Security in Software Design and Implementation

Lightning Talk by Trey Blalock
North Seattle Tech Talks
October 15th, 2018

Quick Discussion on Attack Automation for Conversational Perspective.

Asymmetric Warfare

Background Discussion

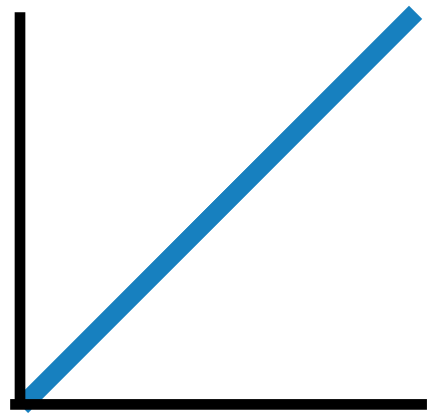
1 SQL-injection vs. 20 million lines of defensive code

$100.00 computer vs. $100 Million in defenses

1 economic DDoS script vs. $1 Million in wasted expenses

1:1,000,000

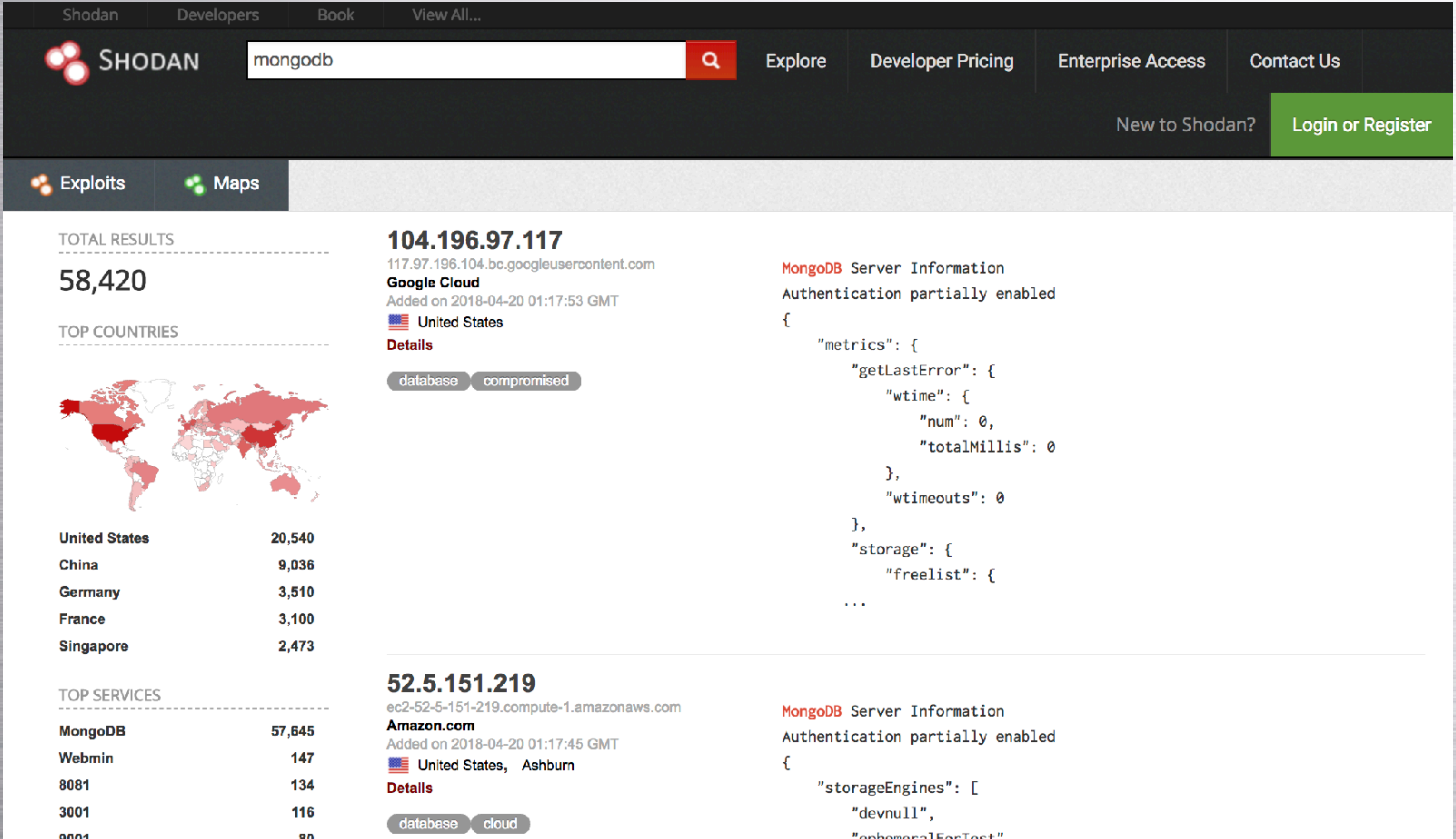
One match vs. a house



Background discussion on Reconnaissance

Shodan.io

Older method of getting global data



TOTAL RESULTS

58,420

TOP COUNTRIES

United States	20,540
China	9,036
Germany	3,510
France	3,100
Singapore	2,473

TOP SERVICES

MongoDB	57,645
Webmin	147
8081	134
3001	116
9001	80

104.196.97.117
117.97.196.104.bc.googleusercontent.com
Google Cloud
Added on 2018-04-20 01:17:53 GMT
🇺🇸 United States
Details

database compromised

```
MongoDB Server Information
Authentication partially enabled
{
    "metrics": {
        "getLastError": {
            "wtime": {
                "num": 0,
                "totalMillis": 0
            },
            "wtimeouts": 0
        },
        "storage": {
            "freelist": {
       ...
```

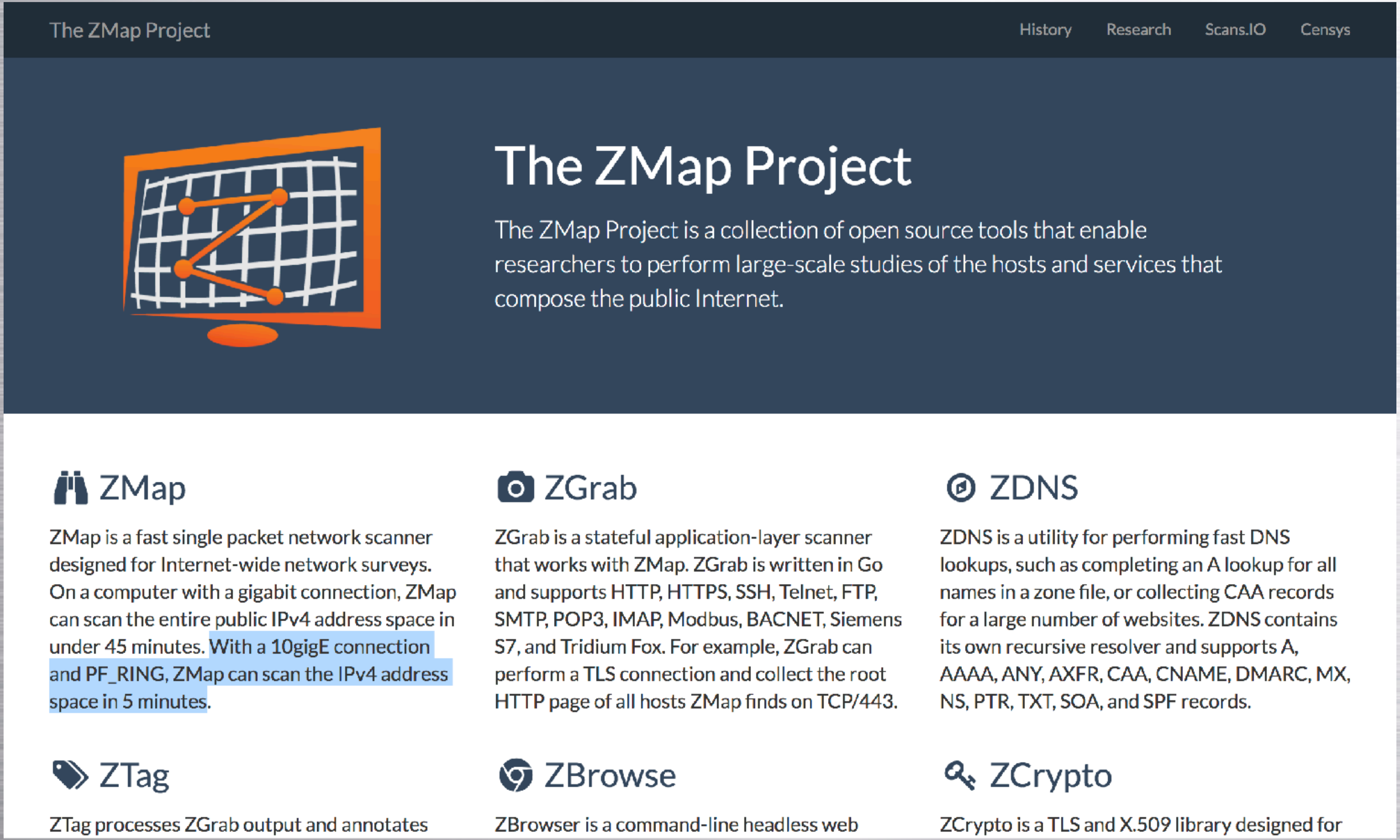
52.5.151.219
ec2-52-5-151-219.compute-1.amazonaws.com
Amazon.com
Added on 2018-04-20 01:17:45 GMT
🇺🇸 United States, Ashburn
Details

database cloud

```
MongoDB Server Information
Authentication partially enabled
{
    "storageEngines": [
        "devnull",
        "ephemeralForTest"
```

ZMAP.IO

Scan every IPv4 address in 5 Minutes



The ZMap Project

The ZMap Project is a collection of open source tools that enable researchers to perform large-scale studies of the hosts and services that compose the public Internet.

ZMap

ZMap is a fast single packet network scanner designed for Internet-wide network surveys. On a computer with a gigabit connection, ZMap can scan the entire public IPv4 address space in under 45 minutes. With a 10gigE connection and PF_RING, ZMap can scan the IPv4 address space in 5 minutes.

ZGrab

ZGrab is a stateful application-layer scanner that works with ZMap. ZGrab is written in Go and supports HTTP, HTTPS, SSH, Telnet, FTP, SMTP, POP3, IMAP, Modbus, BACNET, Siemens S7, and Tridium Fox. For example, ZGrab can perform a TLS connection and collect the root HTTP page of all hosts ZMap finds on TCP/443.

ZDNS

ZDNS is a utility for performing fast DNS lookups, such as completing an A lookup for all names in a zone file, or collecting CAA records for a large number of websites. ZDNS contains its own recursive resolver and supports A, AAAA, ANY, AXFR, CAA, CNAME, DMARC, MX, NS, PTR, TXT, SOA, and SPF records.

ZTag

ZTag processes ZGrab output and annotates

ZBrowse

ZBrowser is a command-line headless web

ZCrypto

ZCrypto is a TLS and X.509 library designed for

Masscan

https://github.com/robertdavidgraham/masscan

MASSCAN: Mass IP port scanner

This is the fastest Internet port scanner. It can scan the entire Internet in under 6 minutes, transmitting 10 million packets per second.

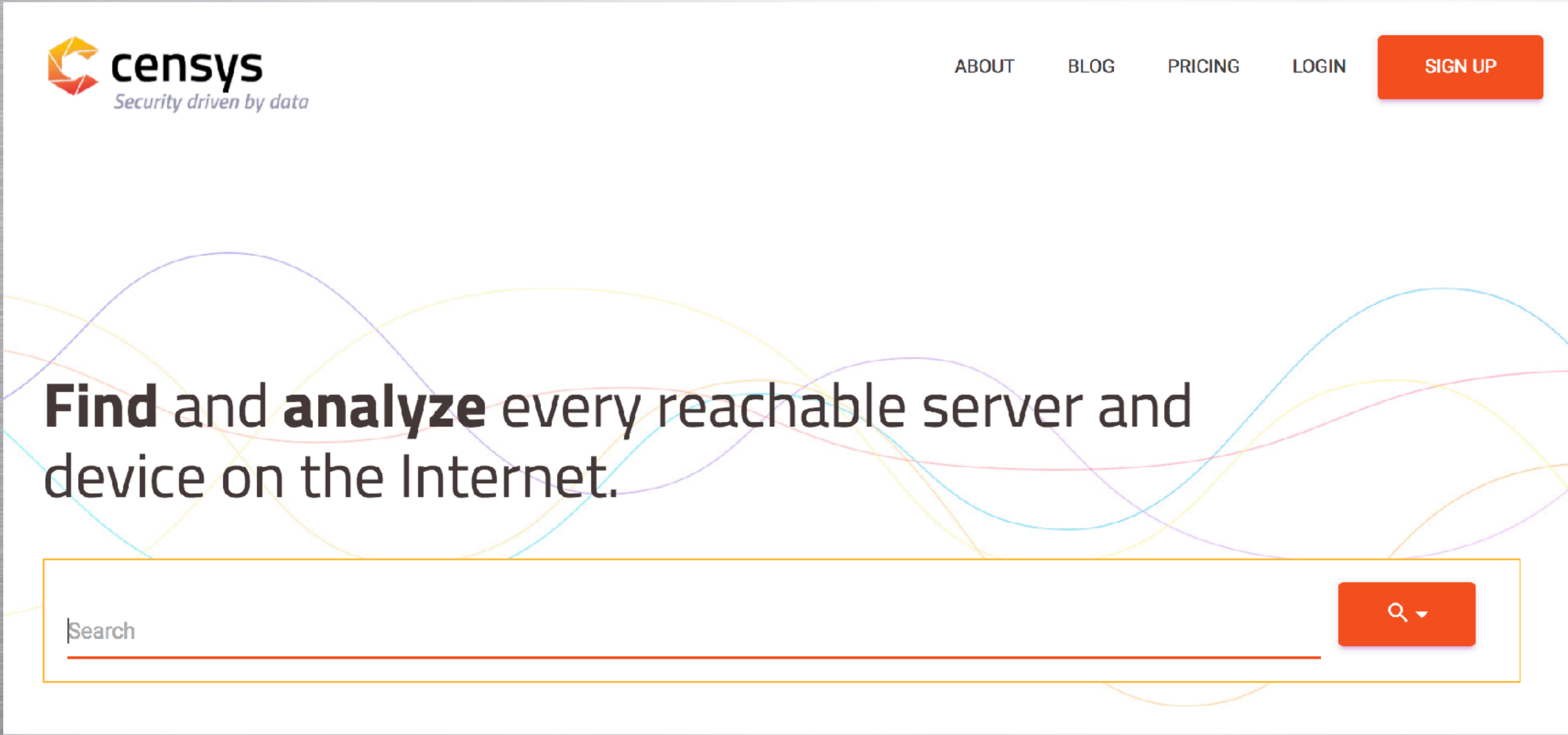
It produces results similar to `nmap`, the most famous port scanner. Internally, it operates more like `scanrand`, `unicornscan`, and `ZMap`, using asynchronous transmission. The major difference is that it's faster than these other scanners. In addition, it's more flexible, allowing arbitrary address ranges and port ranges.

NOTE: masscan uses a **custom TCP/IP stack**. Anything other than simple port scans will cause conflict with the local TCP/IP stack. This means you need to either use the `-S` option to use a separate IP address, or configure your operating system to firewall the ports that masscan uses.

This tool is free, but consider funding it here: 1MASSCANaHUiyTtR3bJ2sLGuMw5kDBaj4T

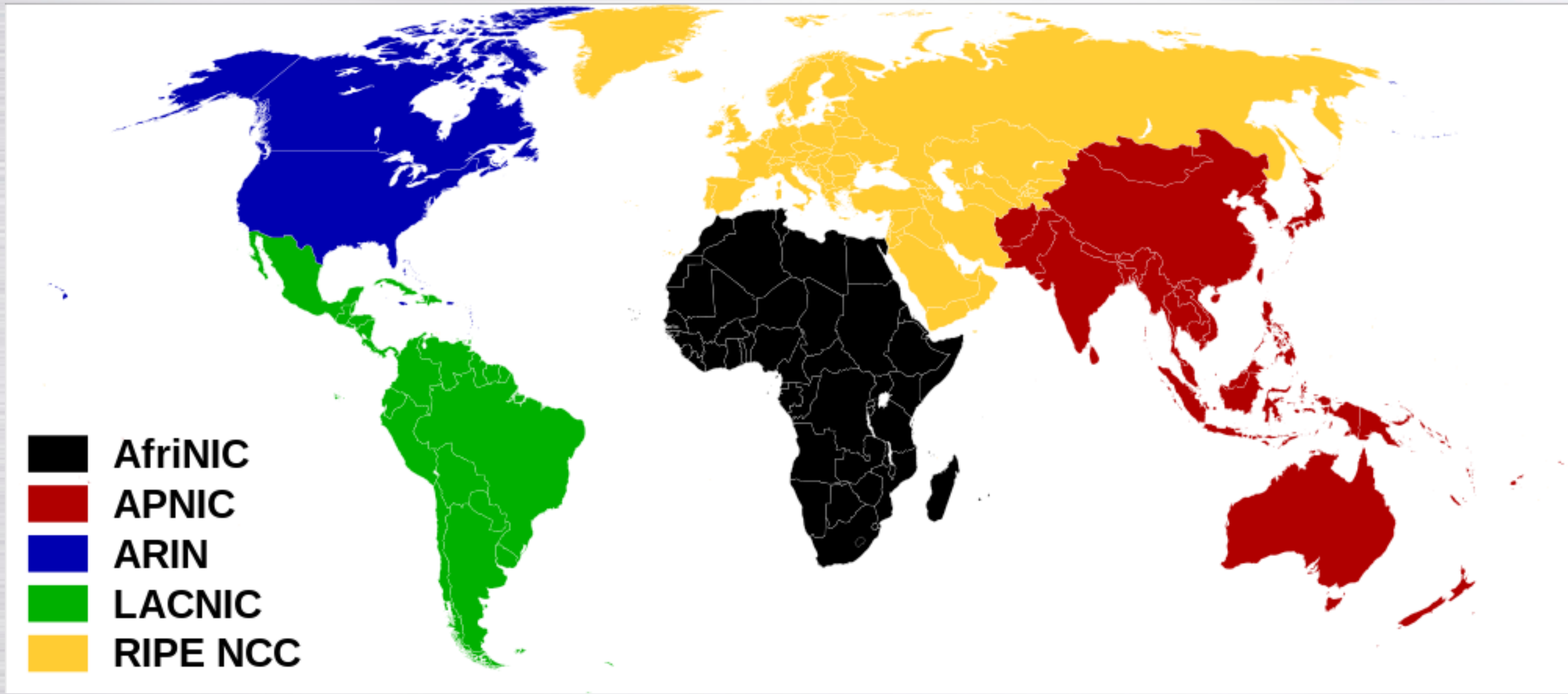
Censys

Many other public & private research groups like this.



Find and **analyze** every reachable server and device on the Internet.

Finding IP Ranges



Search the 5 Regional Internet Registries for BGP Autonomous System Number Information

Note: There are many other tricks to find and correlate IP’s

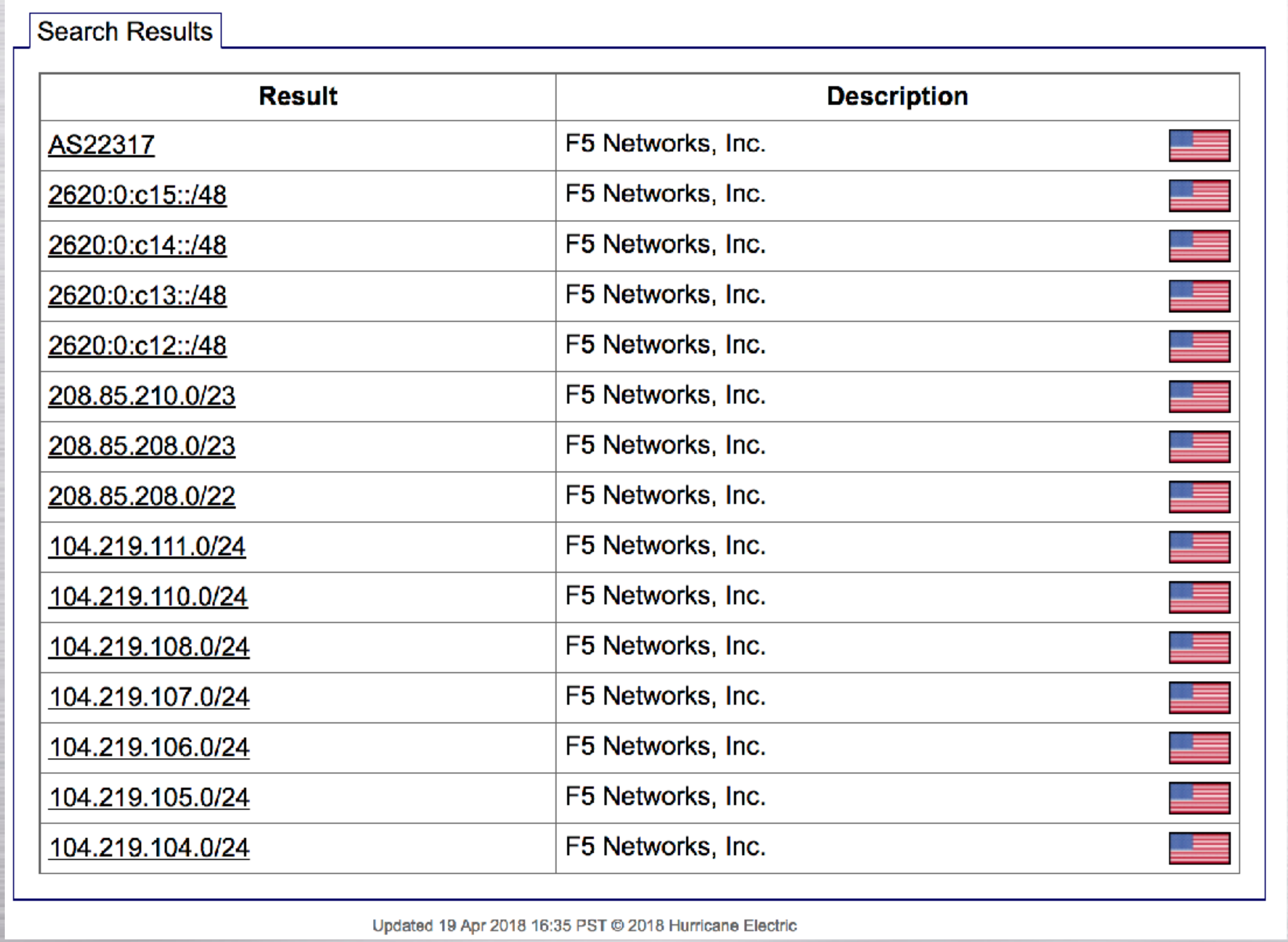
Finding IP addresses

Random Seattle-based Company

HURRICANE ELECTRIC
INTERNET SERVICES

Note: This won’t find all IP’s.

This is public data.



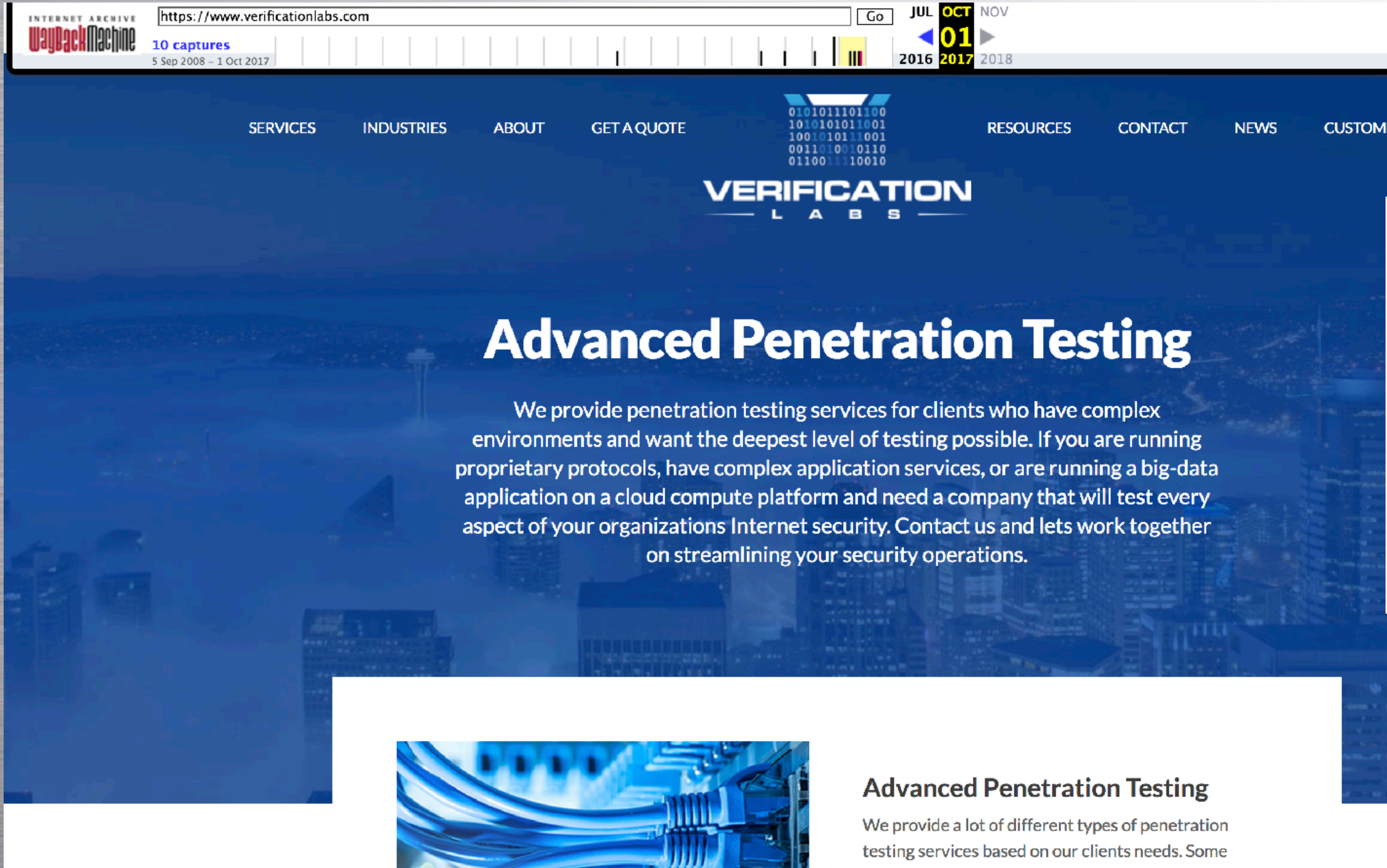
Search Results

Result	Description
AS22317	F5 Networks, Inc. 🇺🇸
2620:0:c15::/48	F5 Networks, Inc. 🇺🇸
2620:0:c14::/48	F5 Networks, Inc. 🇺🇸
2620:0:c13::/48	F5 Networks, Inc. 🇺🇸
2620:0:c12::/48	F5 Networks, Inc. 🇺🇸
208.85.210.0/23	F5 Networks, Inc. 🇺🇸
208.85.208.0/23	F5 Networks, Inc. 🇺🇸
208.85.208.0/22	F5 Networks, Inc. 🇺🇸
104.219.111.0/24	F5 Networks, Inc. 🇺🇸
104.219.110.0/24	F5 Networks, Inc. 🇺🇸
104.219.108.0/24	F5 Networks, Inc. 🇺🇸
104.219.107.0/24	F5 Networks, Inc. 🇺🇸
104.219.106.0/24	F5 Networks, Inc. 🇺🇸
104.219.105.0/24	F5 Networks, Inc. 🇺🇸
104.219.104.0/24	F5 Networks, Inc. 🇺🇸

Updated 19 Apr 2018 16:35 PST © 2018 Hurricane Electric

Wayback Machine

Grab code from 3rd party

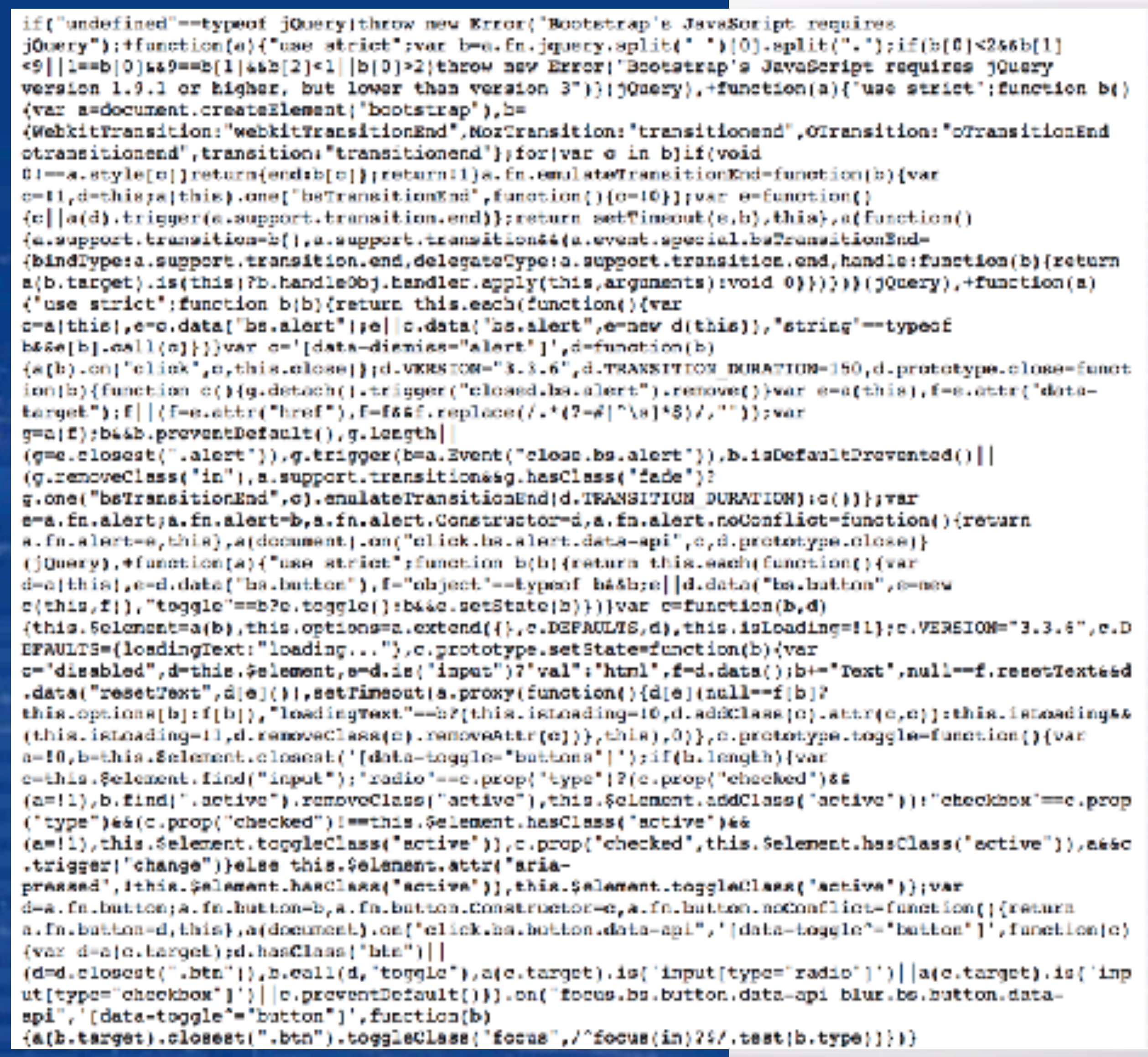


Advanced Penetration Testing

We provide penetration testing services for clients who have complex environments and want the deepest level of testing possible. If you are running proprietary protocols, have complex application services, or are running a big-data application on a cloud compute platform and need a company that will test every aspect of your organizations Internet security. Contact us and lets work together on streamlining your security operations.

Advanced Penetration Testing

We provide a lot of different types of penetration testing services based on our clients needs. Some

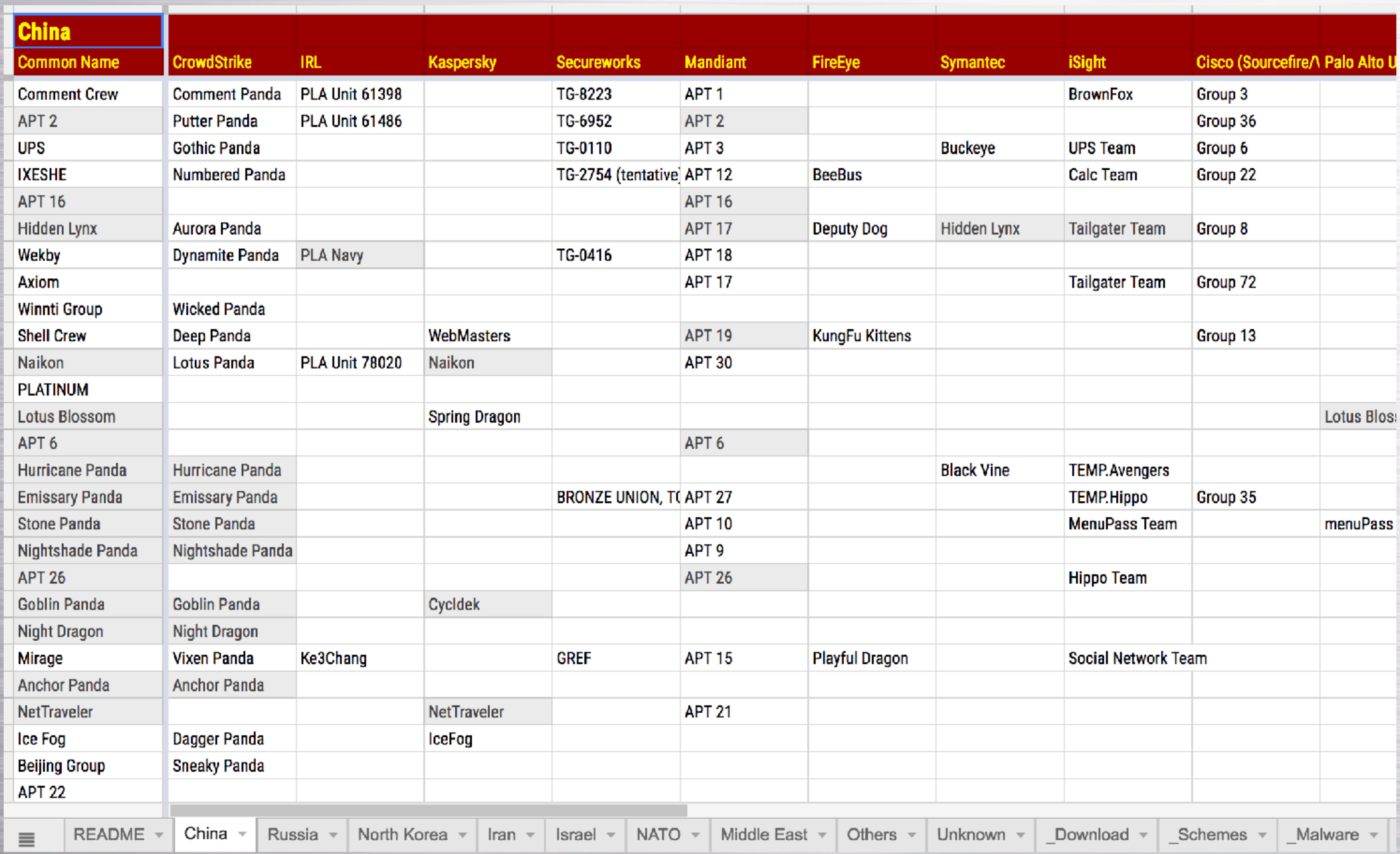


```
if("undefined"==typeof jQuery)throw new Error("Bootstrap's JavaScript requires
jQuery");+function(a){"use strict";var b=a.fn.jquery.split(" ")[0].split(".");if(b[0]<2&&b[1]
<9||1==b[0]&&9==b[1]&&b[2]<1||b[0]>2)throw new Error("Bootstrap's JavaScript requires jQuery
version 1.9.1 or higher, but lower than version 3")}(jQuery),+function(a){"use strict";function b()
{var a=document.createElement("bootstrap"),b=
{WebkitTransition:"webkitTransitionEnd",MozTransition:"transitionend",OTransition:"oTransitionEnd
otransitionend",transition:"transitionend"};for(var c in b)if(void
0!==a.style[c])return{end:b[c]};return!1}a.fn.emulateTransitionEnd=function(b){var
c=!1,d=this;a(this).one("bsTransitionEnd",function(){c=!0});var e=function()
{c||a(d).trigger(a.support.transition.end)};return setTimeout(e,b),this},a(function()
{a.support.transition=b(),a.support.transition&&(a.event.special.bsTransitionEnd=
{bindType:a.support.transition.end,delegateType:a.support.transition.end,handle:function(b){return
a(b.target).is(this)?b.handleObj.handler.apply(this,arguments):void 0}})})}(jQuery),+function(a)
{"use strict";function b(b){return this.each(function(){var
c=a(this),e=c.data("bs.alert");e||c.data("bs.alert",e=new d(this)),"string"==typeof
b&&e[b].call(c)})}var c='[data-dismiss="alert"]',d=function(b)
{a(b).on("click",c,this.close)};d.VERSION="3.3.6",d.TRANSITION_DURATION=150,d.prototype.close=funct
ion(b){function c(){g.detach().trigger("closed.bs.alert").remove()}var e=a(this),f=e.attr("data-
target");f||(f=e.attr("href"),f=f&&f.replace(/.*(?=#[^\s]*$)/,""));var
g=a(f);b&&b.preventDefault(),g.length||
(g=e.closest(".alert")),g.trigger(b=a.Event("close.bs.alert")),b.isDefaultPrevented()||
(g.removeClass("in"),a.support.transition&&g.hasClass("fade")?
g.one("bsTransitionEnd",c).emulateTransitionEnd(d.TRANSITION_DURATION):c())};var
e=a.fn.alert;a.fn.alert=b,a.fn.alert.Constructor=d,a.fn.alert.noConflict=function(){return
a.fn.alert=e,this},a(document).on("click.bs.alert.data-api",c,d.prototype.close)}
(jQuery),+function(a){"use strict";function b(b){return this.each(function(){var
d=a(this),e=d.data("bs.button"),f="object"==typeof b&&b;e||d.data("bs.button",e=new
c(this,f)),"toggle"==b?e.toggle():b&&e.setState(b)})}var c=function(b,d)
{this.$element=a(b),this.options=a.extend({},c.DEFAULTS,d),this.isLoading=!1};c.VERSION="3.3.6",c.D
EFAULTS={loadingText:"loading..."},c.prototype.setState=function(b){var
c="disabled",d=this.$element,e=d.is("input")?"val":"html",f=d.data();b+="Text",null==f.resetText&&d
.data("resetText",d[e]()),setTimeout(a.proxy(function(){d[e](null==f[b]?
this.options[b]:f[b]),"loadingText"==b?(this.isLoading=!0,d.addClass(c).attr(c,c)):this.isLoading&&
(this.isLoading=!1,d.removeClass(c).removeAttr(c))},this),0)},c.prototype.toggle=function(){var
a=!0,b=this.$element.closest('[data-toggle="buttons"]');if(b.length){var
c=this.$element.find("input");"radio"==c.prop("type")?(c.prop("checked")&&
(a=!1),b.find(".active").removeClass("active"),this.$element.addClass("active")):"checkbox"==c.prop
("type")&&(c.prop("checked")!==this.$element.hasClass("active")&&
(a=!1),this.$element.toggleClass("active")),c.prop("checked",this.$element.hasClass("active")),a&&c
.trigger("change")}else this.$element.attr("aria-
pressed",!this.$element.hasClass("active")),this.$element.toggleClass("active")};var
d=a.fn.button;a.fn.button=b,a.fn.button.Constructor=c,a.fn.button.noConflict=function(){return
a.fn.button=d,this},a(document).on("click.bs.button.data-api",'[data-toggle^="button"]',function(c)
{var d=a(c.target);d.hasClass("btn")||
(d=d.closest(".btn")),b.call(d,"toggle"),a(c.target).is('input[type="radio"]')||a(c.target).is('inp
ut[type="checkbox"]')||c.preventDefault()}).on("focus.bs.button.data-api blur.bs.button.data-
api",'[data-toggle^="button"]',function(b)
{a(b.target).closest(".btn").toggleClass("focus",/^focus(in)?$/.test(b.type))})}
```

Attack Automation at Scale

Quick Discussion on Attacking at Scale

Threat Actors have matured.



China										
Common Name	CrowdStrike	IRL	Kaspersky	Secureworks	Mandiant	FireEye	Symantec	iSight	Cisco (Sourcefire/\	Palo Alto U
Comment Crew	Comment Panda	PLA Unit 61398		TG-8223	APT 1			BrownFox	Group 3	
APT 2	Putter Panda	PLA Unit 61486		TG-6952	APT 2				Group 36	
UPS	Gothic Panda			TG-0110	APT 3		Buckeye	UPS Team	Group 6	
IXESHE	Numbered Panda			TG-2754 (tentative	APT 12	BeeBus		Calc Team	Group 22	
APT 16					APT 16					
Hidden Lynx	Aurora Panda				APT 17	Deputy Dog	Hidden Lynx	Tailgater Team	Group 8	
Wekby	Dynamite Panda	PLA Navy		TG-0416	APT 18					
Axiom					APT 17			Tailgater Team	Group 72	
Winnti Group	Wicked Panda									
Shell Crew	Deep Panda		WebMasters		APT 19	KungFu Kittens			Group 13	
Naikon	Lotus Panda	PLA Unit 78020	Naikon		APT 30					
PLATINUM										
Lotus Blossom			Spring Dragon							Lotus Bloss
APT 6					APT 6					
Hurricane Panda	Hurricane Panda						Black Vine	TEMP.Avengers		
Emissary Panda	Emissary Panda			BRONZE UNION, T(	APT 27			TEMP.Hippo	Group 35	
Stone Panda	Stone Panda				APT 10			MenuPass Team		menuPass
Nightshade Panda	Nightshade Panda				APT 9					
APT 26					APT 26			Hippo Team		
Goblin Panda	Goblin Panda		Cycldek							
Night Dragon	Night Dragon									
Mirage	Vixen Panda	Ke3Chang		GREF	APT 15	Playful Dragon		Social Network Team		
Anchor Panda	Anchor Panda									
NetTraveler			NetTraveler		APT 21					
Ice Fog	Dagger Panda		IceFog							
Beijing Group	Sneaky Panda									
APT 22										

Credit: @cyb3rops

Attack Automation at Scale

First Impact used to be recon…

Attack Automation at Scale

Now it’s a punch in the face

Think “working SQL-Injection attack pulling tables” as the first TCP packets coming in.

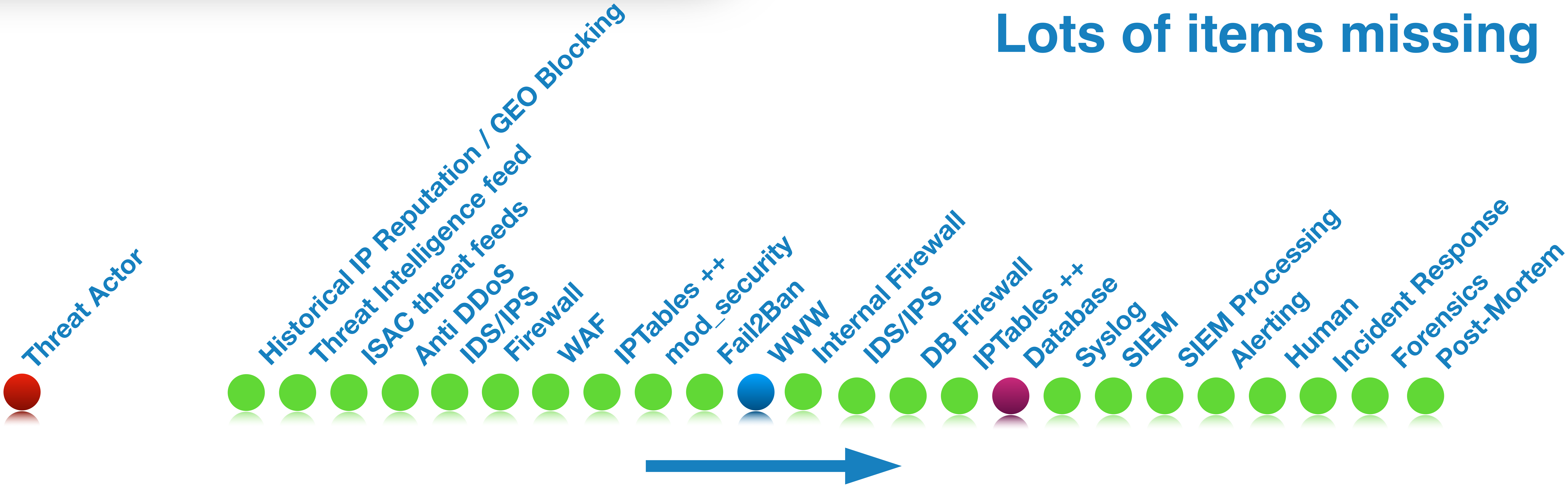
No time for humans to respond.

Weaponized bots scan the entire IPv4 space all the time.

Quick Discussion on Defense Automation.

External Attack Flow

Conversational Diagram
Lots of items missing



Threat Actor

Historical IP Reputation / GEO Blocking

Threat Intelligence feed

ISAC threat feeds

Anti DDoS

IDS/IPS

Firewall

WAF

IPTables ++

mod_security

Fail2Ban

WWW

Internal Firewall

IDS/IPS

DB Firewall

IPTables ++

Database

Syslog

SIEM

SIEM Processing

Alerting

Human

Incident Response

Forensics

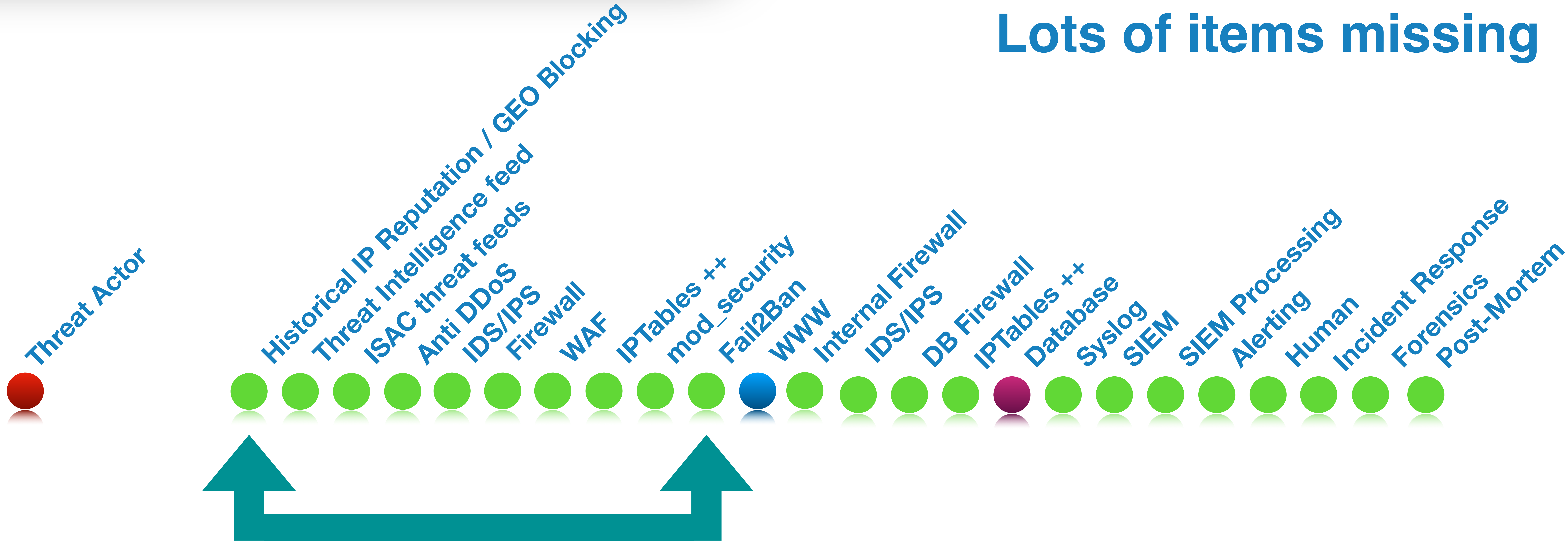
Post-Mortem

Flow of an external attack through a set of controls

**Note: there are many different attack flows,
this is just one example.**

External Attack Flow

Conversational Diagram
Lots of items missing

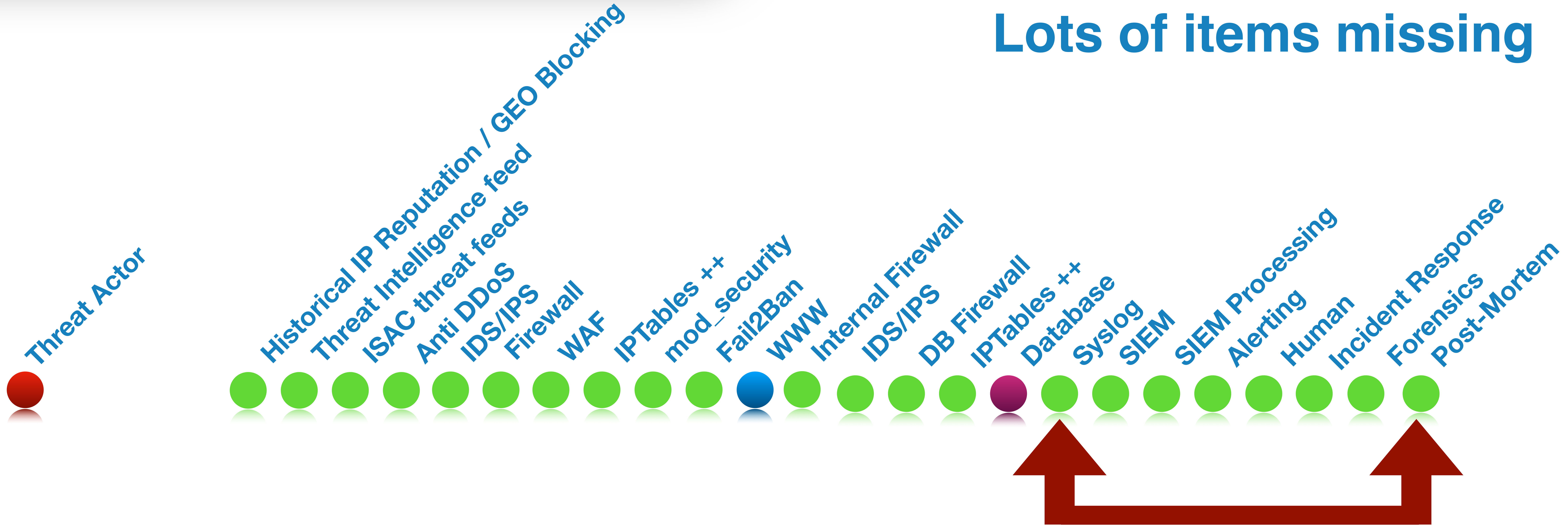


Security spending should be mostly preventative.

We want to prevent things right ???

External Attack Flow

Conversational Diagram
Lots of items missing

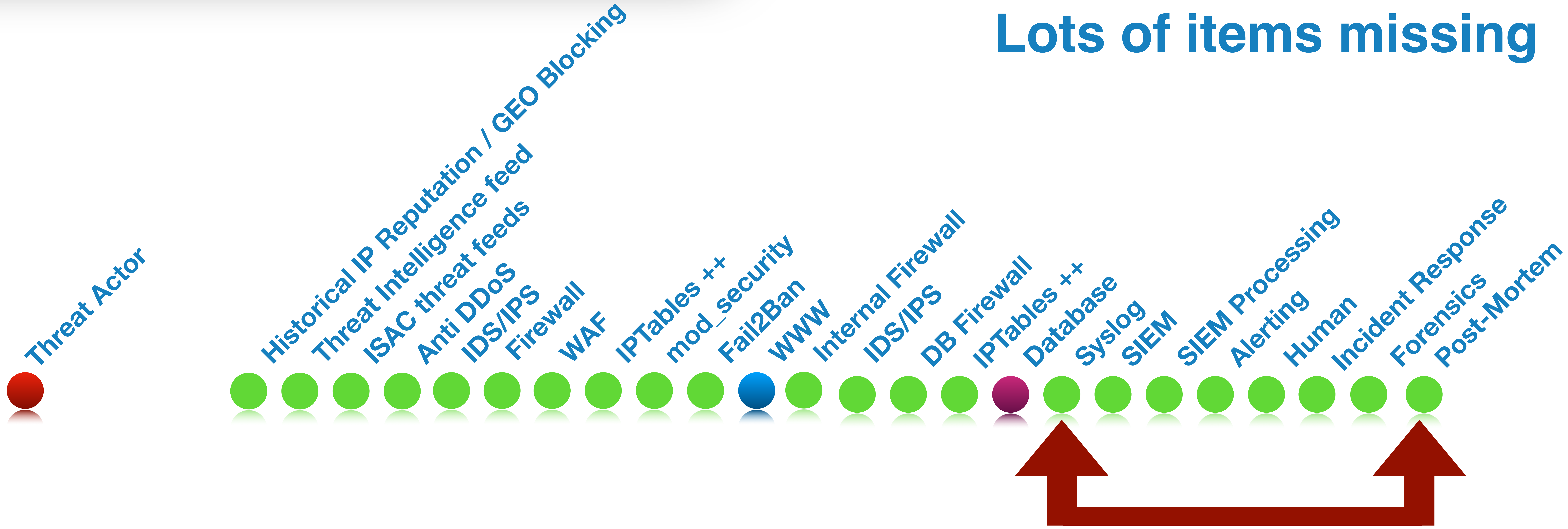


Traditional security spending is almost 80% reactive

A huge portion of this is log-storage and SIEMs

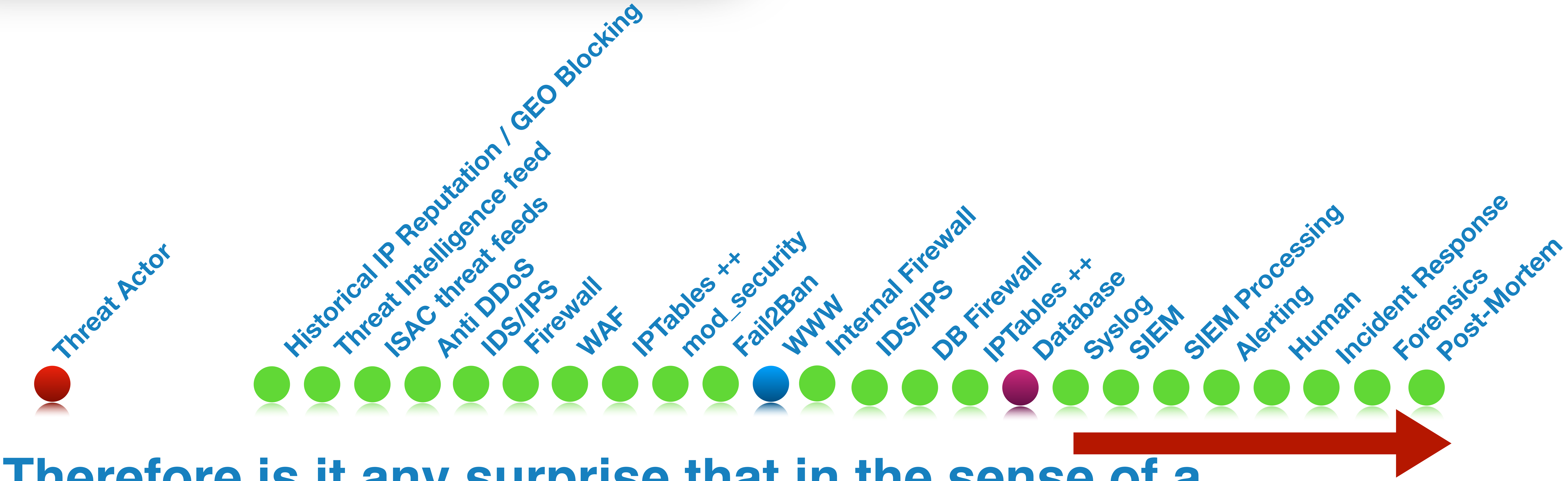
External Attack Flow

Conversational Diagram
Lots of items missing



Most of the human focus is also reactive.

External Attack Flow



Threat Actor

Historical IP Reputation / GEO Blocking

Threat Intelligence feed

ISAC threat feeds

Anti DDoS

IDS/IPS

Firewall

WAF

IPTables ++

mod_security

Fail2Ban

WWW

Internal Firewall

IDS/IPS

DB Firewall

IPTables ++

Database

Syslog

SIEM

SIEM Processing

Alerting

Human

Incident Response

Forensics

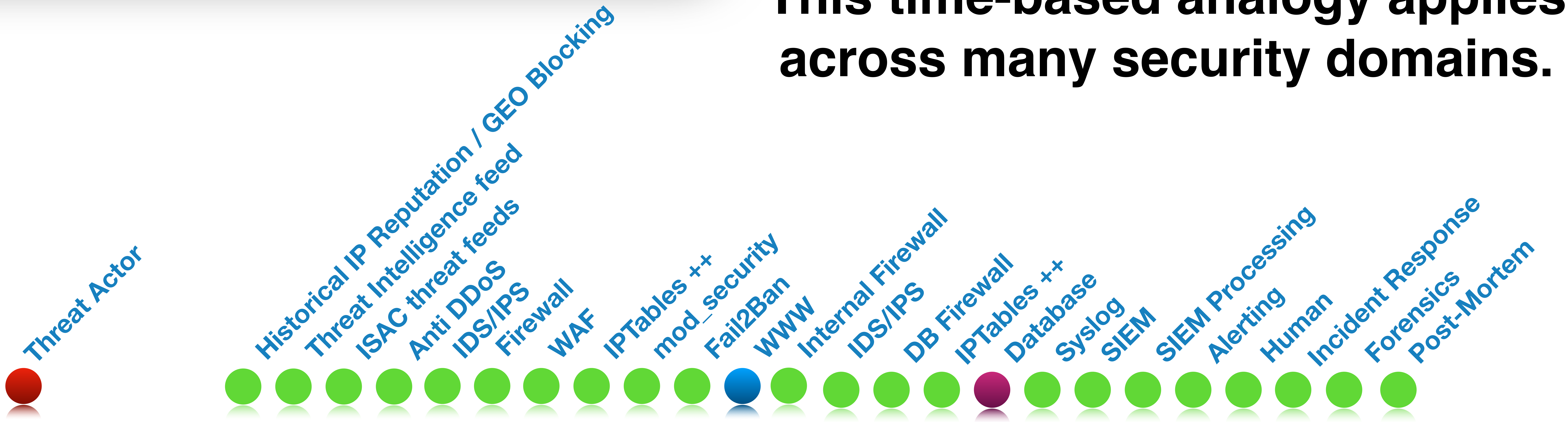
Post-Mortem

Therefore is it any surprise that in the sense of a time-line that this is when we find things?

It is after all where we've been focused and we aren't as fast as the machines.

External Attack Flow

This time-based analogy applies across many security domains.



Threat Actor

Historical IP Reputation / GEO Blocking

Threat Intelligence feed

ISAC threat feeds

Anti DDoS

IDS/IPS

Firewall

WAF

IPTables ++

mod_security

Fail2Ban

WWW

Internal Firewall

IDS/IPS

DB Firewall

IPTables ++

Database

Syslog

SIEM

SIEM Processing

Alerting

Human

Incident Response

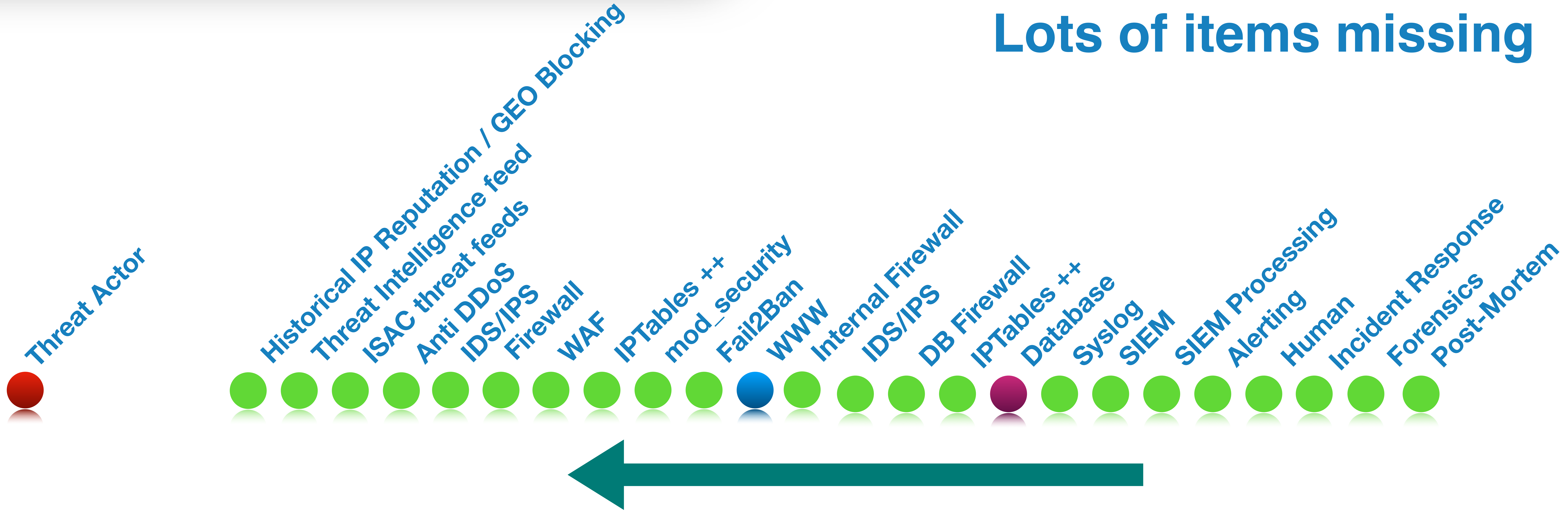
Forensics

Post-Mortem

Testing before deployment. vs. Testing after deployment.
Security Architecture (planning) vs. Security as an afterthought.

External Attack Flow

Conversational Diagram
Lots of items missing

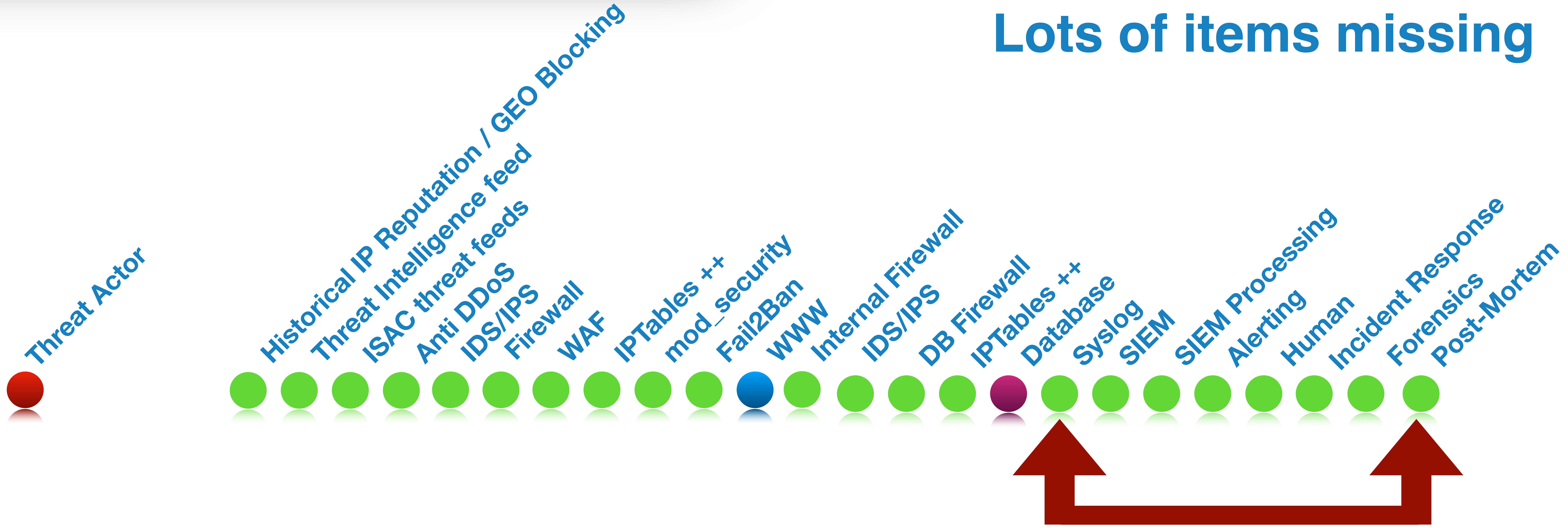


Threat Actor
Historical IP Reputation / GEO Blocking
Threat Intelligence feed
ISAC threat feeds
Anti DDoS
IDS/IPS
Firewall
WAF
IPTables ++
mod_security
Fail2Ban
WWW
Internal Firewall
IDS/IPS
DB Firewall
IPTables ++
Database
Syslog
SIEM
SIEM Processing
Alerting
Human
Incident Response
Forensics
Post-Mortem

We need to push more of the security processing towards the attackers.

External Attack Flow

Conversational Diagram
Lots of items missing



Most of the human focus is also **reactive.**

More importantly we need to block and respond at much faster rates than we have been.

More importantly we need to block and respond at much faster rates than we have been.

Humans are too slow

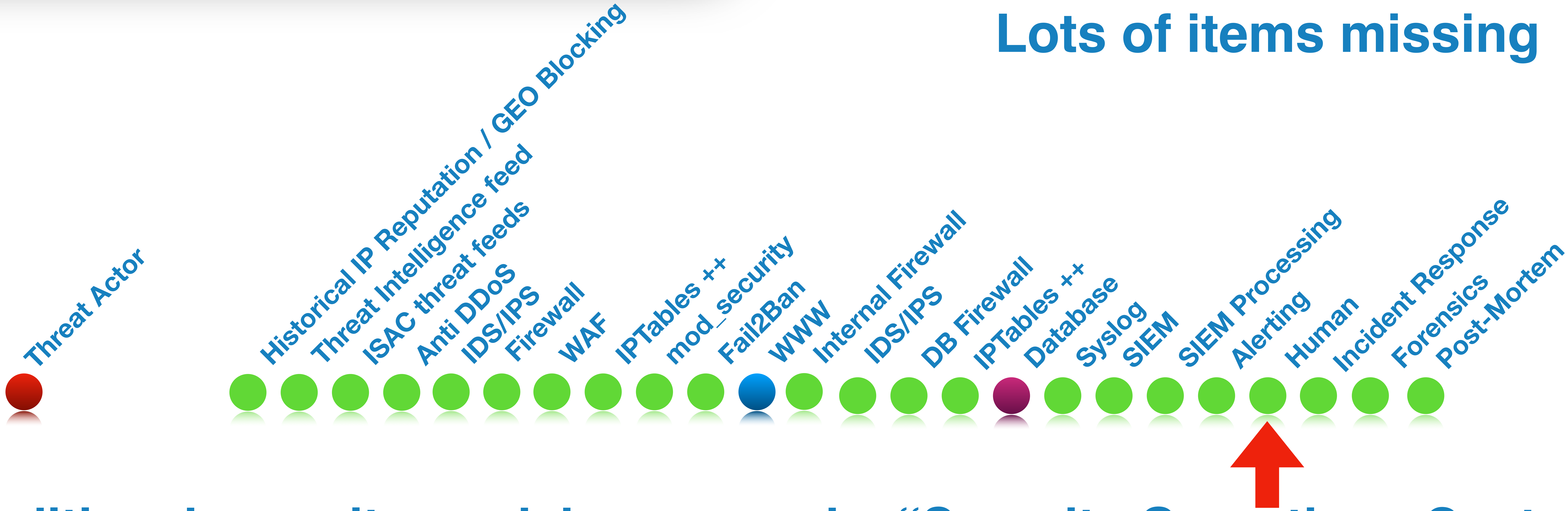
More importantly we need to block and respond at much faster rates than we have been.

Humans are too slow

And our defensive processes should not be based around them.

External Attack Flow

Conversational Diagram
Lots of items missing

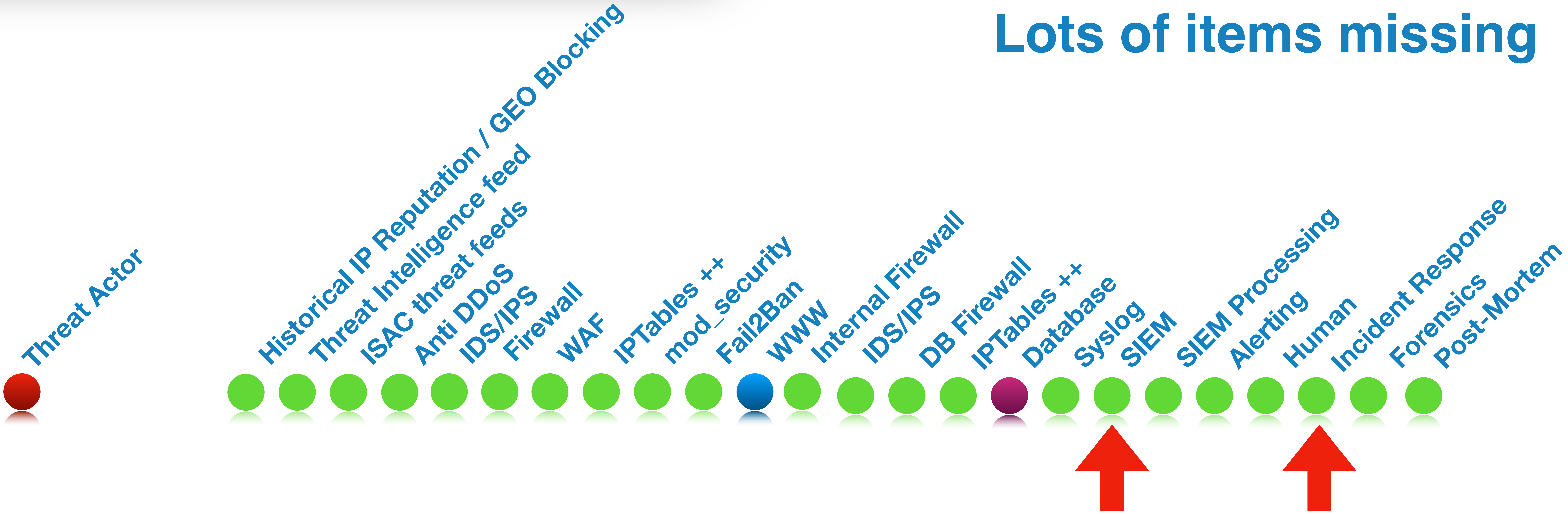


- Threat Actor
- Historical IP Reputation / GEO Blocking
- Threat Intelligence feed
- ISAC threat feeds
- Anti DDoS
- IDS/IPS
- Firewall
- WAF
- IPTables ++
- mod_security
- Fail2Ban
- WWW
- Internal Firewall
- IDS/IPS
- DB Firewall
- IPTables ++
- Database
- Syslog
- SIEM
- SIEM Processing
- Alerting
- Human
- Incident Response
- Forensics
- Post-Mortem

Traditional security models assumed a “Security Operations Center”
Where humans would make decisions about how to respond.

External Attack Flow

Conversational Diagram
Lots of items missing



Threat Actor

Historical IP Reputation / GEO Blocking

Threat Intelligence feed

ISAC threat feeds

Anti DDoS

IDS/IPS

Firewall

WAF

IPTables ++

mod_security

Fail2Ban

WWW

Internal Firewall

IDS/IPS

DB Firewall

IPTables ++

Database

Syslog

SIEM

SIEM Processing

Alerting

Human

Incident Response

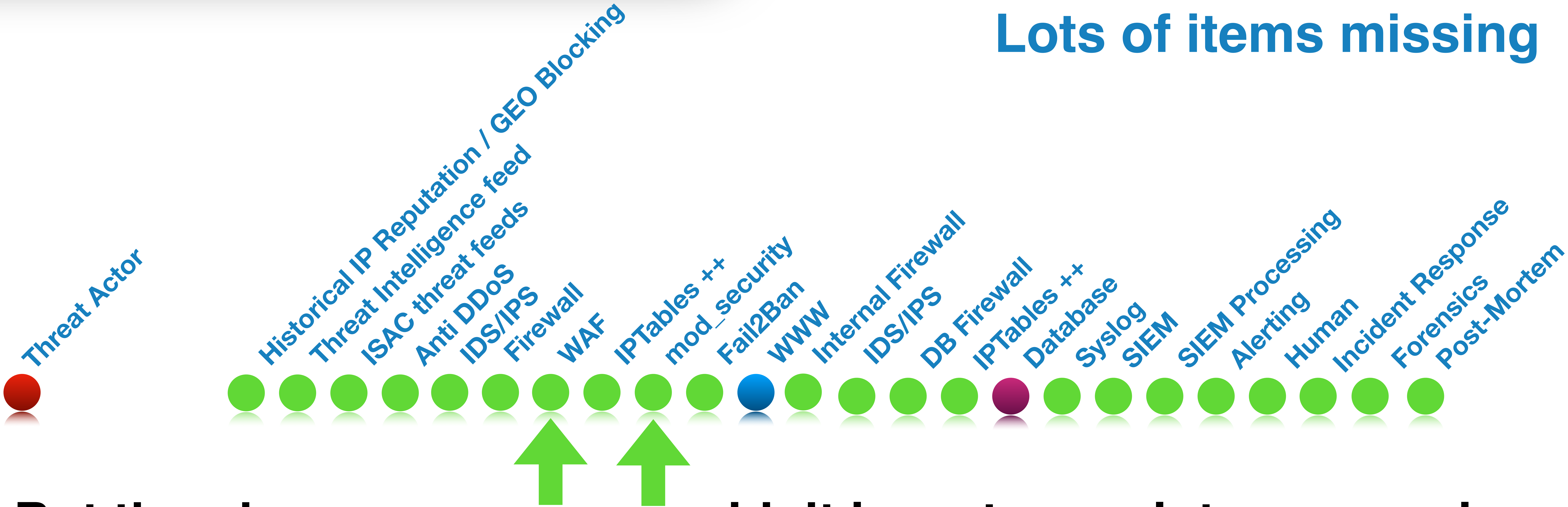
Forensics

Post-Mortem

So we make a lot of decisions “after the fact”

External Attack Flow

Conversational Diagram
Lots of items missing

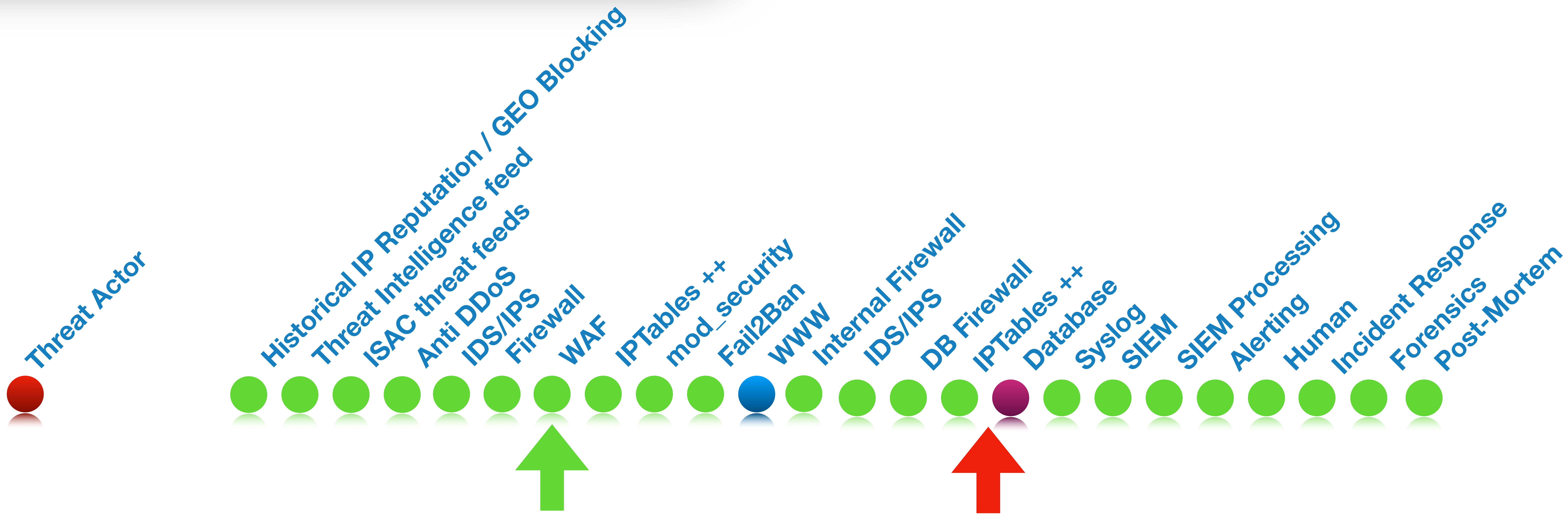


But there’s no reason we couldn’t invest more into processing Security decisions automatically in this general area.

Notably, before attackers can access our systems.

To do this we will need to automate more of our prevention-based defenses.

External Attack Flow



Costs less to block here

Expensive after this

Discussion Points:
Why this is important.
How to be effective.

Thank You

VERIFICATION
LABS

Slides and More Information

HTTP://WWW.VERIFICATIONLABS.COM/NSTT-OCT-2018.HTML

TREY@VERIFICATIONLABS.COM