Automated Defense

(aka Dynamic Firewall)

FACT

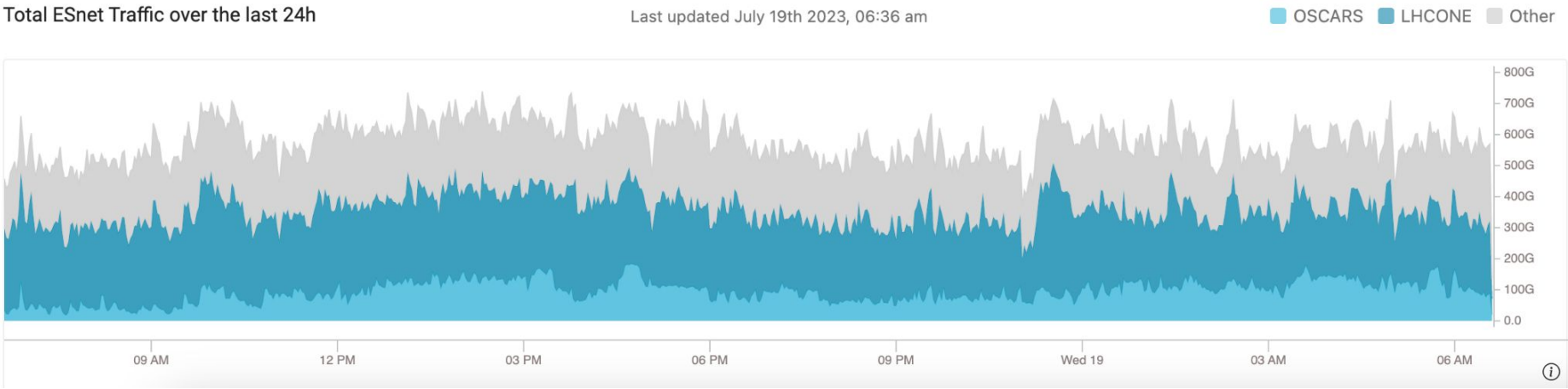
U.S. DEPARTMENT OF
ENERGY

UNIVERSITY OF
CALIFORNIA


ESnet6
ESnet User Facility, 2022
Seattle
PNNL
NETL
Boise
INL
LBNL
Bay Area
SLAC
LLNL
SNL
San Jose
Salt Lake City
NREL
Denver
Las Vegas
Los Angeles
San Diego
Albuquerque
LANL
SNL
El Paso
Dallas
Houston
Kansas City
AMES
ANL
FNAL
Chicago Area
Nashville
ORNL
Chattanooga
Atlanta
SRNL
NETL
NETL
Washington, D.C.
BNL
Boston
New York
PPPL
JLAB
London
Amsterdam
Geneva/ CERN
Hubs
Increasing bandwidth
SITES
Office of Science National Laboratories
AMES Ames Laboratory (Ames, IA)
ANL Argonne National Laboratory (Argonne, IL)
BNL Brookhaven National Laboratory (Upton, NY)
FNAL Fermi National Accelerator Laboratory (Batavia, IL)
JLAB Thomas Jefferson National Accelerator Facility (Newport News, VA)
LBNL Lawrence Berkeley National Laboratory (Berkeley, CA)
ORNL Oak Ridge National Laboratory (Oak Ridge, TN)
PNNL Pacific Northwest National Laboratory (Richland, WA)
PPPL Princeton Plasma Physics Laboratory (Princeton, NJ)
SLAC SLAC National Accelerator Laboratory (Menlo Park, CA)
NNSA Laboratories
LANL Los Alamos National Laboratory (Los Alamos, NM)
LLNL Lawrence Livermore National Laboratory (Livermore, CA)
SNL Sandia National Laboratory (Albuquerque, NM; Livermore, CA)
Other DOE Laboratories
INL Idaho National Laboratory (Idaho Falls, ID)
NETL National Energy Technology Laboratory (Morgantown, WV; Pittsburgh, PA; Albany, OR)
NREL National Renewable Energy Laboratory (Golden, CO)
SRNL Savannah River National Laboratory (Aiken, SC)
ESnet
U.S. DEPARTMENT OF ENERGY
Office of Science

et

How much Data/traffic?



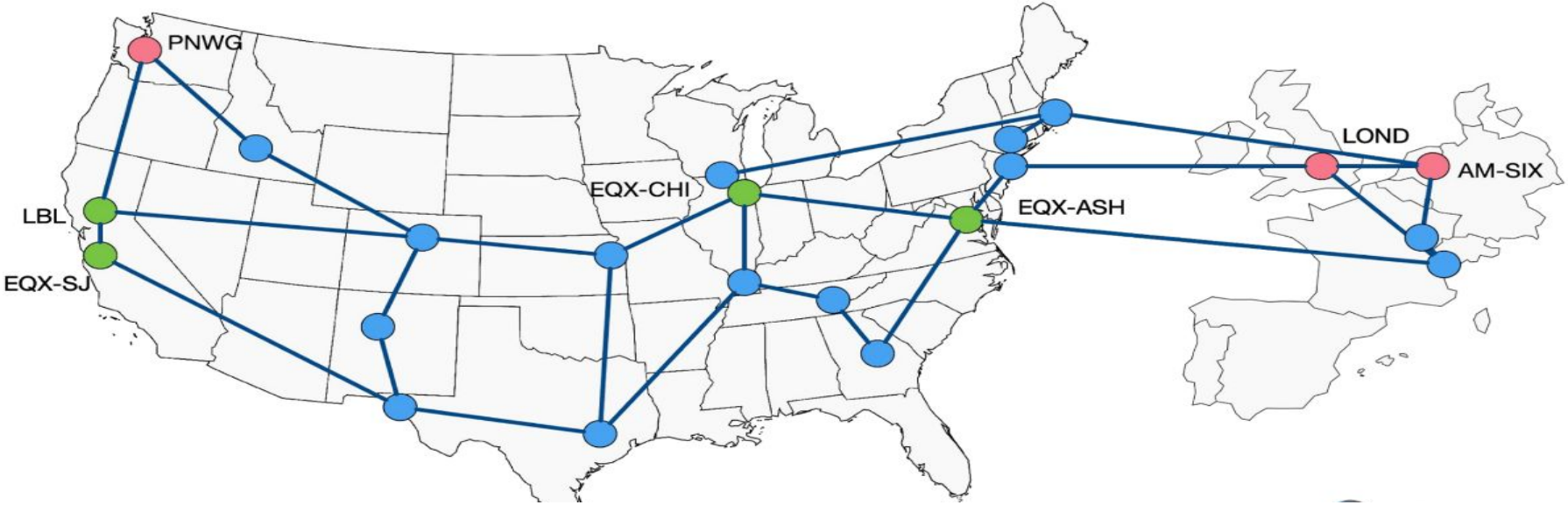
ESnet

What does Securing the network mean?

- Visibility of our important choke points - You can't defend what you can't see!
  - Taps/Port Mirrors
- Traffic monitoring of those choke points
  - NSMs/IDS/IPS
- Log collection and aggregation
  - SIEM
- Alerting and reporting
  - SIEM/CI-CD

ESnet

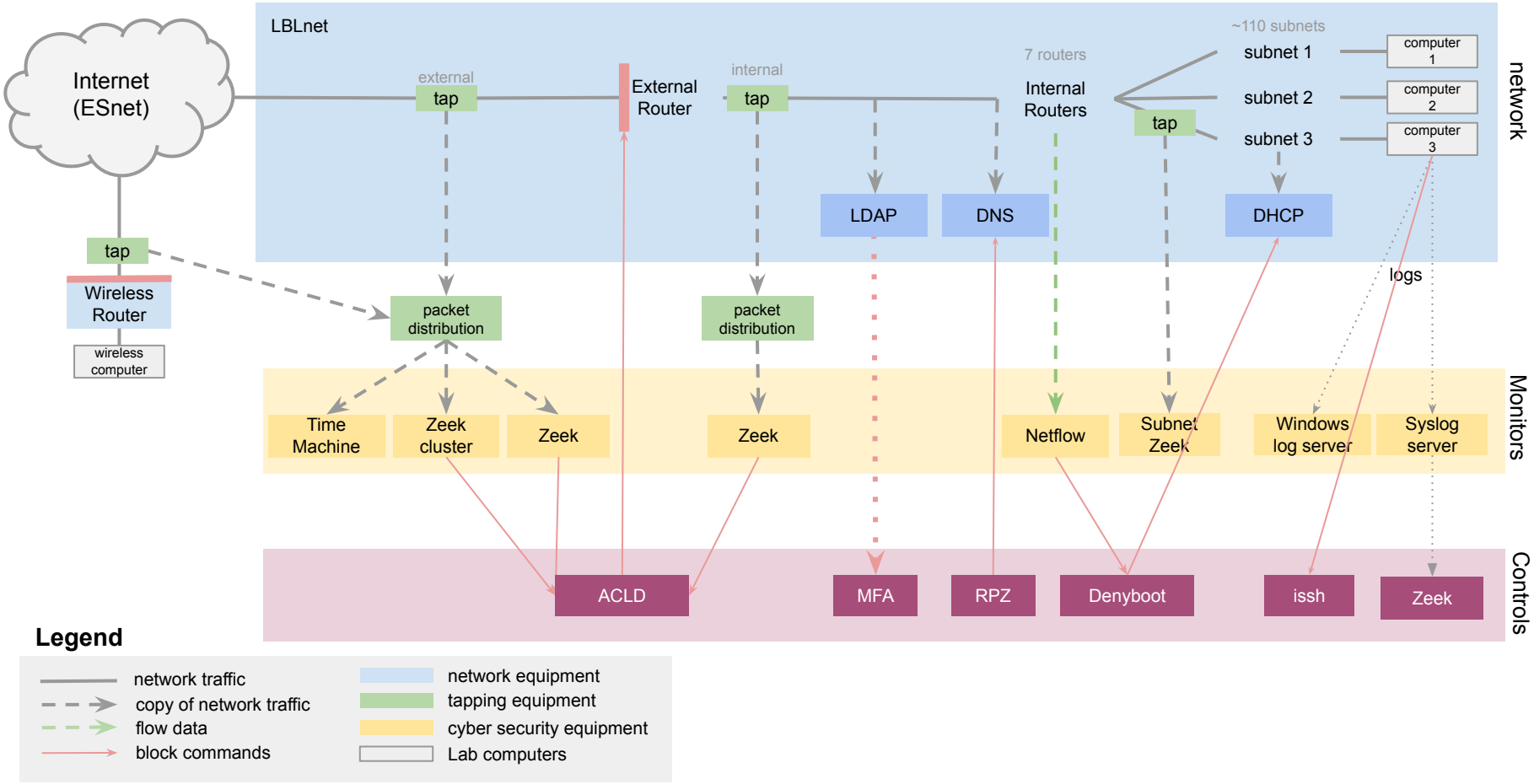
Tackling Visibility of network - WAN
Zeek on WAN (ZoW)



- WAN links b/w 1 - 800Gbps
- High value locations - commodity internet peerings

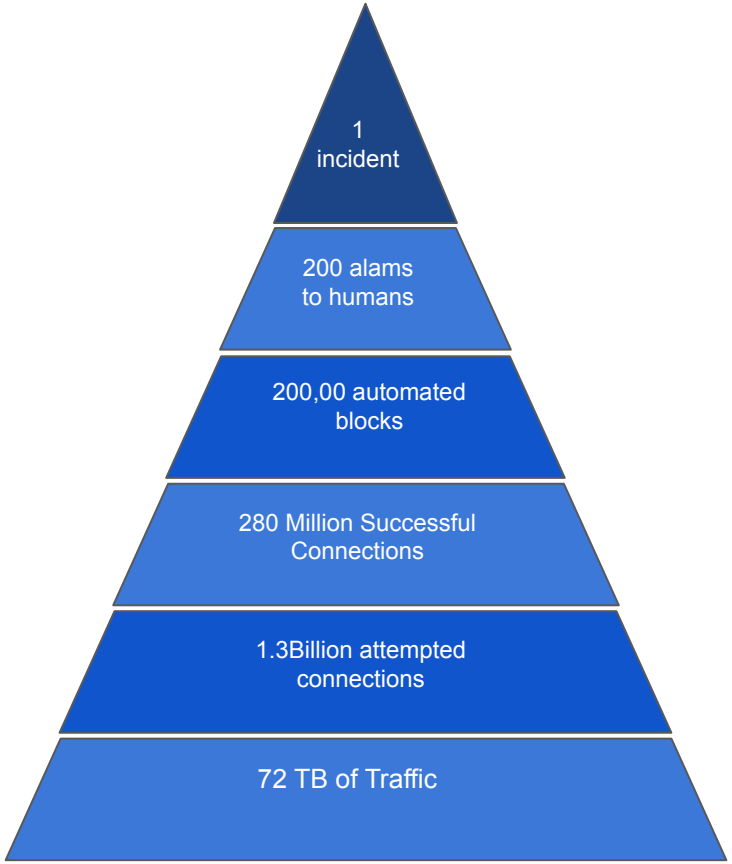
ESnet

LBNL Cyber Security: Border Access Visibility and Controls



Network and Monitoring Environment

Devices:	20,000+ (one of everything) A lot of "Cloud" usage
Users:	6000+
Network:	IPv4: 2 x Class B's IPv6: 3 x /64
Links:	100G and multiple 10G
Core Tools:	Zeek IDS (80G daily logs) Network Flow (35G) Central Syslog (15G)
Endpoints:	Most endpoints are unmanaged BYOD is standard

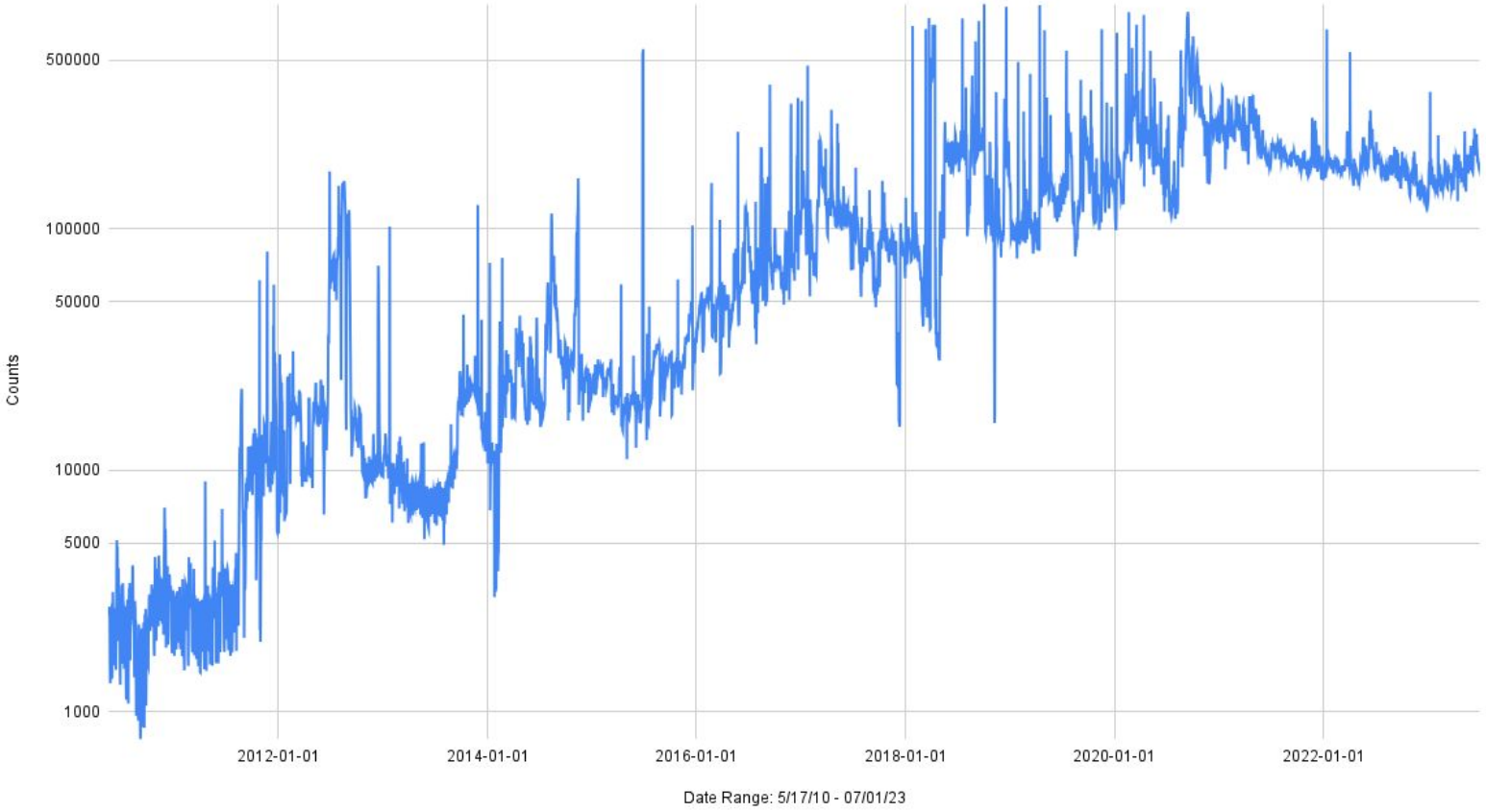


```
114393 Scan::KnockKnockScan
61132 Scan::LandMine
23930 Notice::DropThrottle
15758 Scan::AddressScan
15033 Scan::HotSubnet
8960 WL::PurgeOnWhitelist
6453 Scan::BlocknetsIP
6077 SIP::BadUserAgent
4488 Scan::ShutdownThresh
2307 UDP::AddressScan
 895 ICMP::ICMPAddressScan
 832 PacketFilter::Dropped_Packets
 827 LBL::EduIP
 820 ICMP::ScanSummary
 363 Scan::LowPortTrolling
 337 ICMP::NDP_Unauthorized_Router
 337 ICMP::NDP_NA
 280 WL::WhitelistAdd
 280 Scan::WhitelistAdd
 230 WL::WhitelistChanged
 230 Scan::WhitelistChanged
 100 SSL::Invalid_Server_Cert
  54 Notice::DropIgnore
  52 LBL::AuthIP
  36 CaptureLoss::Too_Much_Loss
  15 Scan::ScanSpike
   6
   4 Scan::WebCrawler
   2 RDP::HotAccount
   2 HTTP::SensitivePOST
   1 Scan::LowPortScanSummary
   1 SIP::Code_401_403
```

```
61146 SSL::Invalid_Server_Cert
25027 SMTPurl::SMTP_Click_Here_Seen
14280 Scan::WhitelistAdd
14000 Scan::PurgeOnWhitelist
10558 SMTPurl::SMTP_URI_Click
9402 Notice::DropThrottle
6904 UDP::AddressScan
6201 SIP::BadUserAgent
4799 Whitelists::RemoteUser
3752 HTTP::HTTPSensitivePOST
3274 Notice::DropIgnore
2259 FTP::BruteforceSummary
1764 SMTPurl::SMTP_Dotted_URL
 472 NTP::NTP_Monlist_Queries
 438 RDP::ScanSummary
 285 RDP1::BruteforceScan
 230 Scan::WhitelistChanged
 208 Software::Vulnerable_Version
 168 RDP::HotAccount
  56 HTTP::HTTP_SensitiveURI
  39 SMTPurl::SMTP_WatchedFileType
  19 Weird::Activity
  13 CaptureLoss::Too_Much_Loss
  12 RDP::PasswordGuessing
   9 HTTP::Sensitive_UserAgent
   6
   4 Notice::RemoteUserScan
   4 FTP::Bruteforcer
   3 HTTP::HTTP_Suspicous_Client_Header
   2 SMTPurl::SMTP_sensitiveURI
   1 SSH::Interesting_Hostname_Login
   1 SIP::Code_401_403
   1 HTTP::HTTP_CrossSiteScripting
   1 FTP::SensitiveURIs
```

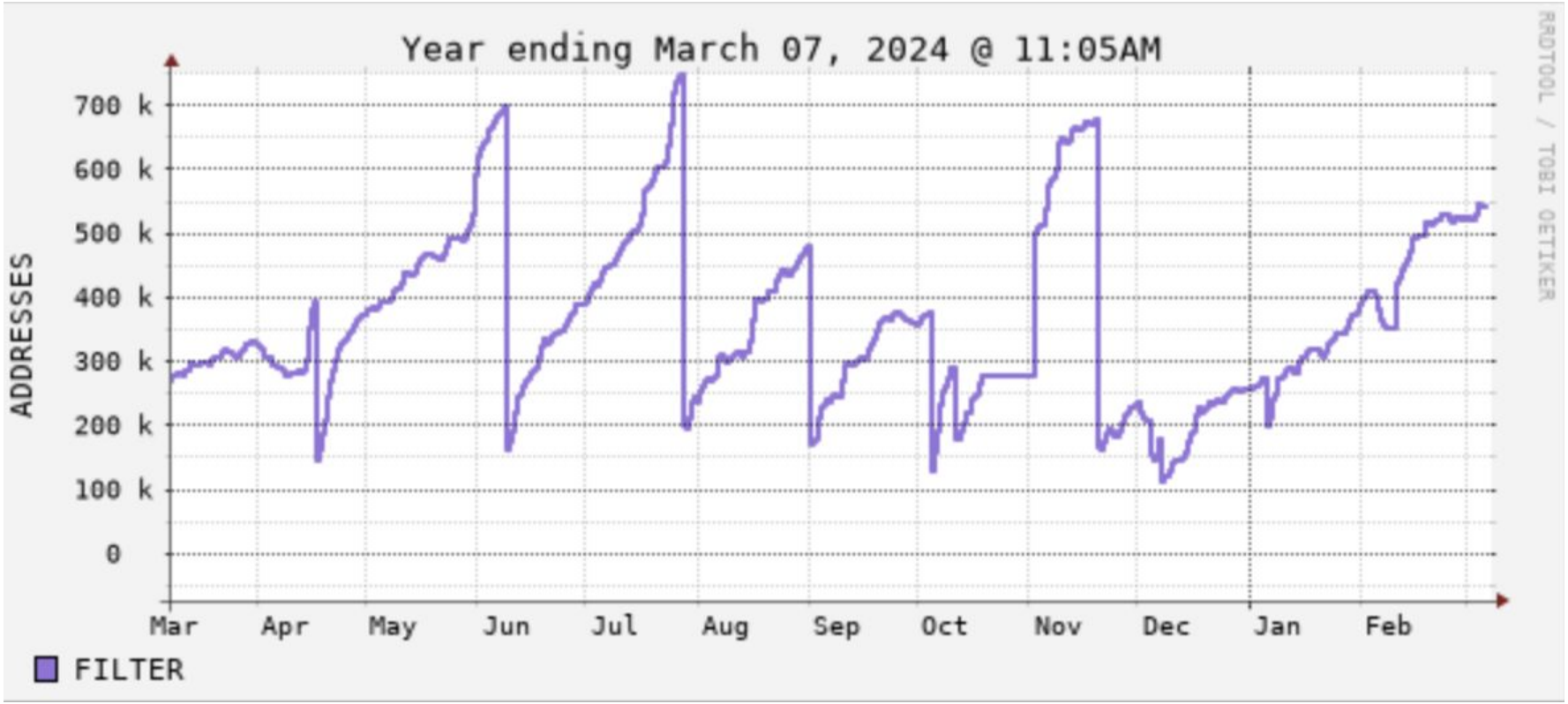
```
63537 SSL::Invalid_Server_Cert
14000 WL::PurgeOnWhitelist
5733 SIP::BadUserAgent
4214 Notice::DropThrottle
4028 HTTP::SensitivePOST
2285 FTP::BruteforceSummary
1002 smtpsink::NotGoogleSPF
 353 RDP::ScanSummary
 306 SSH::Interesting_Hostname_Login
 280 WL::WhitelistAdd
 247 SMTPurl::WatchedFileType
 230 WL::WhitelistChanged
 168 RDP::HotAccount
  83 LBLIntel::LabPhish
  62 SMTPurl::MsgBody
  55 SMTPurl::DottedURL
  48 SSH::Watched_Country_Login
  45 HTTP::HTTP_SensitiveURI
  42 Notice::DropIgnore
  30 PacketFilter::Dropped_Packets
  25 ESnet::REN
  22 smtpsink::Subnet
  17 Weird::Activity
  15 RDP::PasswordGuessing
   8 SSH::Password_Guessing
   8 CVE_2020_1350::Potential
   6 FTP::Bruteforcer
   6
   5 LetsEncrypt::Whitelisted
   4 LBLIntel::ReplyToPhish
   4 CaptureLoss::Too_Much_Loss
   3 HTTP::HTTP_WatchedURI
   2 SMTPurl::SensitiveURI
   1 proto
   1 enum
   1 SIP::Code_401_403
   1 LetsEncrypt::OCSPPost
   1 HTTP::HTTP_CrossSiteScripting
```

Number of IPs Transactions each day

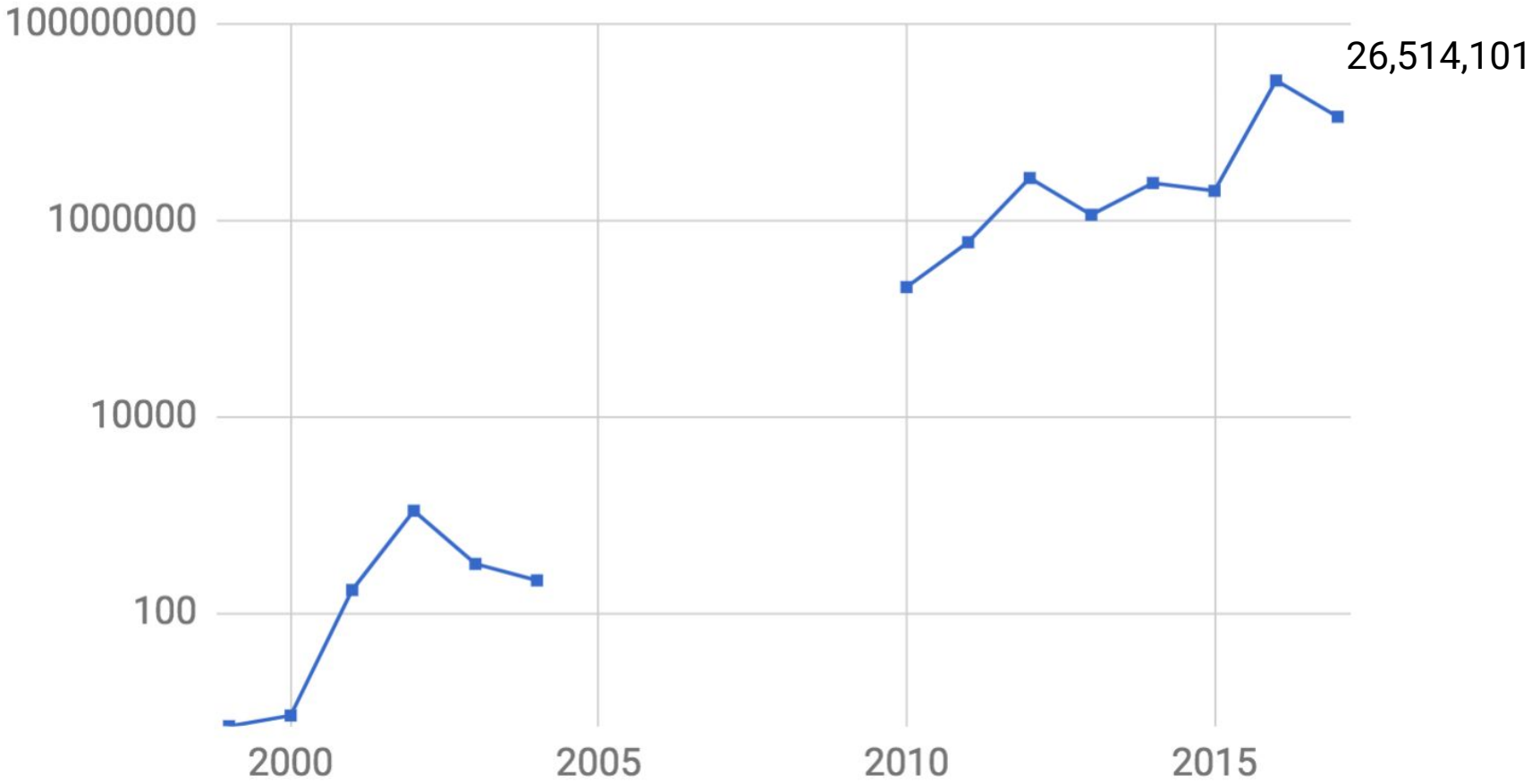


Identifying and blocking “attacks”

blocks



Background Radiation - Unique IP's blocked each year



Strategies*

Strategy	Description	Effects
Catch-n-release	A home grown system of prioritizing block removals	10,000,000 (600-700K at any given time)
Subnet level blocks	Block entire subnets if meet certain criteria of badness	5,000
TCP Syn Flag blocks	Port specific blocks based on TCP flags	500,000 - 1,000,000
Corsa Filters	Ability to block entire IPv4 Space	4.2 Billion IPs

Year Added	Era	Controls	Definition	Volume (as of 2023)	Primarily Subject to	driver/in response to
2022	clouds	Logs and shields	Ability to block entire IPv4 space	300-600K / day	Remote IPs	Huge reconnaissance Activity
2019	Monetization	Filters	Ability to block entire IPv4 space	300-600K / day	Remote IPs	Huge reconnaissance Activity
2017	IoT botnets	TCP syn port blocks	Block a port if syn originating from ext-dmz	300-600K / day	Remote IPs	Huge botnet activity
2017	SSH/Phishing	MFA/OTP	Two factor auth	~8-10K/day	Authentication	Compromised credentials
2016	Phishing	GAM removal	Delete emails on google server	~1 / 3-6 months	EMAIL	Phishing
2011	Drive-by-downloads	RPZ	Response Policy Zone	10-100's / day	All LBNL hosts	Drive by downloads and phishing
2008	SSH credential theft	iSSHD	Instrumented SSH	~1 / month	HPC and Supercomputers	Compromised ssh credentials
2006	Worms/botnets	BGP Nullroutes	Block rule for dropping Packets that match	~ 200K / day	Remote IPs	Remote Scanners Malicious activity Blacklisted IPs Repeated offenders
2004	Worms/botnets	Denyboot	Stop giving out DHCP leases	3-10/day	Internal MAC	Malware Infections, Copyright
2004	Inflationary Period	DHCP Jail (isolation)	Redirections to a notification server	10+/day	Internal MAC	People not fixing vulnerabilities Nimda/code red
1994	Early Incidents	ACLD Drop	ACL at the border	Rare (may be 1/month)	Internet	Internet attacks

- What’s your block budget
- What’s your impact
- What’s your block tolerance - Do you know aashish blocked Facebook ?
- What all controls you got :
  - ACL, Nullroutes, DHCP denyboot, Jailing, DNS RPZ, Shunting
- Do you notify of a block ?
  - Fault tolerances - incorrect blocking - entire process IDS -> Helpdesk -> user
- Fail-safe mechanisms - Can these me automated ?
  - AI to remove a block ?
  - Is this a spam or not ?
- Allow lists / blacklists
    - What if user is 2 continents away - DHCP
    - Hotel/conferences

The Reality of Cyber Security Operations

- No perfect protection
  - Miscreants are always one step ahead
  - **Acknowledging this improves protection!**
- Know your network
- Hire good sysadmins (or train the bad ones)
- Credential stealing is not just an SSH problem
  - Windows, Facebook, Gmail, banks, etc.
- Mutual Cooperation is super beneficial
- Measuring improvements is much much harder than improvement itself

Incidents Happen	Study and Learn	New Controls
There is no perfect protection, incidents are going to happen. Architect to reduce the scope and severity, detect quickly.	Data driven cyber security. What exactly happened, bit by bit. How were controls bypassed? How best to defend in the future?	Take the lessons learned from study and consider new controls. Where to attack the kill chain?