CIRT
BECHTEL IS&T

Zero to 100 in 90 Days

Building Up Your Security Operations

Overview

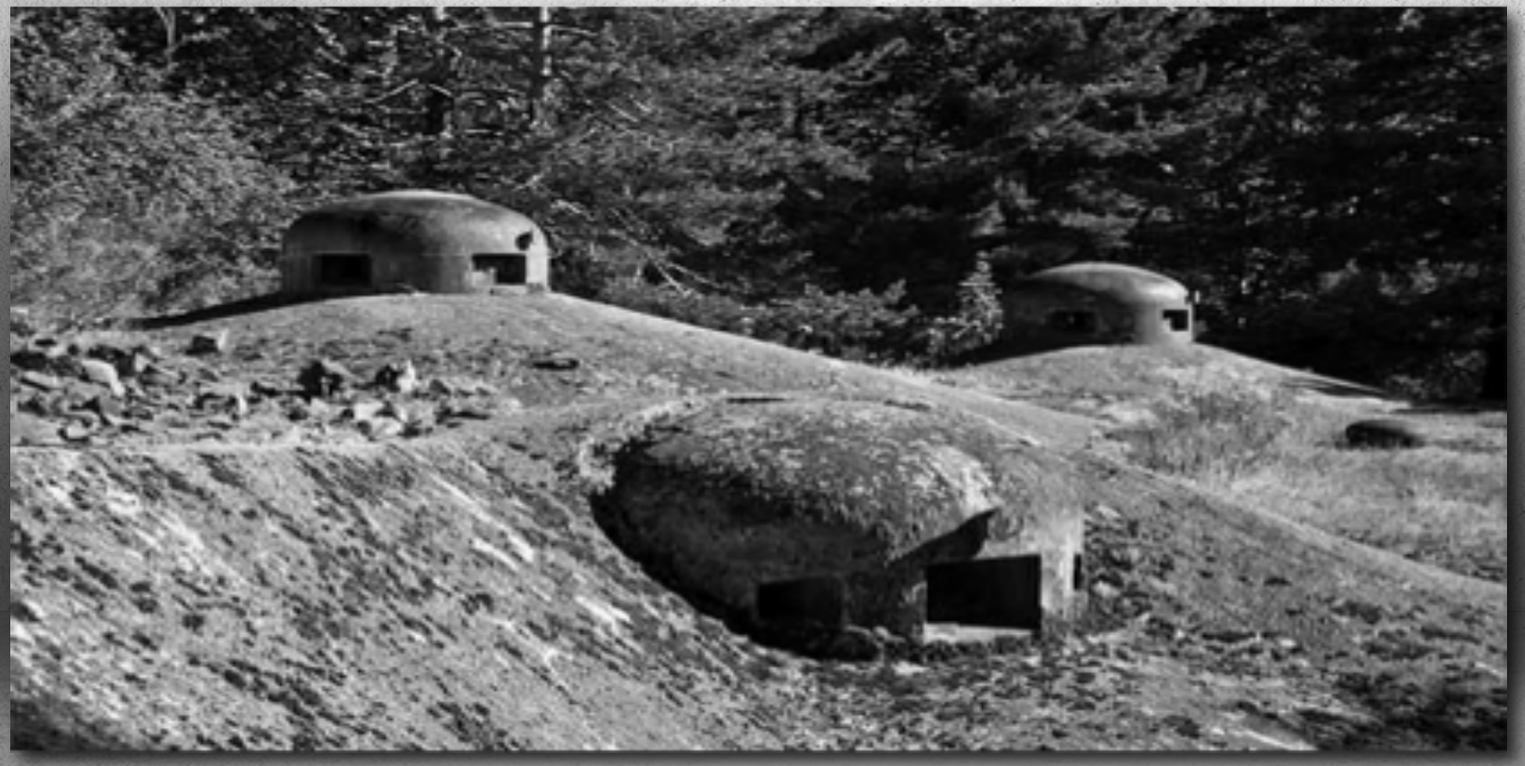
CIRT
BECHTEL IS&T

- About Bechtel
- Bechtel Incident Response
- Building the Team
- Building the Security Infrastructure
- Novel Integration Points
- Stumbling Blocks
- Use Case
- Q&A

About Bechtel

CIRT
BECHTEL IS&T

Old Security Model

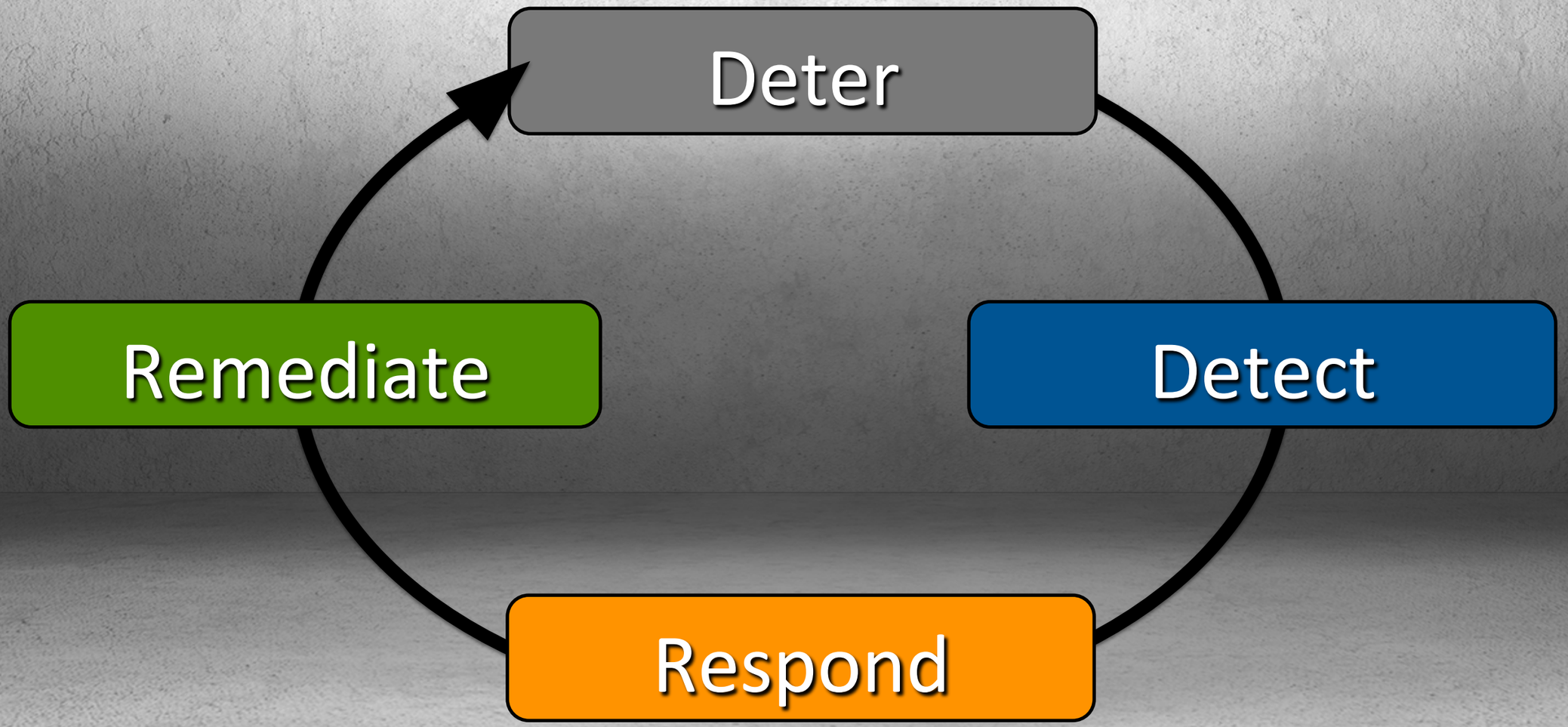


Yes, Something Happened.

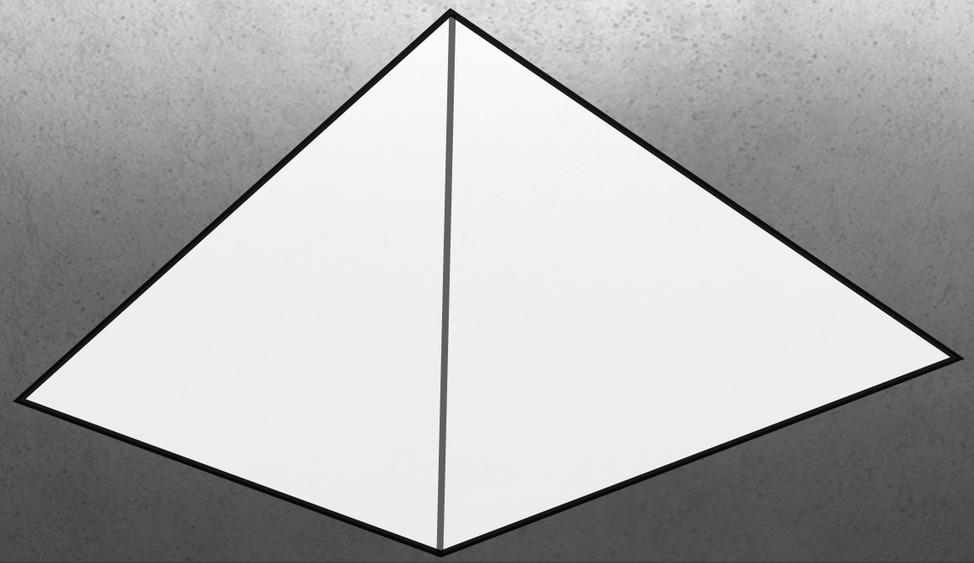
The Problem


貓
CHAIRMAN MEOW

New Security Model



People, Most Important



Tier Two
Tier One

SOC

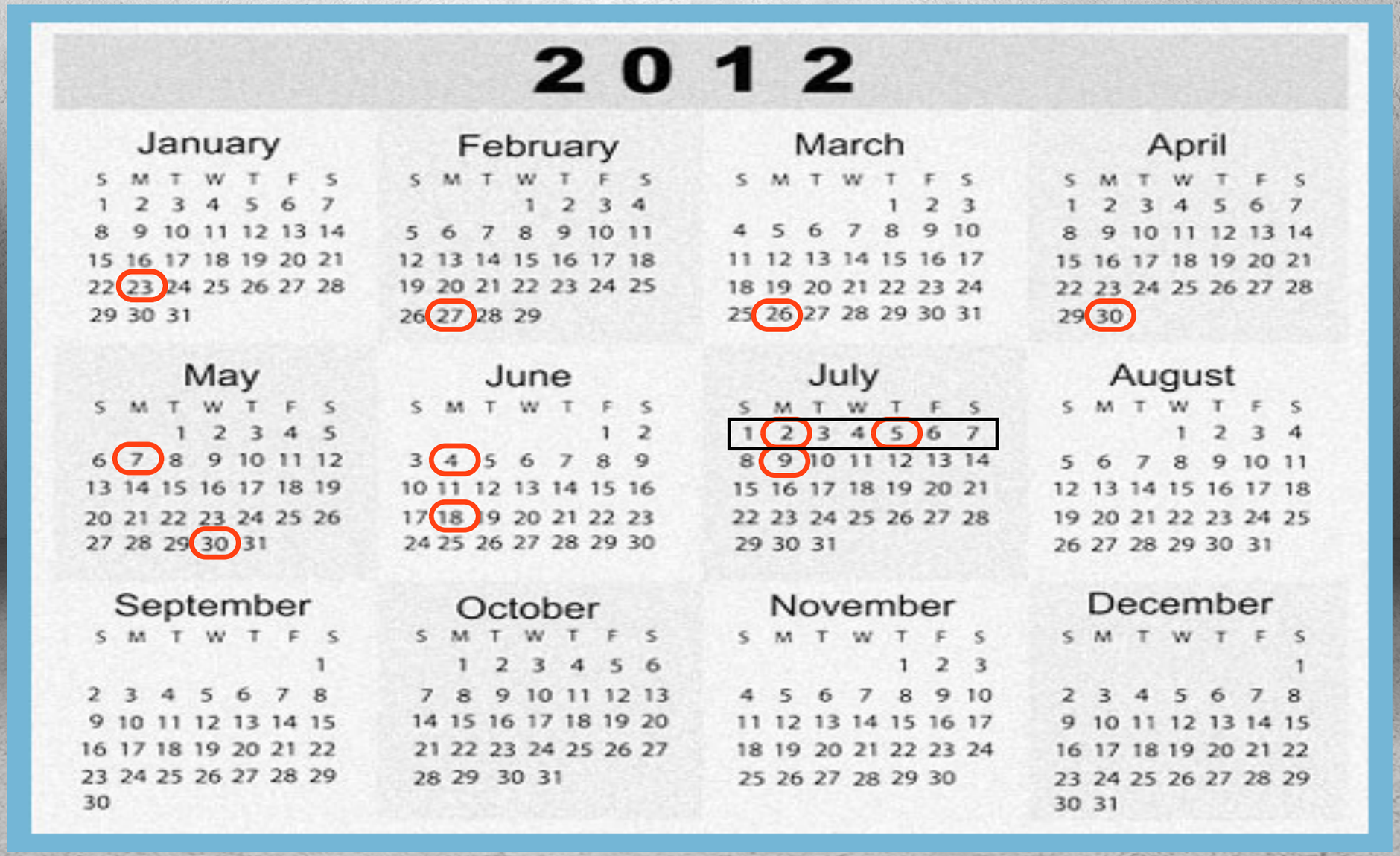
Where’s the CIRT?

CIRT
BECHTEL IS&T

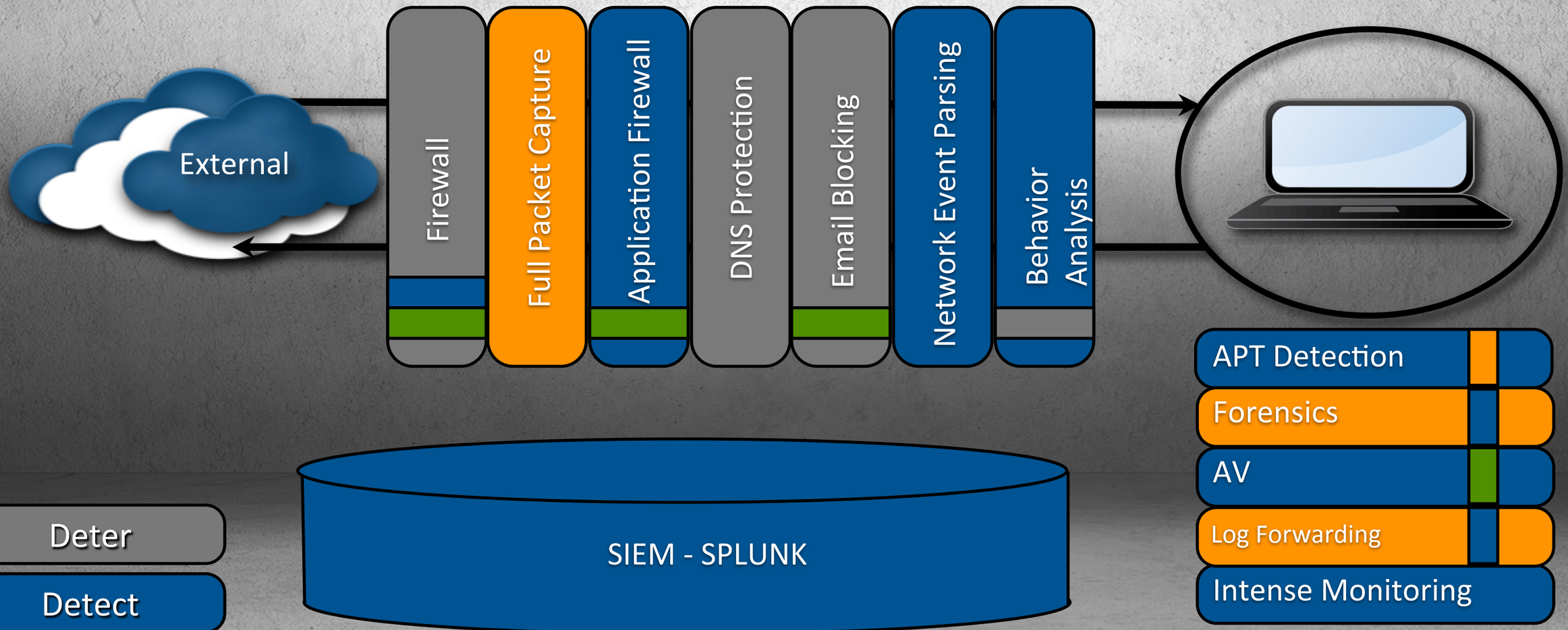
- Untapped talent pool
- Diverse skill sets
- More familiar with emerging tech
- Move where the talent is, where they want to work

The Impossible Task

- Kelcey
- Matt*
- Mark
- Randy
- Lisa
- Steve
- Graeme
- Alex
- Shane*
- Adil
- Chris
- Josh



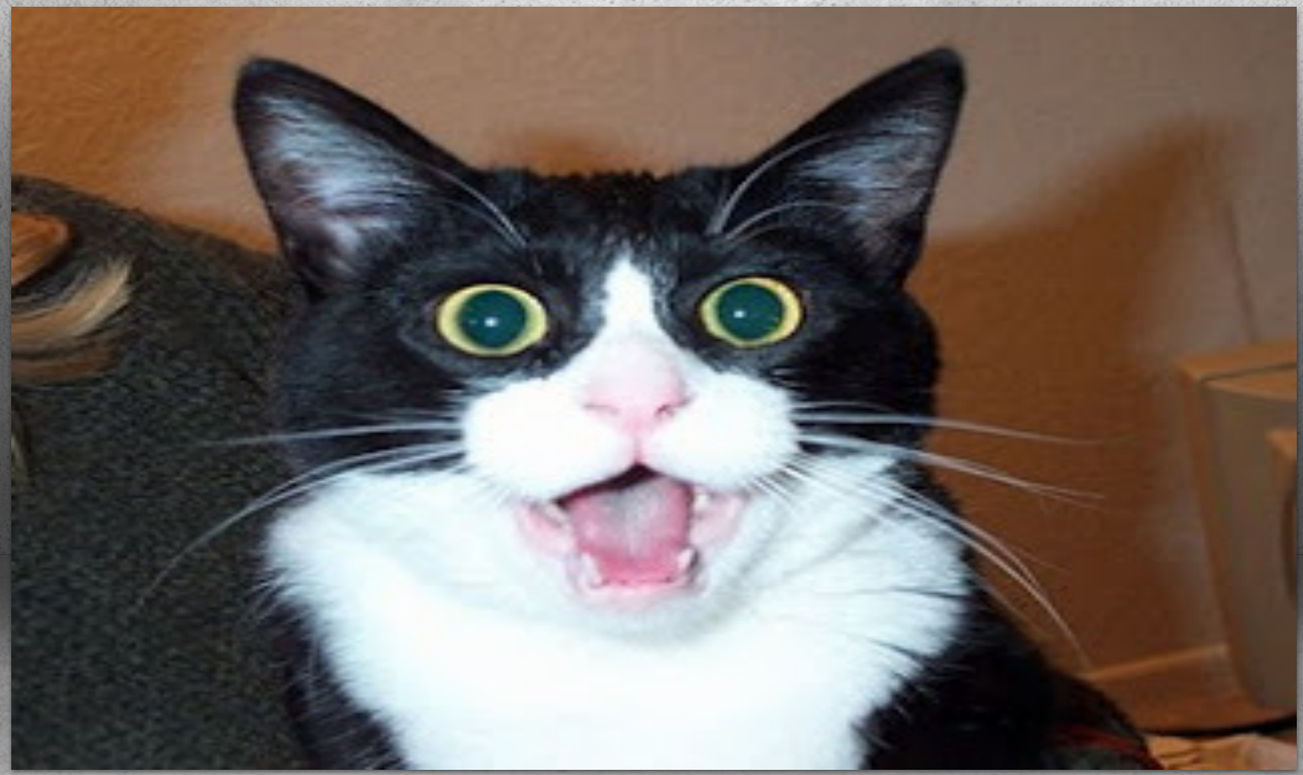
The Stack


External
Firewall
Full Packet Capture
Application Firewall
DNS Protection
Email Blocking
Network Event Parsing
Behavior Analysis
APT Detection
Forensics
AV
Log Forwarding
Intense Monitoring
SIEM - SPLUNK
Deter
Detect
Respond
Remediate

Seven Data Centers

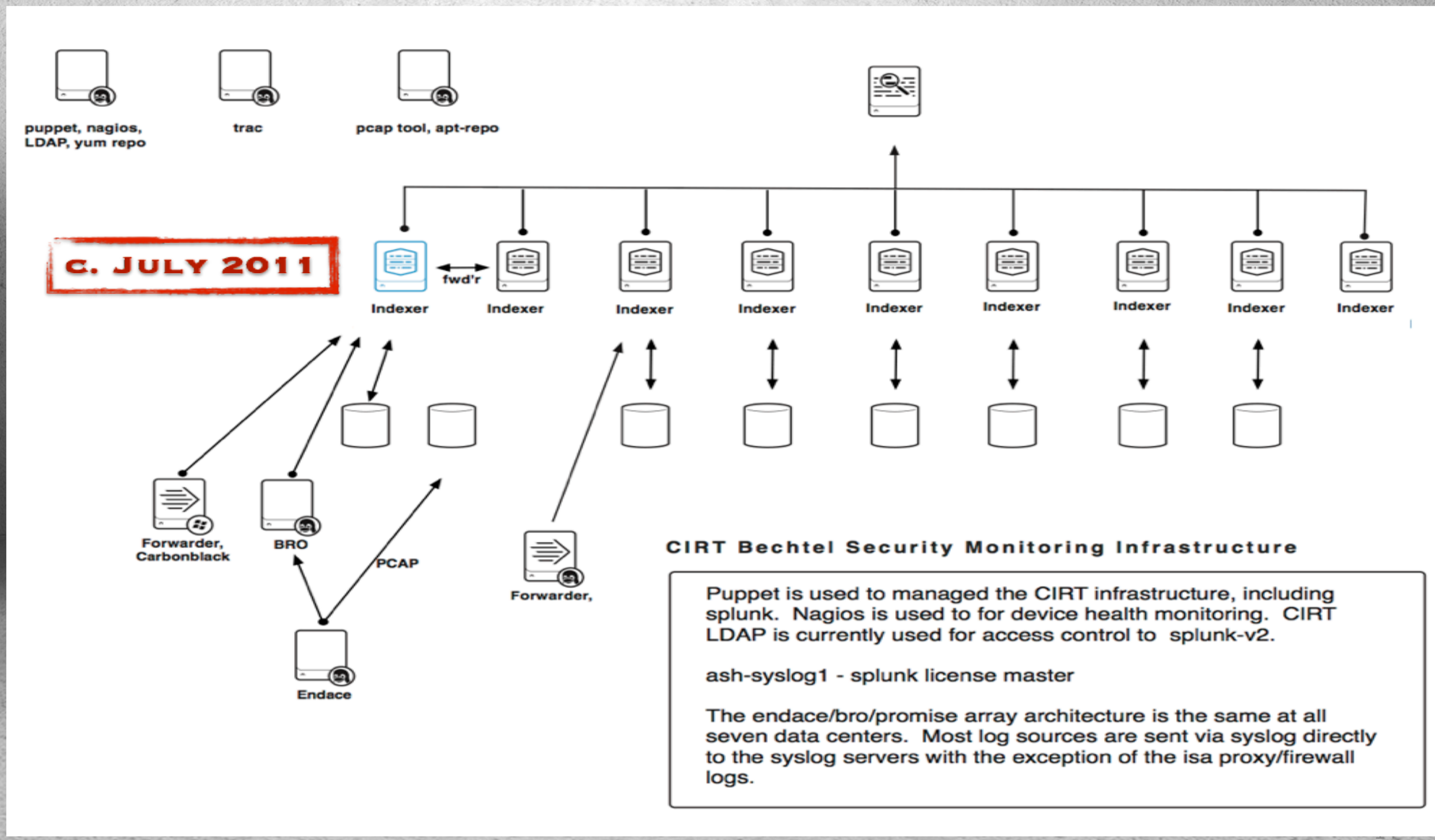
CIRT
BECHTEL IS&T

Hey, Lisa Install Splunk



What About Puppet?

CIRT
BECHTEL IS&T



puppet labs

Still growing but less painful

Where are We Now

Puppet

Puppet can be awesome.... most of the time

The Good

- Configuring NTP
- Managing the Syslog-NG Config
- Configuring Splunk
- Nagios Monitoring Configs
- Hiera /yaml is your friend

The Bad

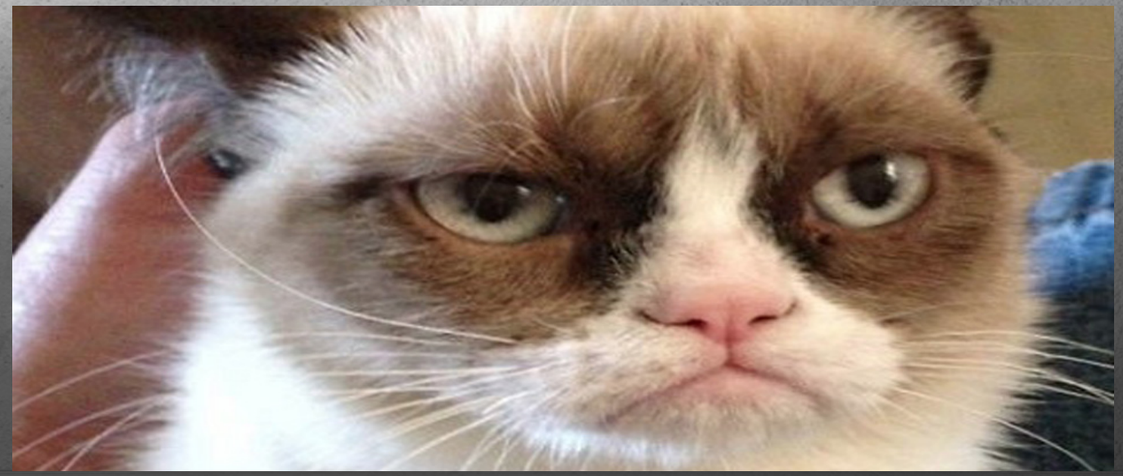
- Inconveniently restarting indexers and search heads at random times
- Obliterated sudoer's file
- Abstracting splunk configs and logic into puppet files adds complexity
- Not using hiera

Performance Woes

What wrong with my indexer.....

- Storage Arrays configured in RAID60
- Everything was configured with syslog
- Old Splunk, Legacy Splunk, Splunk v 1.0

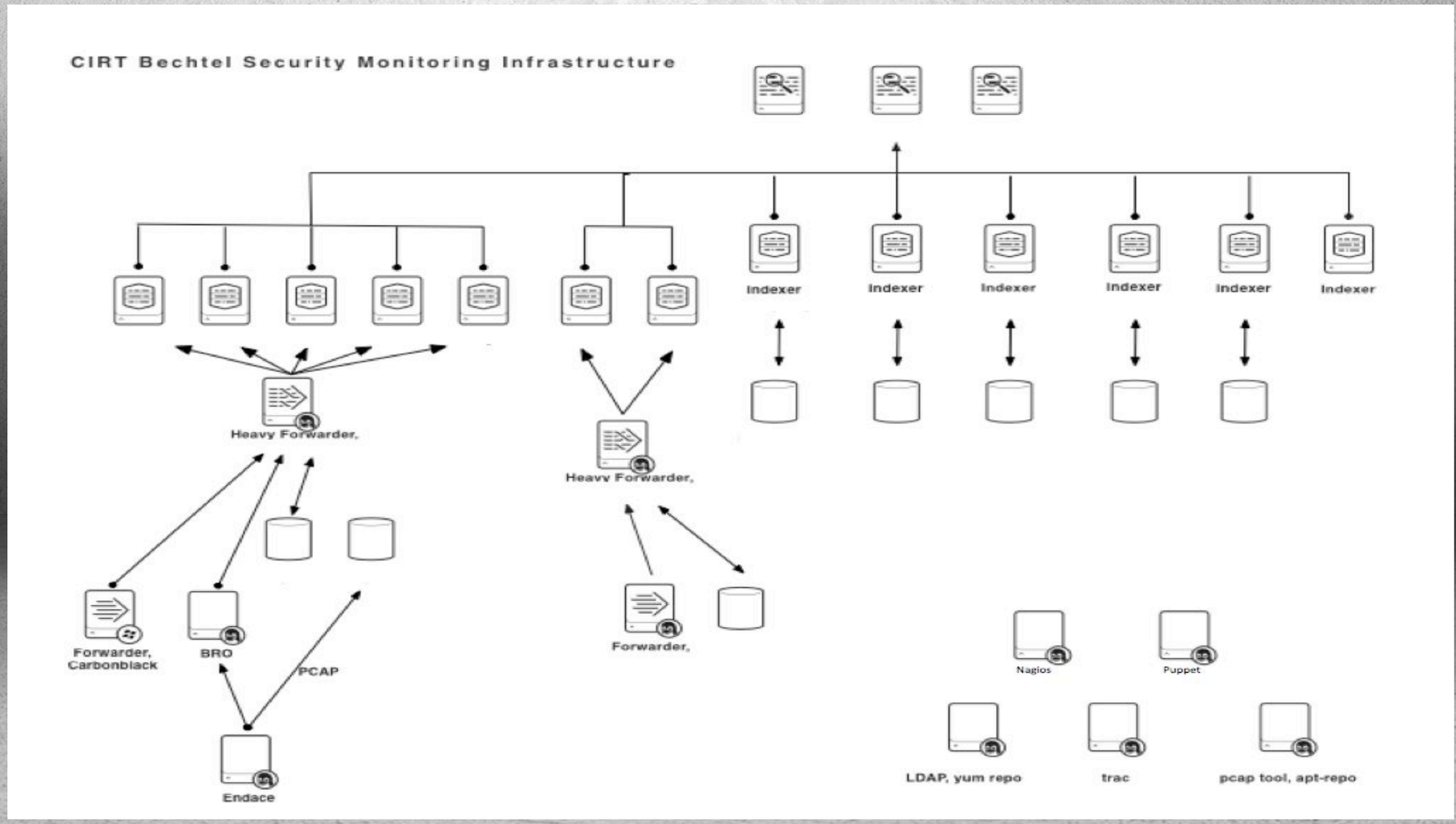
-The all VIRTUAL Splunk



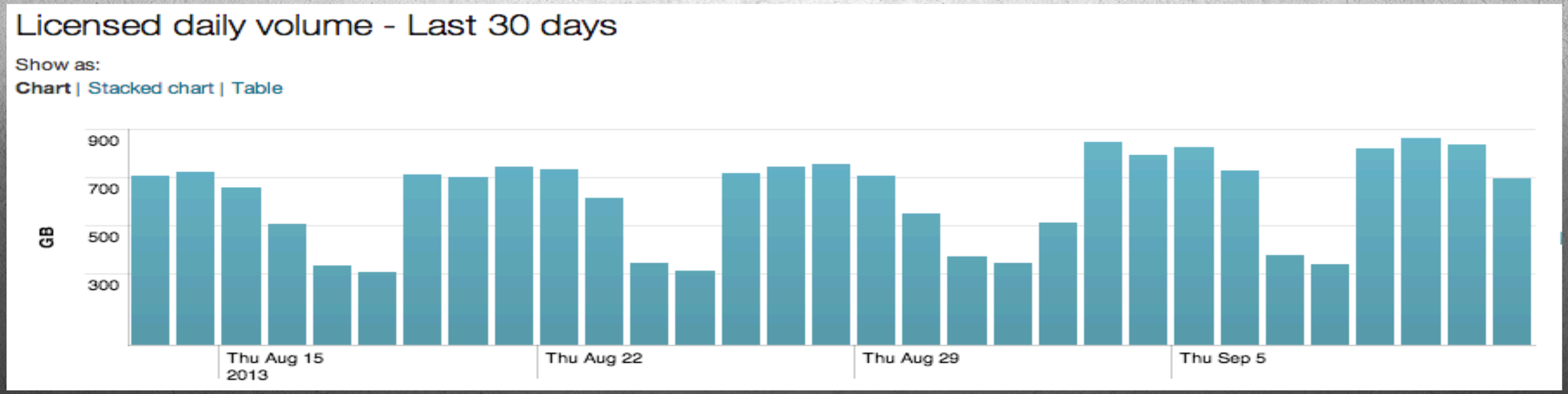
Hardware

By Remediation Week	Post Remediation Week
7 Indexers	13 Indexers
0 Search Heads • RESTFUL Interface to query all indexers	3 Search Heads • CIRT / SOC • Scheduled • IT Operations
~14 Log Sources	~27 Log Sources
Commodity Hardware doing 60 IOPS per server	Enterprise Class Hardware doing 1470 IOPS per server
600 TB SAN Storage	35 Additional TB of Onboard Storage

Where Are We Now?



Splunk Stats



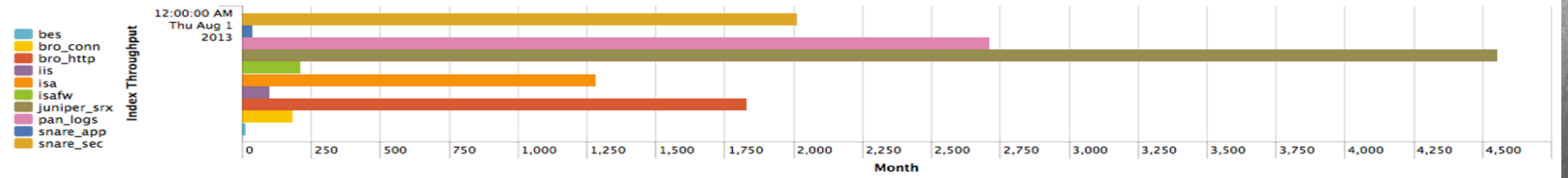
- ~70 Scheduled Searched (1450 times per day)
  - Results in ~35 tickets reviewed by the SOC

- ~1000 User Initiated Searches

August Stats

Monthly Metrics

Top 10 Indexes — 10d ago



View results

Total Monthly License Usage (GB) — 10d ago

17745

Daily Average Index Volume for ALL Indexes (GB) — 10d ago

570

Daily Average Indexing Volume by Index (GB) — 10d ago

« prev 1 2 3 next »

	series	daily_avg_trend	avg_mb
1	juniper_srx		161670.13
2	pan_logs		101748.11
3	snare_sec		97305.07
4	bro_http		77058.95
5	isa		58991.60
6	isafw		24931.39
7	bro_conn		17271.35
8	unix		9344.41
9	iis		5574.69
10	os		5211.42
11	snare_app		3471.21
12	bes		3276.91
13	bro_weird		3022.15

Field Normalization

Bad things happen when you don't normalize your fields.....

```
earliest=-1d (index=iis OR index=juniper_srx OR index=isa* OR index=bro* OR index=pan_logs) ("113.160.249.221" OR
"115.238.238.30" OR "123.100.251.4" OR "132.248.45.198" OR "133.242.2.95" OR "142.54.183.218" OR "183.185.84.245"
OR "183.185.90.26" OR "188.165.95.171" OR "201.255.22.44" OR "204.11.64.216" OR "210.19.7.136" OR
"211.11.140.128" OR "218.237.2.121" OR "218.237.2.2" OR "218.237.2.3" OR "218.237.2.4" OR "218.237.2.5" OR
"31.184.244.18" OR "69.128.68.190" OR "69.128.69.190" OR "70.33.247.100" OR "93.89.66.247" OR "94.75.243.14")|
eval XSRC_IPX=coalesce(src_ip,source_address,cs_ip)|eval XSRC_PORTX=coalesce(src_port,source_port)|eval
XDEST_IPX=coalesce(dest_ip,dst_ip,destination_address,s_ip)|eval
XDEST_PORTX=coalesce(dest_port,destination_port,s_port)|eval XSESSIONX=coalesce(uid,session_id,session_id_32)|
eval XBYTES_INX=coalesce(cs_bytes,bytes_from_client,bytes_in,content_len,orig_ip_bytes)|eval
XBYTES_OUTX=coalesce(sc_bytes,response_body_len,bytes_from_server,bytes_out,resp_ip_bytes,resp_size)|eval
XACTION_METHODX=coalesce(cs_method,method,action,http_method,qtype_name,client)|eval
XRESPONSEX=coalesce(status_code,sc_status,http_response,reason,answers,server)|eval
XUSERX=coalesce(username,user,cs_username,to)|eval XMIMEX=coalesce(mime_type,content_type,cs_mime_type)|eval
XURLX=coalesce(cs_host+cs_uri_stem,domain+uri,misc,url,server_name,query)|eval
XREFERX=coalesce(cs_referer,referrer,http_refer)|eval XDETAILSX=coalesce(post_data,filename+md5,addl,service_name
+attack_name,app_layer,version+cipher,analyzer+failure_reason,msg,direction)|table
_time,index,XSRC_IPX,XSRC_PORTX,XDEST_IPX,XDEST_PORTX,XSESSIONX,XBYTES_INX,XBYTES_OUTX,XACTION_METHODX,XRESPONSEX
,XUSERX,XMIMEX,XURLX,XREFERX,XDETAILSX,user_agent,splunk_server
```

CIRT
BECHTEL IS&T

Functional Security Operations

Case Study – Splunk For IR


CIRT
BECHTEL IS&T