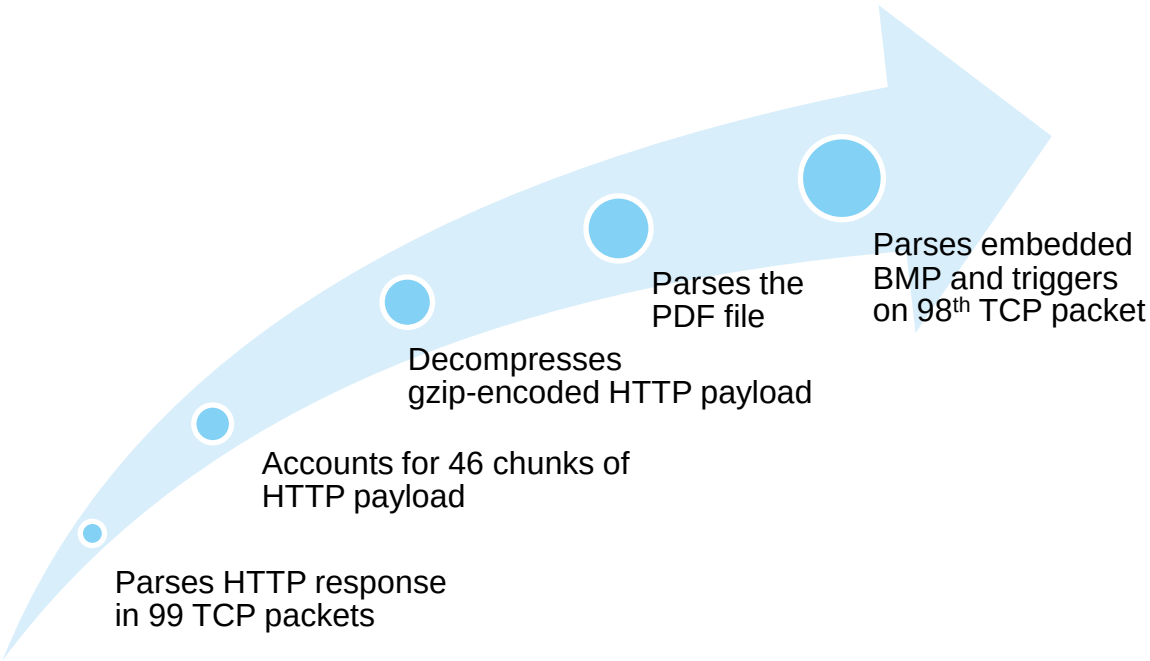
Example of Deep Packet Inspection (4 of 5)

The content of the gzip compressed payload is a PDF file.

```
⊞ Frame 268: 749 bytes on wire (5992 bits), 749 bytes captured (5992 bits)
⊞ Ethernet II, Src: MarvellS_00:6f:52 (00:50:43:00:6f:52), Dst: BuffaloI_3f:88:a7 (4c:e6:76:3f:88:a7)
⊞ Internet Protocol Version 4, Src: 10.1.1.2, Dst: 46.246.42.9
⊞ Transmission Control Protocol, Src Port: http (80), Dst Port: 49825 (49825), Seq: 2719545807, Ack: 3626752787, Len: 695
⊞ [99 Reassembled TCP Segments (398538 bytes): #6(8112), #7(355), #8(4056), #11(8112), #14(8112), #17(8112), #20(8112), #23(8112), #2…
⊟ Hypertext Transfer Protocol
  ⊞ HTTP/1.1 200 OK\r\n
    Date: Thu, 26 Sep 2013 02:24:54 GMT\r\n
    <Date: Thu, 26 Sep 2013 02:24:54 GMT\r\n>
    Server: Apache/2.4.6 (Debian)\r\n
    Transfer-Encoding: chunked\r\n
    <Transfer-Encoding: chunked\r\n>
    Content-Type: application/pdf\r\n
    <Content-Type: application/pdf\r\n>
    \r\n
    <Response: True>
    [HTTP response 1/1]
    [Time since request: 9.320314000 seconds]
    [Request in frame: 4]
  ⊞ HTTP chunked response
    Content-encoded entity body (gzip): 397812 bytes -> 91012590 bytes
⊟ Media Type
    Media type: application/pdf (91012590 bytes)
```

Example of Deep Packet Inspection (5 of 5)

Hidden in the PDF file is a malicious .bmp image file, which PAM catches




```
2136000 (PDF_XFA_RLE_BMP_Overflow) on frame 266
        intruder=10.1.1.2:80
        victim=46.246.42.9:49825
        protocolflags=TCP [ACK]
        reporttype=SRC_ATTACKS_DST
        adapterid=0
        time="2013-09-25 22:25:04.035081"
        resultflags=TCP
        priority=High
        URL=/evil/PDF_BMP_Overflow.pdf
        server=66.141.47.121
        accessed=yes
        code=200
        protocol=http
        skip entry count=16777216
        pdfObj=5
        compressed=gzip
```

Ahead of the Threat (AOTT)

OVERVIEW AND EXAMPLES

Ahead of The Threat (AOTT)

- AOTT – pre-existing coverage for a vulnerability on the day it is publicly reported

CVE-2013-2729

Adobe Reader and Acrobat integer overflow

Reported: May 14, 2013

Criteria for AOTT items in this presentation:

1. At least 90 days of pre-existing PAM coverage
2. Default Blocked if using “Trust X-Force”
3. Notable vendor (e.g. Microsoft, Adobe, HP, Oracle)
4. Recent – 2012 to present
5. CVSS base score 5 or higher

X-Force Top 100 Ahead of the Threat Coverage

Blocking coverage at least 90 days ahead of the threat for notable vendors since 2012 with CVSS >=5

Average AOTT = 3.8 yrs Average CVSS base = 8.6

Adobe

CVE-2015-5097	5.1 yrs
CVE-2014-8438	7.6 yrs
CVE-2013-3346	1.3 yrs
CVE-2013-2729	7.2 yrs
CVE-2013-2555	0.7 yrs
CVE-2013-0634	1.8 yrs
CVE-2012-4170	7.5 yrs
CVE-2012-1535	1.4 yrs
CVE-2012-0769	0.9 yrs
CVE-2012-0768	0.9 yrs
BID-52632	7.0 yrs

Apache

CVE-2013-2251	2.4 yrs
CVE-2013-2135	2.3 yrs
CVE-2013-2134	2.3 yrs
CVE-2013-2115	2.3 yrs
CVE-2013-1966	2.3 yrs
CVE-2012-0838	1.0 yrs
CVE-2012-0391	0.9 yrs

Apple

CVE-2012-3753	0.8 yrs

CA

BID-51915	7.0 yrs

GNU

CVE-2015-0235	9.9 yrs

ISC

CVE-2012-3571	1.9 yrs
CVE-2012-3523	1.2 yrs

Google

CVE-2015-3864	8.4 yrs
CVE-2015-3829	8.3 yrs
CVE-2015-3828	8.3 yrs
CVE-2015-3827	6.5 yrs
CVE-2015-3826	8.3 yrs
CVE-2015-3824	8.3 yrs
CVE-2015-1539	8.3 yrs
CVE-2015-1538	8.3 yrs
BID-52632	7.0 yrs

HP

CVE-2014-7883	1.1 yrs
CVE-2014-2625	9.4 yrs
CVE-2014-2621	1.1 yrs
CVE-2014-2620	1.2 yrs
CVE-2014-2617	1.9 yrs
CVE-2013-6195	0.3 yrs
CVE-2013-4799	5.9 yrs
CVE-2012-5201	6.8 yrs

Microsoft

CVE-2016-0103	0.8 yrs
CVE-2015-6143	0.5 yrs
CVE-2015-6142	0.5 yrs
CVE-2015-6150	1.4 yrs
CVE-2015-6087	4.6 yrs
CVE-2015-2464	3.3 yrs
CVE-2015-2461	4.7 yrs
CVE-2015-2397	1.7 yrs
CVE-2015-1662	4.0 yrs
CVE-2015-0090	1.4 yrs
CVE-2015-0086	4.6 yrs
CVE-2014-6369	1.1 yrs

Microsoft (cont)

CVE-2014-6343	3.6 yrs
CVE-2014-6332	0.4 yrs
CVE-2014-2799	0.5 yrs
CVE-2014-2797	0.7 yrs
CVE-2014-1811	4.8 yrs
CVE-2014-1761	1.3 yrs
CVE-2013-3906	1.2 yrs
CVE-2013-3893	0.7 yrs
CVE-2013-3163	0.5 yrs
CVE-2013-1331	3.7 yrs
CVE-2013-1347	2.6 yrs
CVE-2013-1313	0.5 yrs
CVE-2013-0026	6.9 yrs
CVE-2013-0025	6.9 yrs
CVE-2012-4781	6.7 yrs
CVE-2012-2522	0.8 yrs
CVE-2012-1891	1.5 yrs
CVE-2012-1879	6.2 yrs
CVE-2012-1878	6.2 yrs
CVE-2012-1876	6.2 yrs
CVE-2012-1875	6.2 yrs
CVE-2012-0171	6.1 yrs
CVE-2012-0170	6.1 yrs
CVE-2012-0169	6.1 yrs
CVE-2012-0159	1.6 yrs
CVE-2012-0158	2.7 yrs
CVE-2012-0155	5.9 yrs
CVE-2012-0016	1.1 yrs
CVE-2012-0011	5.9 yrs
CVE-2012-0003	0.3 yrs

NGINX

CVE-2014-3556	3.1 yrs
CVE-2013-2070	8.2 yrs

Novell

CVE-2015-0779	3.0 yrs
CVE-2012-0271	0.6 yrs

NTP

CVE-2013-5211	0.5 yrs

Oracle

CVE-2013-2465	0.8 yrs
CVE-2013-2463	0.8 yrs
CVE-2013-2431	8.2 yrs
CVE-2013-0431	0.3 yrs
CVE-2013-0422	7.9 yrs
BID-56791	1.5 yrs
BID-56772	1.6 yrs
CVE-2012-3342	0.3 yrs

PHP

CVE-2015-4022	7.2 yrs
CVE-2014-4049	5.5 yrs

PowerDNS

CVE-2015-1868	10.2 yrs

Samba

CVE-2014-0239	0.8 yrs

Squid

CVE-2013-4115	8.4 yrs

X-Force Top 100 Ahead of the Threat Coverage

Blocking coverage at least 90 days ahead of the threat for notable vendors since 2012 with CVSS >=5

Let's look at 4 examples

Average AOTT = 3.8 yrs Average CVSS base = 8.6

Adobe

CVE-2015-5097	5.1 yrs
CVE-2014-8438	7.6 yrs
CVE-2013-3346	1.3 yrs
CVE-2013-2729	7.2 yrs
CVE-2013-2555	0.7 yrs
CVE-2013-0634	1.8 yrs
CVE-2012-4170	7.5 yrs
CVE-2012-1535	1.4 yrs
CVE-2012-0769	0.9 yrs
CVE-2012-0768	0.9 yrs
BID-52632	7.0 yrs

QuickTime *Protocol anomaly*

Apache

CVE-2013-2251	2.4 yrs
CVE-2013-2135	2.3 yrs
CVE-2013-2134	2.3 yrs
CVE-2013-2115	2.3 yrs
CVE-2013-1966	2.3 yrs
CVE-2012-0838	1.0 yrs
CVE-2012-0391	0.9 yrs

Apple

CVE-2012-3753	0.8 yrs

CA

BID-51915	7.0 yrs

GNU

CVE-2015-0235	9.9 yrs

ISC

CVE-2012-3571	1.9 yrs
CVE-2012-3523	1.2 yrs

Google

CVE-2015-3864	8.4 yrs
CVE-2015-3829	8.3 yrs
CVE-2015-3828	8.3 yrs
CVE-2015-3827	6.5 yrs
CVE-2015-3826	8.3 yrs
CVE-2015-3824	8.3 yrs
CVE-2015-1539	8.3 yrs
CVE-2015-1538	8.3 yrs
BID-52632	7.0 yrs

HP

CVE-2014-7883	1.1 yrs
CVE-2014-2625	9.4 yrs
CVE-2014-2621	1.1 yrs
CVE-2014-2620	1.2 yrs
CVE-2014-2617	1.9 yrs
CVE-2013-6195	0.3 yrs
CVE-2013-4799	5.9 yrs
CVE-2012-5201	6.8 yrs

ZIP *History repeats*

Microsoft

CVE-2016-0103	0.8 yrs
CVE-2015-6143	0.5 yrs
CVE-2015-6142	0.5 yrs
CVE-2015-6150	1.4 yrs
CVE-2015-6087	4.6 yrs
CVE-2015-2464	3.3 yrs
CVE-2015-2461	4.7 yrs
CVE-2015-2397	1.7 yrs
CVE-2015-1662	4.0 yrs
CVE-2015-0090	1.4 yrs
CVE-2015-0086	4.6 yrs
CVE-2014-6369	1.1 yrs

JavaScript *Newest AOTT*

Microsoft (cont)

CVE-2014-6343	3.6 yrs
CVE-2014-6332	0.4 yrs
CVE-2014-2799	0.5 yrs
CVE-2014-2797	0.7 yrs
CVE-2014-1811	4.8 yrs
CVE-2014-1761	1.3 yrs
CVE-2013-3906	1.2 yrs
CVE-2013-3893	0.7 yrs
CVE-2013-3163	0.5 yrs
CVE-2013-1331	3.7 yrs
CVE-2013-1347	2.6 yrs
CVE-2013-1313	0.5 yrs
CVE-2013-0026	6.9 yrs
CVE-2013-0025	6.9 yrs
CVE-2012-4781	6.7 yrs
CVE-2012-2522	0.8 yrs
CVE-2012-1891	1.5 yrs
CVE-2012-1879	6.2 yrs
CVE-2012-1878	6.2 yrs
CVE-2012-1876	6.2 yrs
CVE-2012-1875	6.2 yrs
CVE-2012-0171	6.1 yrs
CVE-2012-0170	6.1 yrs
CVE-2012-0169	6.1 yrs
CVE-2012-0159	1.6 yrs
CVE-2012-0158	2.7 yrs
CVE-2012-0155	5.9 yrs
CVE-2012-0016	1.1 yrs
CVE-2012-0011	5.9 yrs
CVE-2012-0003	0.3 yrs

VBScript *X-Force internal find*

NGINX

CVE-2014-3556	3.1 yrs
CVE-2013-2070	8.2 yrs

Novell

CVE-2015-0779	3.0 yrs
CVE-2012-0271	0.6 yrs

NTP

CVE-2013-5211	0.5 yrs

Oracle

CVE-2013-2465	0.8 yrs
CVE-2013-2463	0.8 yrs
CVE-2013-2431	8.2 yrs
CVE-2013-0431	0.3 yrs
CVE-2013-0422	7.9 yrs
BID-56791	1.5 yrs
BID-56772	1.6 yrs
CVE-2012-3342	0.3 yrs

PHP

CVE-2015-4022	7.2 yrs
CVE-2014-4049	5.5 yrs

PowerDNS

CVE-2015-1868	10.2 yrs

Samba

CVE-2014-0239	0.8 yrs

Squid

CVE-2013-4115	8.4 yrs

AOTT coverage with **MOV_Container_Overflow**

released April 10, 2007

detects malformed QuickTime (.mov) files having an atom whose size exceeds its container size

1: QuickTime
Protocol anomaly

2007: Protocol signature MOV_Container_Overflow (no CVE, no known exploits)

2009: Microsoft DirectX QuickTime code execution, CVE-2009-1539

```
00000000: moov <0> atomSize=0x0000018b, extent=0x0000018b
00000008: trak  <1> atomSize=0x00000178, extent=0x00000180
00000010: tkhd   <2> atomSize=0x0000005c, extent=0x0000006c
0000006c: mdia   <2> atomSize=0x000000f0, extent=0x0000015c
00000074: mdhd    <3> atomSize=0x00000020, extent=0x00000094
00000094: hdlr    <3> atomSize=0x00000024, extent=0x000000b8
000000b8: minf    <3> atomSize=0x000000a4, extent=0x0000015c
000000c0: stbl     <4> atomSize=0x0000009c, extent=0x0000015c
000000c8: stsd      <5> atomSize=0x00000020, extent=0x000000e8
000000d8: AAAA       <6> atomSize=0x41414141, extent=0x41414219
000000e8: stts      <5> atomSize=0x00000030, extent=0x00000118
```

atom overflows container

2012: Real Networks RealPlayer .mp4 code execution, CVE-2012-1904

```
000001b7: stsd      <5> atomSize=0x0000005b, extent=0x00000212
000001c7: mp4a       <6> atomSize=0x6200004b, extent=0x62000212
```

atom overflows container

2014: Adobe Flash Player and Adobe Air code execution, CVE-2014-8438

```
00007a7a: stsd      <5> atomSize=0x00000096, extent=0x00007b10
00007a8a: avc1       <6> atomSize=0x00f00086, extent=0x00f07b10
```

atom overflows container

2015: Google Android Stagefright media engine covr integer underflow, CVE-2015-3827

```
00000020: stbl  <1> atomSize=0x00010010, extent=0x00010030
00000028: covr   <2> atomSize=0x00000017, extent=0x0000003f
0000003f: ====   <2> atomSize=0xf0f0f0f0, extent=0xf0f0f12f
```

atom overflows container

AOTT coverage with **Script_DOM_Unconditional_Undo**

2: JavaScript
newest AOTT

released June 9, 2015

detects a web script using .execCommand() followed unconditionally by .execCommand('Undo')

2015: Microsoft Internet Explorer code execution, CVE-2015-1753
Reported: June 9, 2015

```
text.execCommand("…");                    [details under NDA]
text….
document.execCommand("Undo");
```

2015: Microsoft Internet Explorer code execution, CVE-2015-6142
Microsoft Internet Explorer code execution, CVE-2015-6143
Reported: Dec 8, 2015

```
document.execCommand("…");                [details under NDA]
document….
document.execCommand("Undo");
```

2016: Microsoft Internet Explorer code execution, CVE-2016-0103

Reported: Mar 8, 2016

```
…                                         [details under NDA]
….execCommand("Delete", false, null);
document.execCommand("Undo", false);
```

AOTT coverage with **Zip_Directory_Traversal**

3: ZIP
history repeats

released May 9, 2006

detects a 'zip' file having a filename containing "../" or "..\"

file=../../../../ROOT/f4pbhNrwDT9dQt7QLY3Aq8Fc53Yn9Zh.jsp

2006: IBM Lotus Notes compressed file preview directory traversal, CVE-2005-2619
Reported: February 10, 2006
A remote attacker could traverse directories and delete arbitrary files.

2010: Apache Tomcat WAR directory traversal, CVE-2009-2693
Reported: January 25, 2010
A remote attacker could create arbitrary files on the system outside of the Web root.

2013: Multiple HP products code execution, CVE-2012-5201
Reported: March 7, 2013
An attacker could execute arbitrary code on the system with SYSTEM privileges.

2015: ManageEngine ServiceDesk uploaded files code execution, SecChkId 105842 (no CVE)
Reported: August 20, 2015
An attacker could execute arbitrary code on the system.

AOTT coverage with **Script_Array_Overflow**

released June 11, 2014

detects VBScript code that overflows an array

4: VBScript
internal find

CVE-2014-6332 **Microsoft OLE automation array code execution**

"Unicorn" *arbitrary code execution caused by improperly accessing an object in memory*

2014

May	June	July	Aug	Sep	Oct	Nov

May 12: Vulnerability Discovered
X-Force researcher Robert Freeman finds the issue

May 16: Private Disclosure
Robert discloses to Microsoft and demonstrates RCE.
Microsoft determines "not in wild" and sets schedule

June 11: X-Force Blocking Coverage
Release of PAM signature
Script_Array_Overflow

Nov 11: Public Disclosure/Patch
Microsoft Super Tuesday includes **CVE-2014-6332**

Nov 13: Metasploit Public Exploit

Pattern Matching vs. Deep Packet Inspection

Advantages: Pattern Matching vs. Deep Packet Inspection

Rules-based Pattern Matching

- Customization and collaboration
- Faster time-to-market for new coverage
- Visibility of detection logic
  - *But, hackers have visibility too!*

Deep Packet Inspection (PAM)

- Ahead of the Threat coverage
- Fewer false negatives (mutation detection)
- Detection of traffic on unexpected ports via protocol heuristics
- Protocol anomaly signatures
  (MOV_Container_Overflow, TLS_Zero_Length_Record)
- Heuristics-based signatures
  (SQL Injection, Java_Malicious_Applet, Script_Suspicious_Score)
- Shellcode heuristics
  (PDF_Shellcode_Detected, JavaScript_Shellcode_Detected)
- Flood detection and mitigation
  (DNS_Dot_Query_Flood, SMB_Mass_Login, Syslog_Flood)
- Complex data leakage protection
  (social security AND credit card in any order)

X-Force Top 100 Ahead of the Threat Coverage

Blocking coverage at least 90 days ahead of the threat for notable vendors since 2012 with CVSS >=5

Average AOTT = 3.8 yrs Average CVSS base = 8.6

Adobe

CVE-2015-5097	5.1 yrs
CVE-2014-8438	7.6 yrs
CVE-2013-3346	1.3 yrs
CVE-2013-2729	7.2 yrs
CVE-2013-2555	0.7 yrs
CVE-2013-0634	1.8 yrs
CVE-2012-4170	7.5 yrs
CVE-2012-1535	1.4 yrs
CVE-2012-0769	0.9 yrs
CVE-2012-0768	0.9 yrs
BID-52632	7.0 yrs

QuickTime *Protocol anomaly*

Apache

CVE-2013-2251	2.4 yrs
CVE-2013-2135	2.3 yrs
CVE-2013-2134	2.3 yrs
CVE-2013-2115	2.3 yrs
CVE-2013-1966	2.3 yrs
CVE-2012-0838	1.0 yrs
CVE-2012-0391	0.9 yrs

Apple

CVE-2012-3753	0.8 yrs

CA

BID-51915	7.0 yrs

GNU

CVE-2015-0235	9.9 yrs

ISC

CVE-2012-3571	1.9 yrs
CVE-2012-3523	1.2 yrs

Google

CVE-2015-3864	8.4 yrs
CVE-2015-3829	8.3 yrs
CVE-2015-3828	8.3 yrs
CVE-2015-3827	6.5 yrs
CVE-2015-3826	8.3 yrs
CVE-2015-3824	8.3 yrs
CVE-2015-1539	8.3 yrs
CVE-2015-1538	8.3 yrs
BID-52632	7.0 yrs

HP

CVE-2014-7883	1.1 yrs
CVE-2014-2625	9.4 yrs
CVE-2014-2621	1.1 yrs
CVE-2014-2620	1.2 yrs
CVE-2014-2617	1.9 yrs
CVE-2013-6195	0.3 yrs
CVE-2013-4799	5.9 yrs
CVE-2012-5201	6.8 yrs

ZIP *History repeats*

Microsoft

CVE-2016-0103	0.8 yrs
CVE-2015-6143	0.5 yrs
CVE-2015-6142	0.5 yrs
CVE-2015-6150	1.4 yrs
CVE-2015-6087	4.6 yrs
CVE-2015-2464	3.3 yrs
CVE-2015-2461	4.7 yrs
CVE-2015-2397	1.7 yrs
CVE-2015-1662	4.0 yrs
CVE-2015-0090	1.4 yrs
CVE-2015-0086	4.6 yrs
CVE-2014-6369	1.1 yrs

JavaScript *Newest AOTT*

Microsoft (cont)

CVE-2014-6343	3.6 yrs
CVE-2014-6332	0.4 yrs
CVE-2014-2799	0.5 yrs
CVE-2014-2797	0.7 yrs
CVE-2014-1811	4.8 yrs
CVE-2014-1761	1.3 yrs
CVE-2013-3906	1.2 yrs
CVE-2013-3893	0.7 yrs
CVE-2013-3163	0.5 yrs
CVE-2013-1331	3.7 yrs
CVE-2013-1347	2.6 yrs
CVE-2013-1313	0.5 yrs
CVE-2013-0026	6.9 yrs
CVE-2013-0025	6.9 yrs
CVE-2012-4781	6.7 yrs
CVE-2012-2522	0.8 yrs
CVE-2012-1891	1.5 yrs
CVE-2012-1879	6.2 yrs
CVE-2012-1878	6.2 yrs
CVE-2012-1876	6.2 yrs
CVE-2012-1875	6.2 yrs
CVE-2012-0171	6.1 yrs
CVE-2012-0170	6.1 yrs
CVE-2012-0169	6.1 yrs
CVE-2012-0159	1.6 yrs
CVE-2012-0158	2.7 yrs
CVE-2012-0155	5.9 yrs
CVE-2012-0016	1.1 yrs
CVE-2012-0011	5.9 yrs
CVE-2012-0003	0.3 yrs

VBScript *X-Force internal find*

NGINX

CVE-2014-3556	3.1 yrs
CVE-2013-2070	8.2 yrs

Novell

CVE-2015-0779	3.0 yrs
CVE-2012-0271	0.6 yrs

NTP

CVE-2013-5211	0.5 yrs

Oracle

CVE-2013-2465	0.8 yrs
CVE-2013-2463	0.8 yrs
CVE-2013-2431	8.2 yrs
CVE-2013-0431	0.3 yrs
CVE-2013-0422	7.9 yrs
BID-56791	1.5 yrs
BID-56772	1.6 yrs
CVE-2012-3342	0.3 yrs

PHP

CVE-2015-4022	7.2 yrs
CVE-2014-4049	5.5 yrs

PowerDNS

CVE-2015-1868	10.2 yrs

Samba

CVE-2014-0239	0.8 yrs

Sun

CVE-2013-4115	8.4 yrs

Same 4 examples for Pattern Matching

Pattern Matching: False Negative

2009: Microsoft DirectX QuickTime code execution, CVE-2009-1539

1: QuickTime
Protocol anomaly

PAM signature (2007):
MOV_Container_Overflow

```
if ((state->depth > 0) && (extent > state->atomExtent[state->depth-1]))
```

Snort coverage:

```
… flow:to_client,established; file_data; content:"AAAAAAAA|00 00 00|0stts|04 00 00 00|"; …
```

2009 PoC:

```
00000000: moov <0> atomSize=0x0000018b, extent=0x0000018b
00000008: trak  <1> atomSize=0x00000178, extent=0x00000180
00000010: tkhd   <2> atomSize=0x0000005c, extent=0x0000006c
0000006c: mdia   <2> atomSize=0x000000f0, extent=0x0000015c
00000074: mdhd    <3> atomSize=0x00000020, extent=0x00000094
00000094: hdlr    <3> atomSize=0x00000024, extent=0x000000b8
000000b8: minf    <3> atomSize=0x000000a4, extent=0x0000015c
000000c0: stbl     <4> atomSize=0x0000009c, extent=0x0000015c
000000c8: stsd      <5> atomSize=0x00000020, extent=0x000000e8
000000d8: AAAA       <6> atomSize=0x41414141, extent=0x41414219
000000e8: stts      <5> atomSize=0x00000030, extent=0x00000118
```

overflow →

Known Exploit:

```
00000000: moov <0> atomSize=0x00000480, extent=0x00000480
00000008: mvhd  <1> atomSize=0x0000001c, extent=0x00000024
00000024: trak  <1> atomSize=0x00000322, extent=0x00000346
0000002c: tkhd   <2> atomSize=0x0000026c, extent=0x00000298
00000298: mdia   <2> atomSize=0x0000011e, extent=0x000003b6
000002a0: mdhd    <3> atomSize=0x000000ff, extent=0x0000039f
00000346: AAAA  <1> atomSize=0x41414141, extent=0x41414487
00000480: XXXX <0> atomSize=0x58585858, extent=0x58585cd8
```

overflow →

Pattern Matching: A rule for each exploit

2015-2016: Related Microsoft IE code execution vulnerabilities

2: JavaScript
newest AOTT

PAM signature (2015):
Script_DOM_Unconditional_Undo

```
if (state->saw_execCommand && execCommandVulnerable && isUndo)
```

Snort coverage:

CVE-2015-1753 Reported: June 9, 2015

```
… flow:to_server,established; file_data; … content:".execCommand"; within:100; nocase; …
nocase; content:".scrollIntoView"; within:100; nocase; content:".execCommand"; nocase;
content:"Undo"; within:25; nocase; …
```

CVE-2015-6142 Reported: Dec 8, 2015

```
… flow:to_server,established; file_data; content:"ms-beginUndoUnit"; fast_pattern:only;
content:"execCommand"; nocase; content:"undo"; within:10; nocase; …
```

CVE-2015-6143 Reported: Dec 8, 2015

```
… flow:to_server,established; file_data; content:".addEventListener"; nocase;
content:"DOMAttrModified"; within:25; nocase; content:".execCommand"; nocase; … nocase;
content:".execCommand"; nocase; content:"undo"; within:15; nocase; …
```

CVE-2016-0103 Reported: Mar 8, 2016 ???

Pattern Matching: Lack of Coverage

2006-2015: Related Zip Traversal vulnerabilities

3: ZIP
history repeats

PAM signature (2006):
Zip_Directory_Traversal

```
if (dirClimb(psom, &dirClimbState, zip->file.name, zip->file.nameLen))
```

Snort coverage:

2006: IBM Lotus Notes compressed file preview directory traversal, CVE-2005-2619

--- no Snort coverage ---

2010: Apache Tomcat WAR directory traversal, CVE-2009-2693

--- no Snort coverage ---

2013: Multiple HP products code execution, CVE-2012-5201

```
… flow:to_server,established; content:"/imc/webdm/mibbrowser/mibFileUpload";
fast_pattern:only; http_uri; content:"..|5C|..|5C|..|5C|..|5C|"; http_client_body; …

… flow:to_server,established; content:"/imc/webdm/mibbrowser/mibFileUpload";
fast_pattern:only; http_uri; content:"../../../../"; http_client_body; …
```

2015: ManageEngine ServiceDesk code execution, SecChkId 105842 (no CVE)

--- no Snort coverage ---

Pattern Matching: Large Rule Set

Microsoft OLE automation array code execution, CVE-2014-6332, “Unicorn”

4: VBScript
internal find

PAM signature (2014):
Script_Array_Overflow

```
int32 newArraySize = jcalc(args, len, NULL, NULL);
if ((newArraySize > threshold)
    || (state->builtChrwString && (state->suspiciousTraits & STmask(ST_Shell_Exec))))
```

Snort coverage (14 rules):

```
./rules/browser-ie.rules:alert tcp $EXTERNAL_NET any -> $SMTP_SERVERS 25 (msg:"BROWSER-IE Microsoft Internet Explorer 11 VBScript redim preserve denial-of-service attempt"; flow:to_server,established; file_data; content:"redim";
nocase; content:"preserve"; within:20; nocase; content:"(&h"; within:20; byte_test:6,>,1000,0,relative,string,hex; metadata:policy balanced-ips drop, policy max-detect-ips drop, policy security-ips drop, service smtp;
reference:cve,2014-6332; reference:url,technet.microsoft.com/en-us/security/bulletin/ms14-064; classtype:attempted-dos; sid:32473; rev:4;)
./rules/browser-ie.rules:alert tcp $EXTERNAL_NET any -> $SMTP_SERVERS 25 (msg:"BROWSER-IE Microsoft Internet Explorer 11 VBScript redim preserve denial-of-service attempt"; flow:to_server,established; file_data; content:"redim";
nocase; content:"preserve"; within:20; nocase; content:"("; within:20; byte_test:6,>,1000,0,relative,string,dec; metadata:policy balanced-ips drop, policy max-detect-ips drop, policy security-ips drop, service smtp;
reference:cve,2014-6332; reference:url,technet.microsoft.com/en-us/security/bulletin/ms14-064; classtype:attempted-dos; sid:32472; rev:4;)
./rules/browser-ie.rules:alert tcp $EXTERNAL_NET $FILE_DATA_PORTS -> $HOME_NET any (msg:"BROWSER-IE Microsoft Internet Explorer 11 VBScript redim preserve denial-of-service attempt"; flow:to_client,established; file_data;
content:"redim"; nocase; content:"preserve"; within:20; nocase; content:"(&h"; within:20; byte_test:6,>,1000,0,relative,string,hex; metadata:policy balanced-ips drop, policy max-detect-ips drop, policy security-ips drop, service
ftp-data, service http, service imap, service pop3; reference:cve,2014-6332; reference:url,technet.microsoft.com/en-us/security/bulletin/ms14-064; classtype:attempted-dos; sid:32471; rev:4;)
./rules/browser-ie.rules:alert tcp $EXTERNAL_NET $FILE_DATA_PORTS -> $HOME_NET any (msg:"BROWSER-IE Microsoft Internet Explorer 11 VBScript redim preserve denial-of-service attempt"; flow:to_client,established; file_data;
content:"redim"; nocase; content:"preserve"; within:20; nocase; content:"("; within:20; byte_test:6,>,1000,0,relative,string,dec; metadata:policy balanced-ips drop, policy max-detect-ips drop, policy security-ips drop, service
ftp-data, service http, service imap, service pop3; reference:cve,2014-6332; reference:url,technet.microsoft.com/en-us/security/bulletin/ms14-064; classtype:attempted-dos; sid:32470; rev:4;)
./rules/browser-ie.rules:alert tcp $EXTERNAL_NET any -> $SMTP_SERVERS 25 (msg:"BROWSER-IE Microsoft Internet Explorer 11 VBScript redim preserve denial-of-service attempt"; flow:to_server,established; file_data;
content:"myarray"; content:"chrw"; within:10; content:"chrw"; within:20; content:"32767"; within:10; metadata:policy balanced-ips drop, policy max-detect-ips drop, policy security-ips drop, service smtp; reference:cve,2014-6332;
reference:url,technet.microsoft.com/en-us/security/bulletin/ms14-064; classtype:attempted-dos; sid:32565; rev:4;)
./rules/browser-ie.rules:alert tcp $EXTERNAL_NET $FILE_DATA_PORTS -> $HOME_NET any (msg:"BROWSER-IE Microsoft Internet Explorer 11 VBScript redim preserve denial-of-service attempt"; flow:to_client,established; file_data;
content:"myarray"; content:"chrw"; within:10; content:"chrw"; within:20; content:"32767"; within:10; metadata:policy balanced-ips drop, policy max-detect-ips drop, policy security-ips drop, service ftp-data, service http,
service imap, service pop3; reference:cve,2014-6332; reference:url,technet.microsoft.com/en-us/security/bulletin/ms14-064; classtype:attempted-dos; sid:32564; rev:4;)
./rules/browser-ie.rules:alert tcp $EXTERNAL_NET any -> $SMTP_SERVERS 25 (msg:"BROWSER-IE Microsoft Internet Explorer 11 VBScript redim preserve denial-of-service attempt"; flow:to_server,established; file_data; content:"redim
Preserve arr(&h8000002)"; fast_pattern:only; metadata:policy balanced-ips drop, policy security-ips drop, service smtp; reference:cve,2014-6332; reference:url,technet.microsoft.com/en-us/security/bulletin/ms14-064;
classtype:attempted-dos; sid:32630; rev:2;)
./rules/browser-ie.rules:alert tcp $EXTERNAL_NET $FILE_DATA_PORTS -> $HOME_NET any (msg:"BROWSER-IE Microsoft Internet Explorer 11 VBScript redim preserve denial-of-service attempt"; flow:to_client,established; file_data;
content:"redim  Preserve arr(&h8000002)"; fast_pattern:only; metadata:policy balanced-ips drop, policy security-ips drop, service ftp-data, service http, service imap, service pop3; reference:cve,2014-6332;
reference:url,technet.microsoft.com/en-us/security/bulletin/ms14-064; classtype:attempted-dos; sid:32629; rev:2;)
./rules/browser-ie.rules:alert tcp $EXTERNAL_NET any -> $SMTP_SERVERS 25 (msg:"BROWSER-IE Microsoft Internet Explorer 11 VBScript redim preserve denial-of-service attempt"; flow:to_server,established; file_data;
content:"HIvIauuKF6i9p*qI1wE8J*znjk3Yl8td"; fast_pattern:only; metadata:policy balanced-ips drop, policy security-ips drop, service smtp; reference:cve,2014-6332; reference:url,technet.microsoft.com/en-us/security/bulletin/ms14-
064; classtype:attempted-dos; sid:33116; rev:2;)
./rules/browser-ie.rules:alert tcp $EXTERNAL_NET $FILE_DATA_PORTS -> $HOME_NET any (msg:"BROWSER-IE Microsoft Internet Explorer 11 VBScript redim preserve denial-of-service attempt"; flow:to_client,established; file_data;
content:"HIvIauuKF6i9p*qI1wE8J*znjk3Yl8td"; fast_pattern:only; metadata:policy balanced-ips drop, policy security-ips drop, service ftp-data, service http, service imap, service pop3; reference:cve,2014-6332;
reference:url,technet.microsoft.com/en-us/security/bulletin/ms14-064; classtype:attempted-dos; sid:33115; rev:2;)
./rules/browser-ie.rules:alert tcp $EXTERNAL_NET any -> $SMTP_SERVERS 25 (msg:"BROWSER-IE Microsoft Internet Explorer 11 VBScript redim preserve denial-of-service attempt"; flow:to_server,established; file_data; content:"76723";
content:"wrhc"; within:10; content:"wrhc"; within:20; content:"yarraym"; within:10; metadata:policy balanced-ips drop, policy security-ips drop, service smtp; reference:cve,2014-6332; reference:url,technet.microsoft.com/en-
us/security/bulletin/ms14-064; classtype:attempted-dos; sid:33980; rev:1;)
./rules/browser-ie.rules:alert tcp $EXTERNAL_NET $FILE_DATA_PORTS -> $HOME_NET any (msg:"BROWSER-IE Microsoft Internet Explorer 11 VBScript redim preserve denial-of-service attempt"; flow:to_client,established; file_data;
content:"76723"; content:"wrhc"; within:10; content:"wrhc"; within:20; content:"yarraym"; within:10; metadata:policy balanced-ips drop, policy security-ips drop, service ftp-data, service http, service imap, service pop3;
reference:cve,2014-6332; reference:url,technet.microsoft.com/en-us/security/bulletin/ms14-064; classtype:attempted-dos; sid:33979; rev:1;)
./rules/browser-ie.rules:# alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"BROWSER-IE Microsoft Internet Explorer 11 VBScript redim preserve denial-of-service attempt"; flow:to_client,established; content:"new ActiveXObject";
content:"WScript.Shell"; within:30; content:"Run("; within:30; metadata:policy max-detect-ips drop, policy security-ips drop, service http; reference:cve,2014-6332; reference:url,technet.microsoft.com/en-
us/security/bulletin/ms14-064; classtype:attempted-user; sid:36896; rev:1;)
./rules/exploit-kit.rules:# alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"EXPLOIT-KIT Known exploit kit obfuscation routine detected"; flow:to_client,established; content:"vbscript>"; content:"=Split("; within:40;
content:"UBound("; within:40; content:"+Chrw(eval("; within:40; content:"End Function"; within:40; metadata:policy max-detect-ips drop, policy security-ips drop, service http; reference:cve,2014-6332; classtype:attempted-user;
sid:36824; rev:1;)
```

Powered by PAM provides broad threat coverage

Comprehensive protection, visibility, and control over network traffic

Deep Packet Inspection

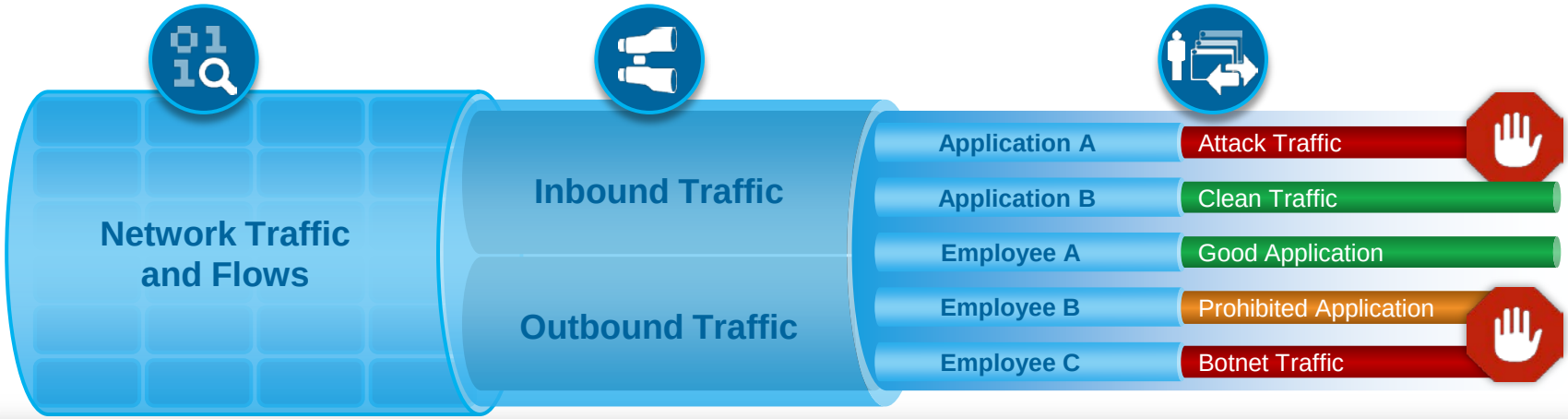
Fully classifies network traffic, regardless of address, port, or protocol

SSL Visibility

Identifies inbound and outbound traffic threats, without needing a separate appliance

Identity and Application Awareness

Associates users and groups with their network activity, application usage and actions



500+	25+ Billion	2,000+
Protocols and file formats analyzed	URLs classified in 70 categories	Applications and actions identified

IBM X-Force monitors and analyzes the changing threat landscape

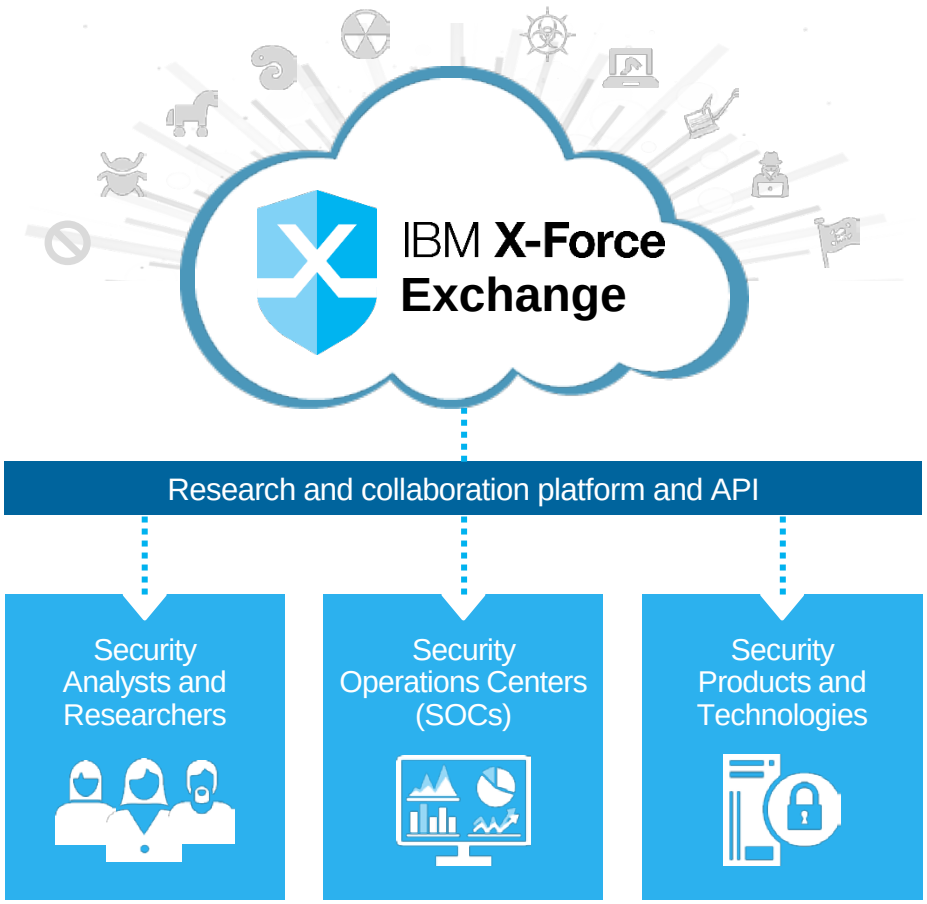
Coverage

20,000+ devices under contract
15B+ events managed per day
133 monitored countries (MSS)
1,000+ security related patents
100M+ customers protected from fraudulent transactions

Depth

25B analyzed web pages & images
8M spam & phishing attacks daily
89K documented vulnerabilities
860K malicious IP addresses
Millions of unique malware samples

IBM X-Force® Exchange



A platform to discover, collaborate, and act on threat intelligence

IBM X-Force Exchange is

OPEN
a robust platform with access to a wealth of threat intelligence data

SOCIAL
a collaborative platform for sharing threat intelligence

ACTIONABLE
an integrated solution to help quickly stop threats

Backed by the reputation and scale of IBM X-Force

IBM Security

THANK YOU

FOLLOW US ON:

- ibm.com/security
- securityintelligence.com
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions

IBM