Build Your Own SIEM

Kyle Donnelly – Security Engineer – Haas Automation
Zane Gittins – Security Engineer – Haas Automation

Our Backgrounds

- Kyle
  - ~4.5 Years @ Haas
  - Multiple Technical Roles
  - CSU Chico Alum
- Zane
  - ~1.5 Years @ Haas
  - First Security Engineer
  - CSU Channel Islands Alum & Working on Graduate in Computer Science

What is a SIEM?

- Security Information and Event Management
- One Stop Shop

Why Build Your Own?

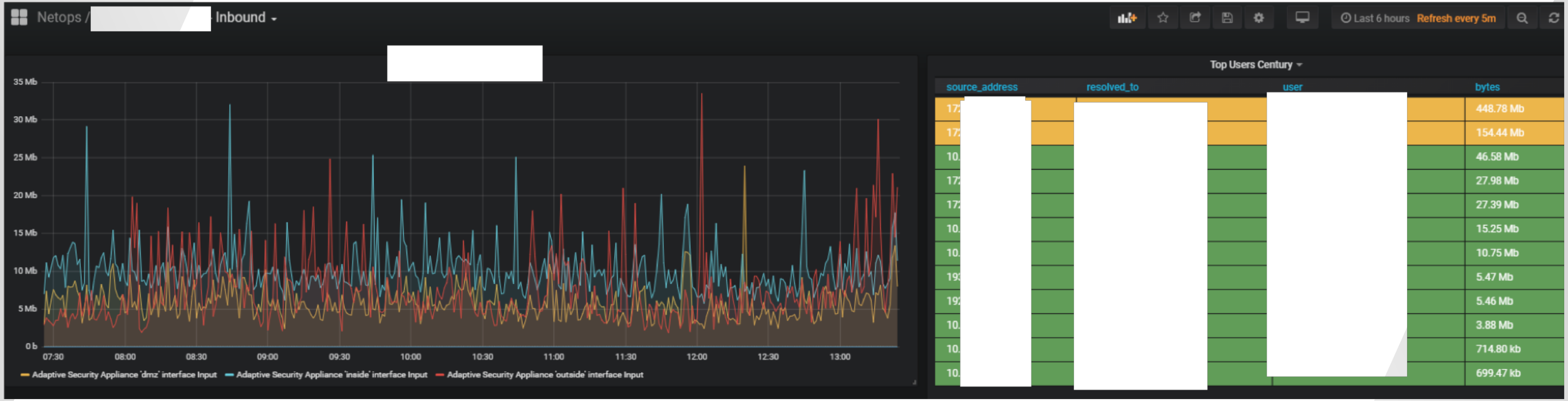
- Central Log Management
- Highly Configurable
- Gets Grease Under Fingernails
- Only Cost Is Man Hours + VM's
- Scalable

Technologies Used

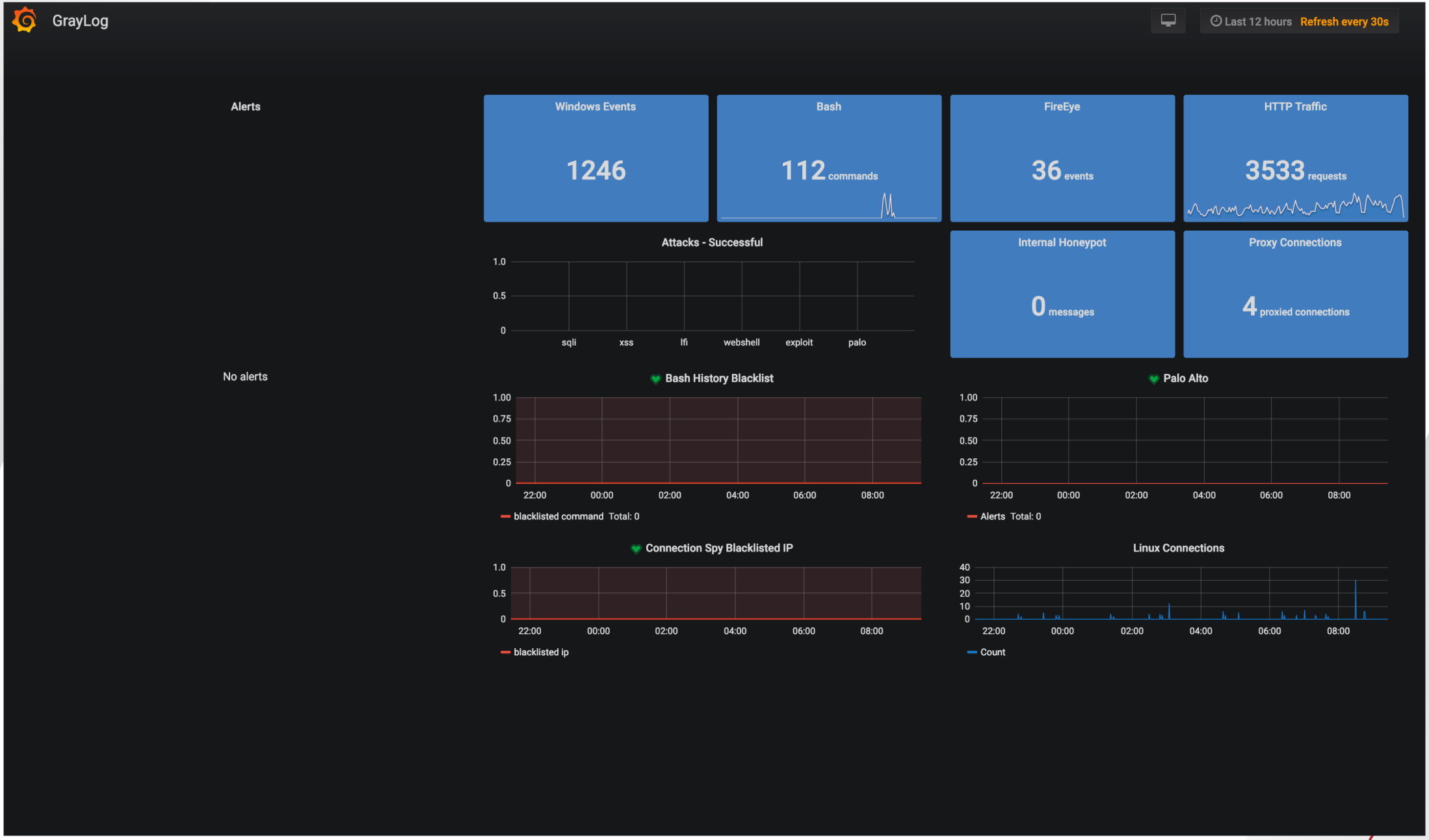
- Graylog
  - ElasticSearch
  - MongoDB
- Zabbix
  - MySQL
- Grafana
- Syslog
- Winlogbeat/Filebeat
- InfluxDB
- HAProxy
- CentOS/Ubuntu

Grafana

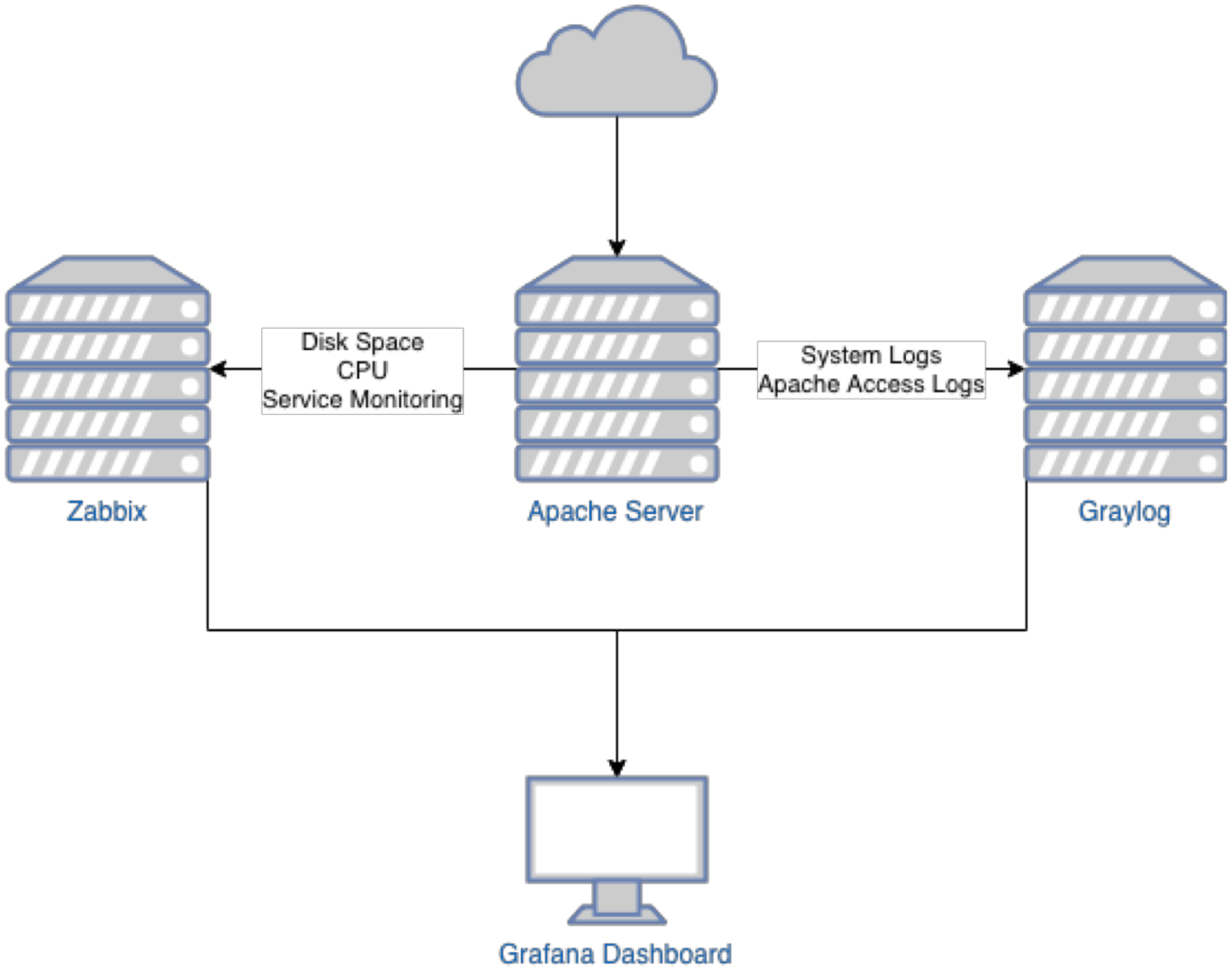
- Monitoring/Analytics Tool
- Dashboards
- Plugins
- Many DataSources
- Alerts

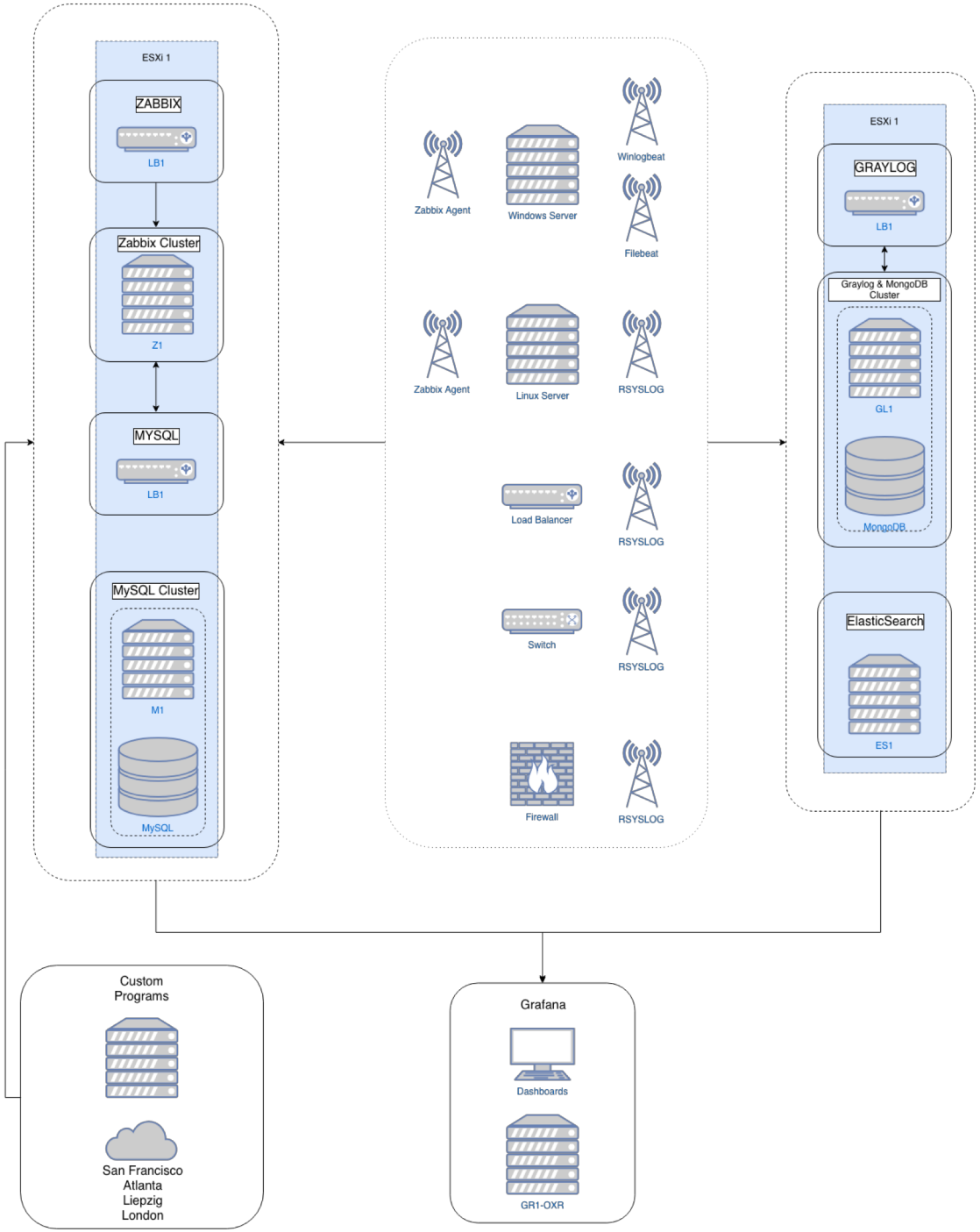


Haas F1 Team
OFFICIAL MACHINE TOOL


GrayLog
Last 12 hours
Refresh every 30s
Alerts
Windows Events
1246
Bash
112 commands
FireEye
36 events
HTTP Traffic
3533 requests
Attacks - Successful
1.0
0.5
0
sqli
xss
lfi
webshell
exploit
palo
Internal Honeypot
0 messages
Proxy Connections
4 proxied connections
No alerts
Bash History Blacklist
1.00
0.75
0.50
0.25
0
22:00
00:00
02:00
04:00
06:00
08:00
blacklisted command Total: 0
Palo Alto
Alerts Total: 0
Connection Spy Blacklisted IP
blacklisted ip
Linux Connections
40
30
20
10
Count

Landscape Overview

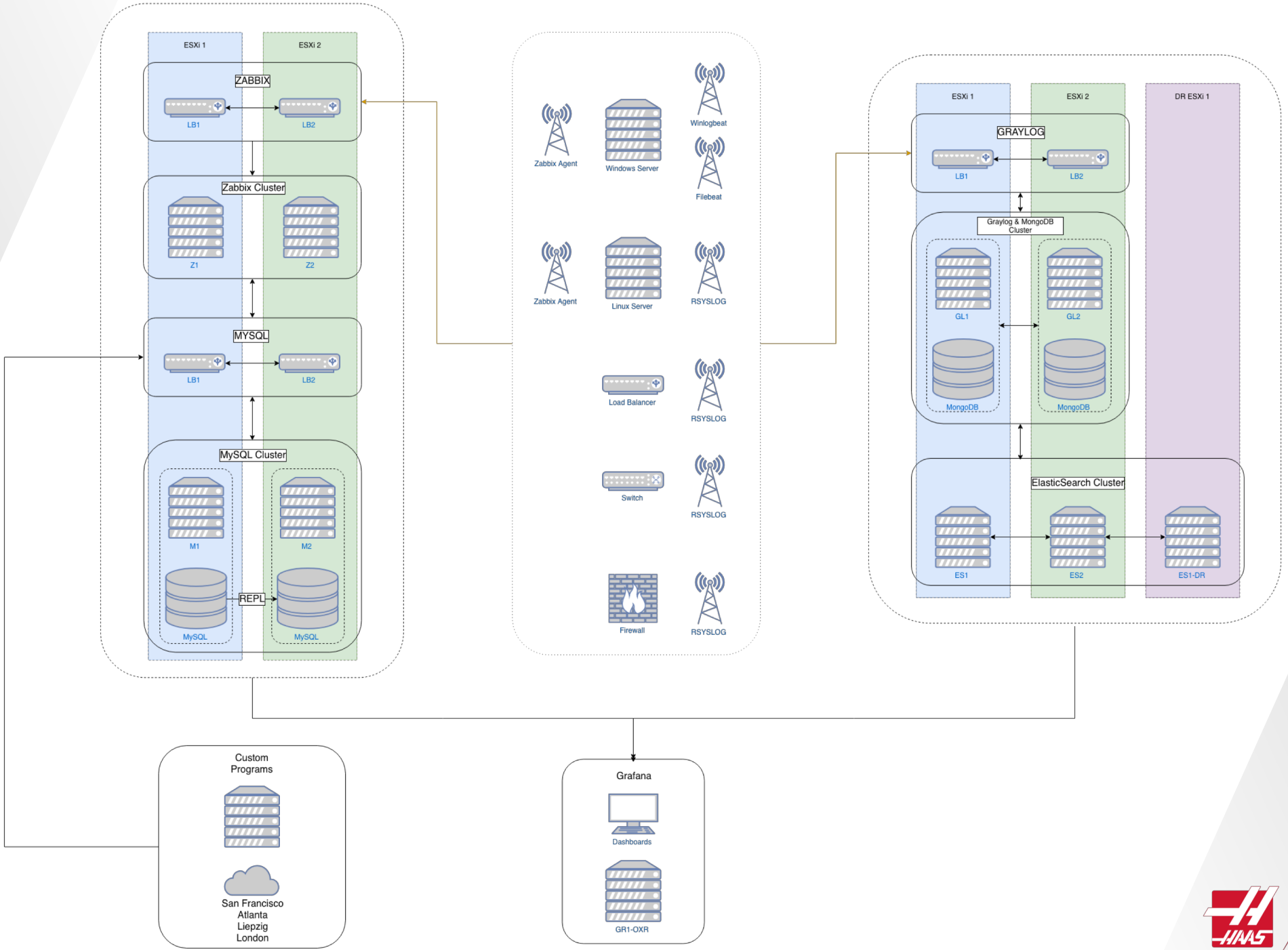




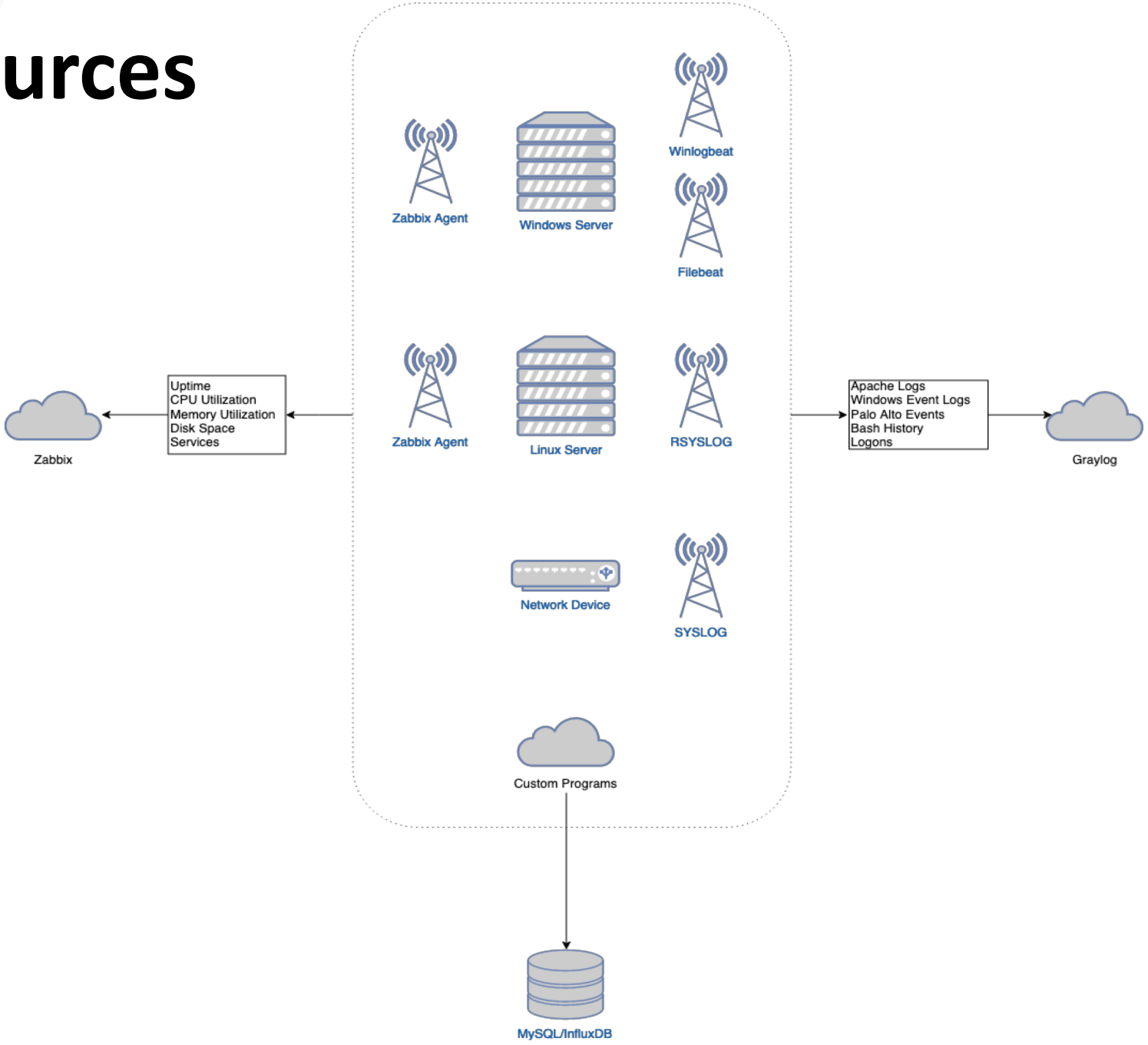
Haas F1 Team
OFFICIAL MACHINE TOOL

v1 Sizing

- Three VMs
- Zabbix/Grafana Server
  - 2 vCPU / 8GB RAM
  - 25 GB Disk (MySQL Database)
- Graylog Servers
  - Graylog/MongoDB
    - 4 vCPU / 4GB RAM
    - 25 GB Disk (MongoDB)
  - ElasticSearch
    - 4 vCPU / 16GB RAM
    - 100 GB Disk



Data Sources



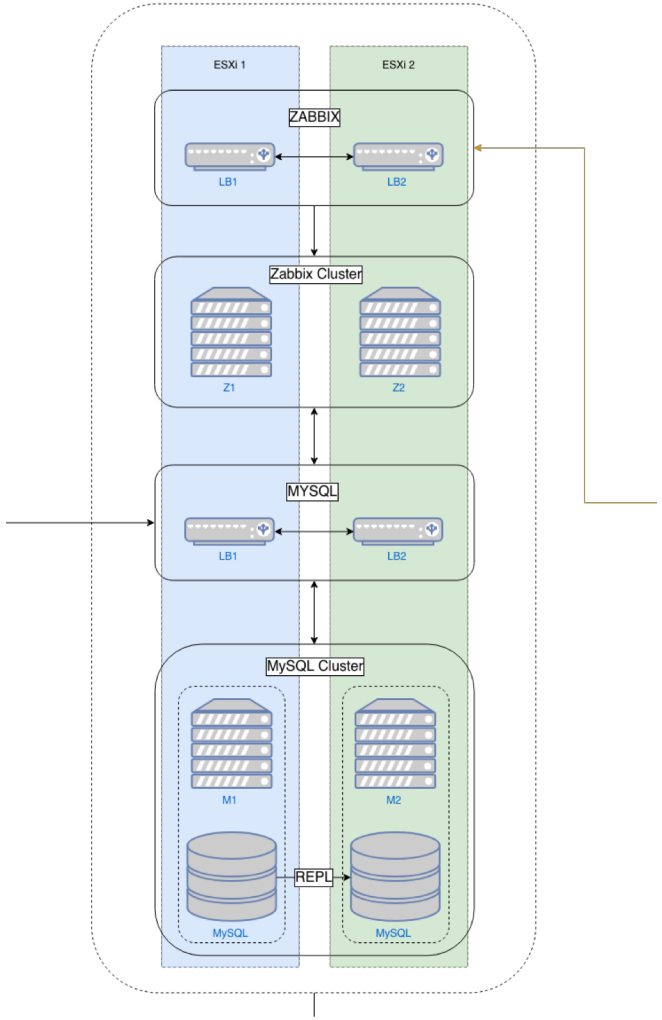
Data Sources

- Windows
  - Event Logs (Winlogbeat)
  - Flat File Logs (Filebeat)
- Linux
  - System Logs (Rsyslog)
  - Application Logs (Local Facilities -> Rsyslog)
- Network Devices
  - Cisco Devices
  - Palo Alto
  - F5
- Zabbix
- Custom Programs/Scripts
  - San Francisco

Zabbix Overview

- Open Source Monitoring Tool
- Agent & Agentless
- 3.4 -> 4.0 LTS
- Web GUI

Zabbix Landscape



Zabbix Server

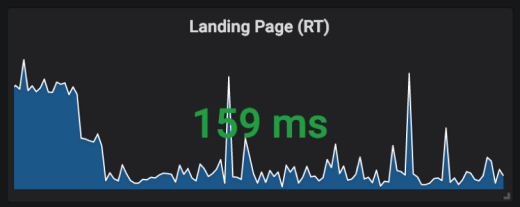
- Host Monitoring
  - CPU
  - Disk
  - Memory
  - Services
- Web Monitoring
  - Unit Testing
  - Performance Testing

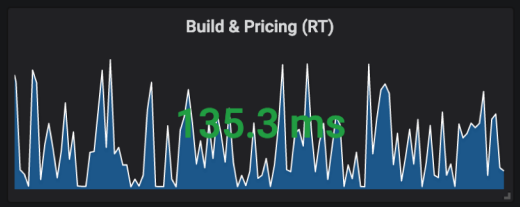
Wizard	Name ▲	Triggers	Key
•••	Haas - Windows: Agent ping	Triggers 1	agent.ping
•••	Haas - Windows: Average disk read queue length		perf_counter[\234(_Total)\1402]
•••	Haas - Windows: Average disk write queue length		perf_counter[\234(_Total)\1404]
•••	Haas - Windows: File read bytes per second		perf_counter[\2\16]
•••	Haas - Windows: File write bytes per second		perf_counter[\2\18]
•••	Mounted filesystem discovery: Free disk space on C:		vfs.fs.size[C:,free]
•••	Mounted filesystem discovery: Free disk space on E:		vfs.fs.size[E:,free]
•••	Mounted filesystem discovery: Free disk space on C: (percentage)	Triggers 1	vfs.fs.size[C:,pfree]
•••	Mounted filesystem discovery: Free disk space on E: (percentage)	Triggers 1	vfs.fs.size[E:,pfree]

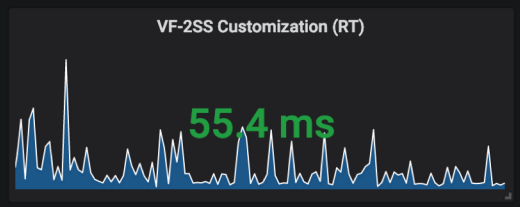
Severity	Name ▲
Average	Mounted filesystem discovery: Free disk space is less than 10% on volume C:
Average	Mounted filesystem discovery: Free disk space is less than 10% on volume E:
Average	Haas - Windows: Host information was changed on {HOST.NAME}
Information	Haas - Windows: Host name of zabbix_agentd was changed on {HOST.NAME}
Average	Haas - Windows: Lack of available virtual memory on server {HOST.NAME}
Average	Haas - Windows: Lack of free memory on server {HOST.NAME}
Average	Haas - Windows: Processor load is too high on {HOST.NAME}
High	SQL Service Broker Status
High	TCP Tunnel Status
Average	Haas - Windows: Too many processes on {HOST.NAME}
Information	Haas - Windows: Version of zabbix_agent(d) was changed on {HOST.NAME}
Average	Haas - Windows: Zabbix agent on {HOST.NAME} is unreachable for 5 minutes
Average	Haas - Windows: {HOST.NAME} has just been restarted

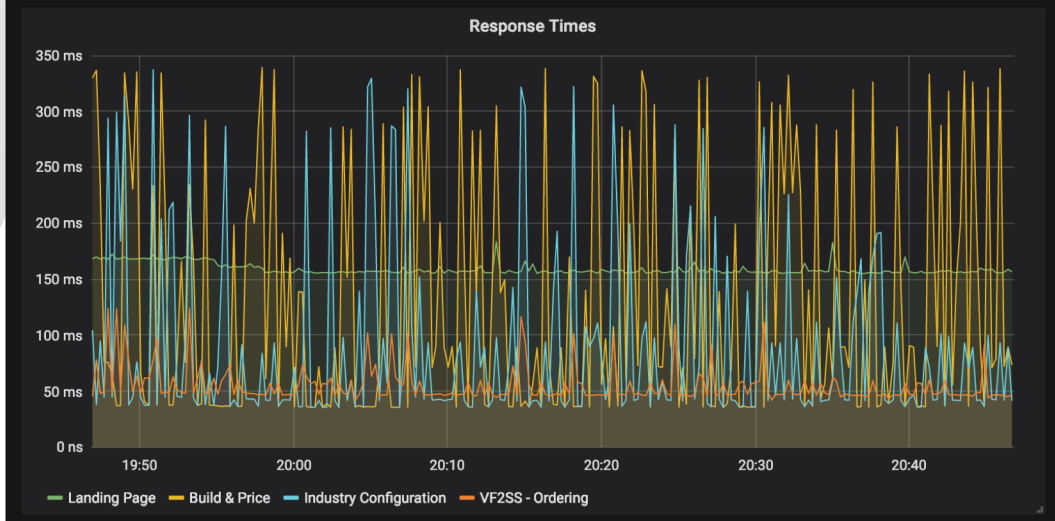
https://haascnc.com

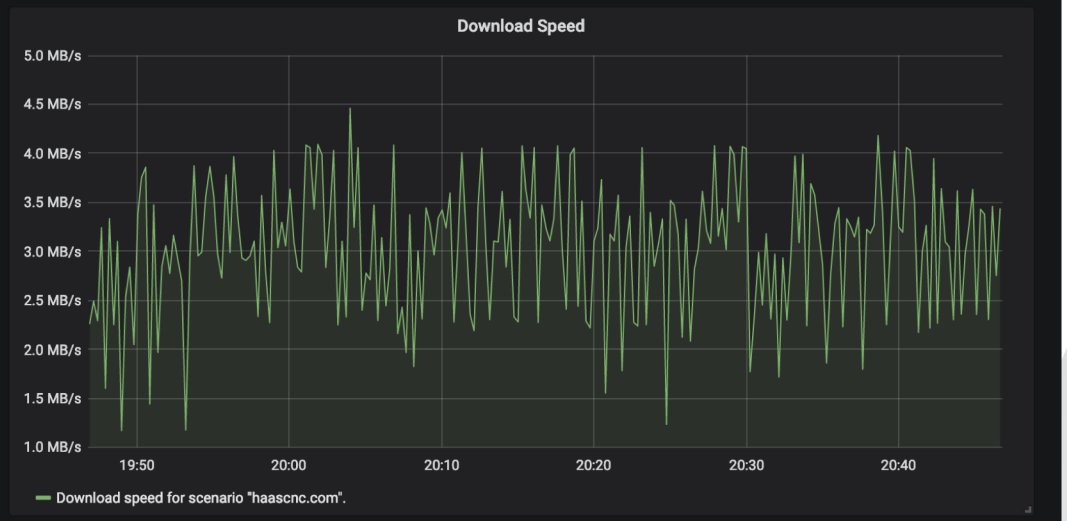
Up

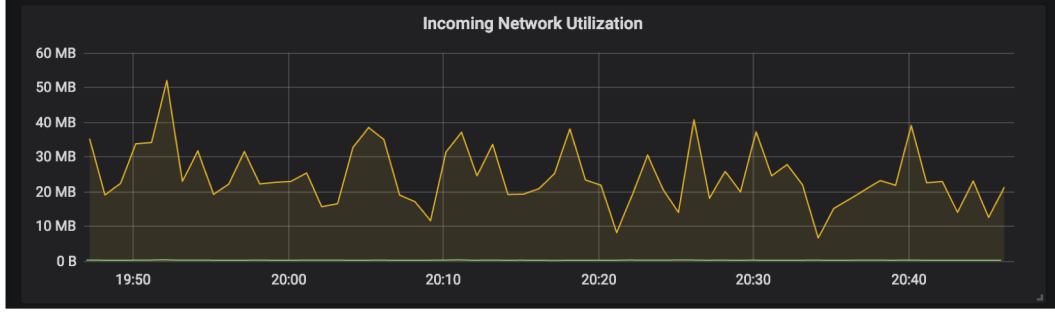


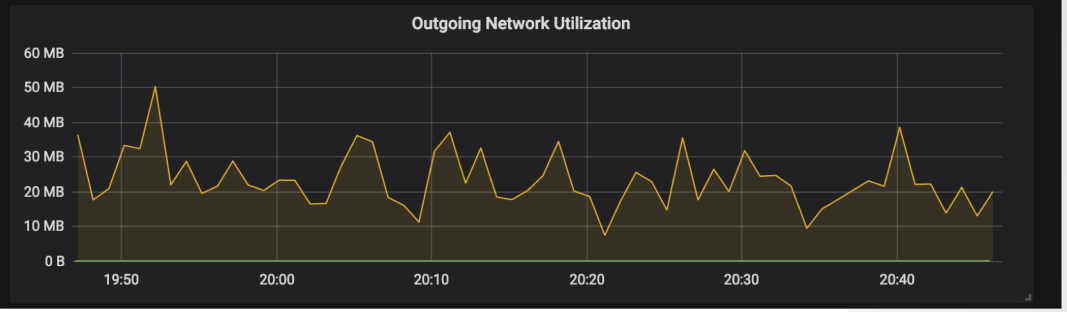




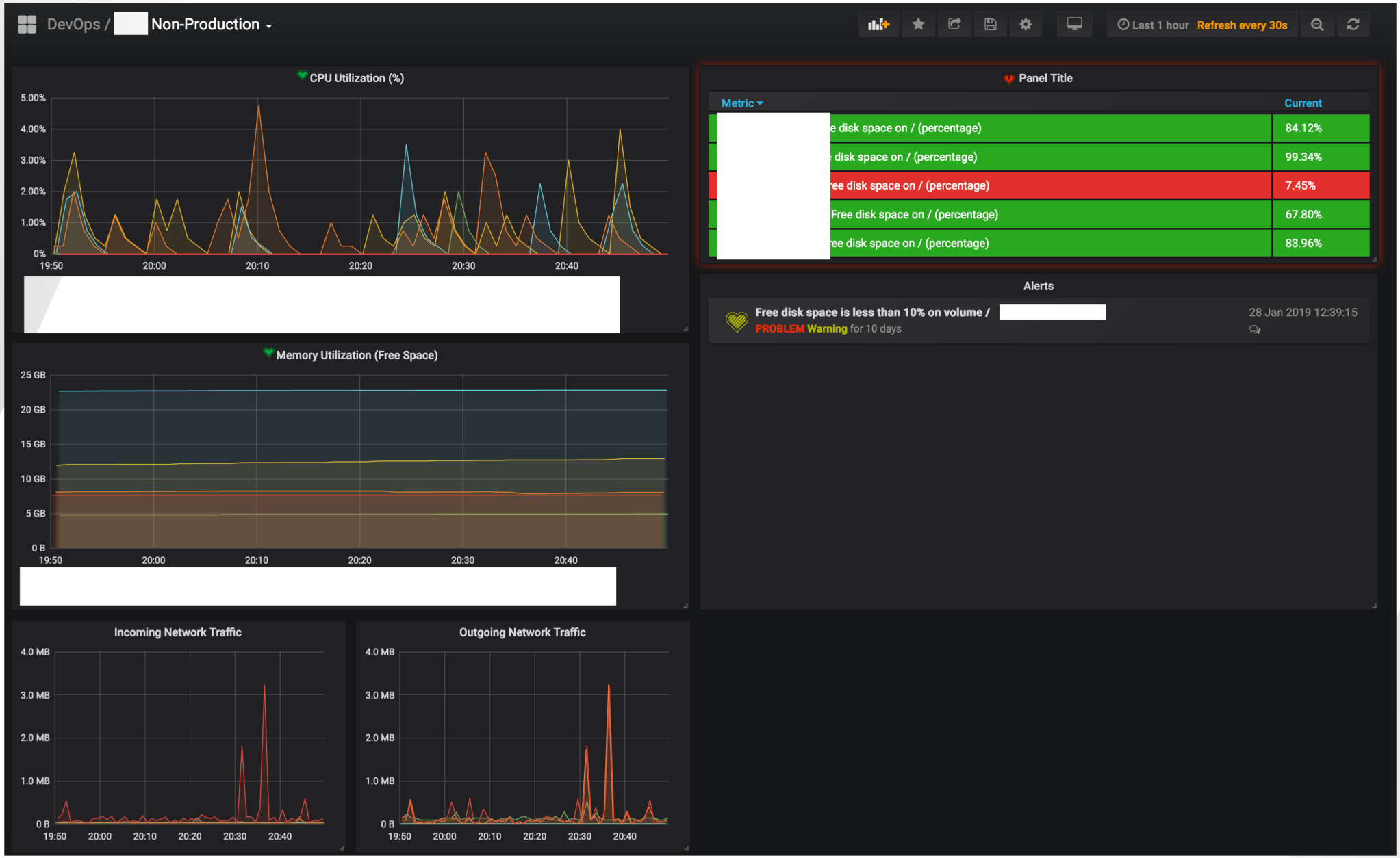








Haas F1 Team
OFFICIAL MACHINE TOOL

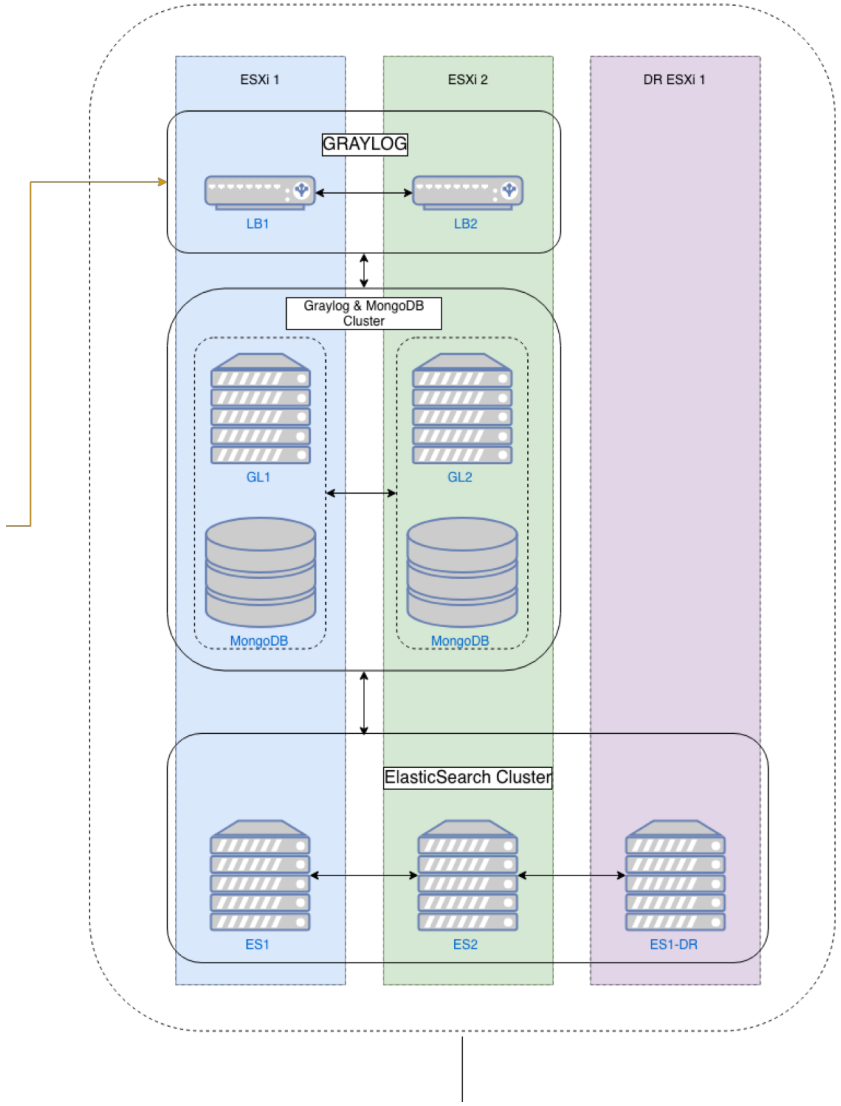


Haas F1 Team
OFFICIAL MACHINE TOOL

GrayLog Overview

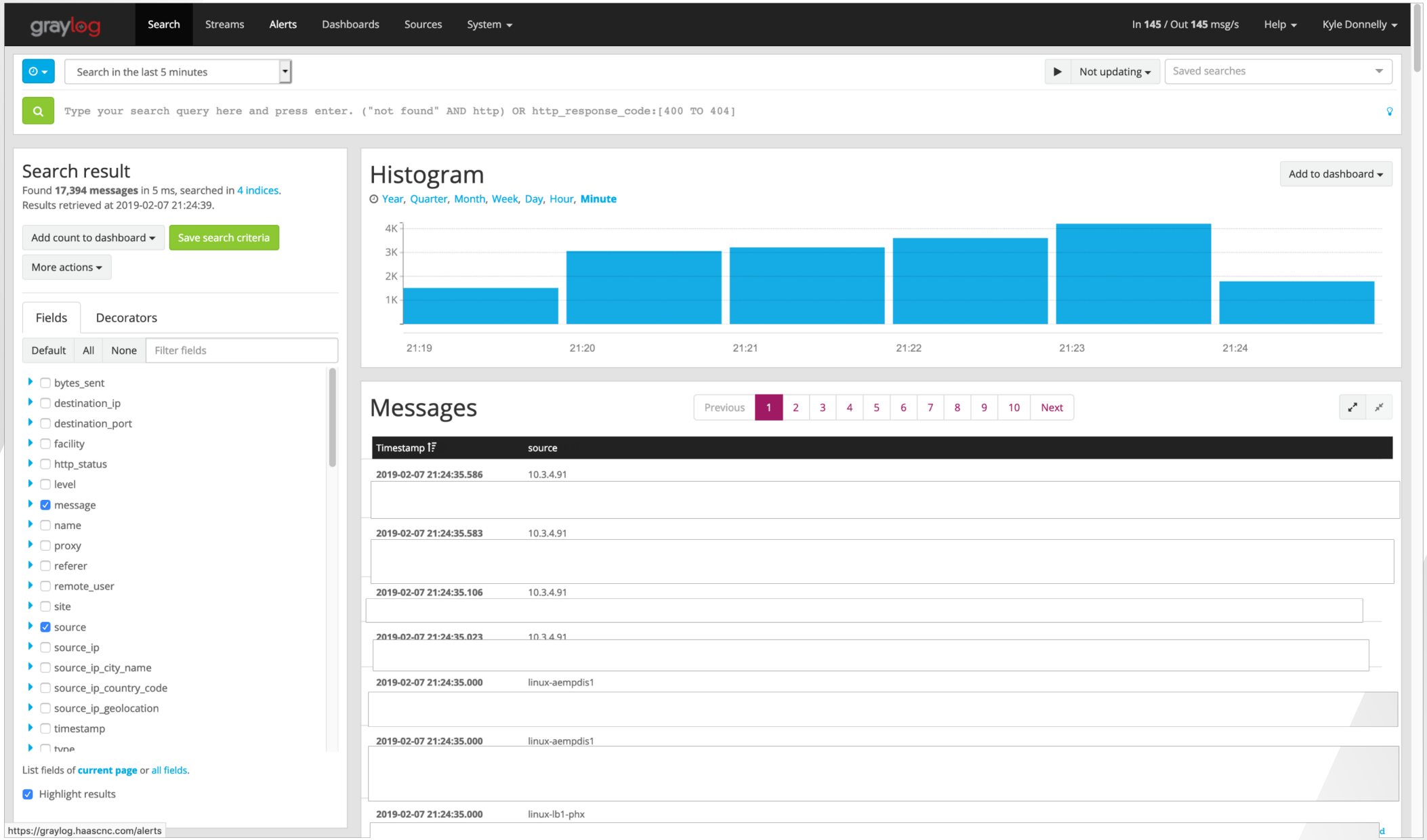
- Log Management Platform
- Intuitive Web Console
- MongoDB/ElasticSearch
- 2.5 -> 3.0 LTS

GrayLog Landscape



GrayLog Server

- Network/System/Application Logs
  - RSYSLOG – Linux
    - Application
  - SYSLOG – Appliances
  - Filebeat
  - Winlogbeat

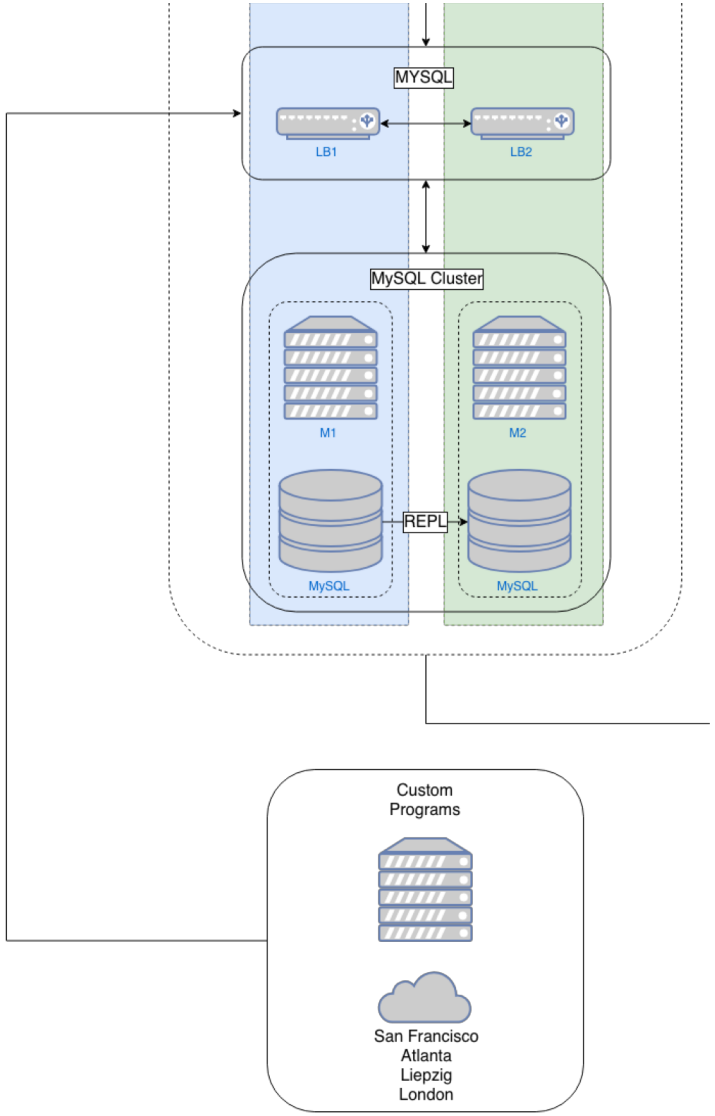


Haas F1 Team
OFFICIAL MACHINE TOOL

Custom Monitoring Programs

- Application Monitoring
- Custom Host Monitoring
- Database Monitoring

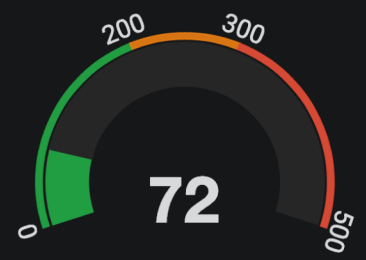
Custom Programs Landscape



PowerShell Example

- Get-NetTCPConnection -LocalPort 443
- Write Script to Parse Returned Values
- Put on Scheduled Task
- Script + Zabbix

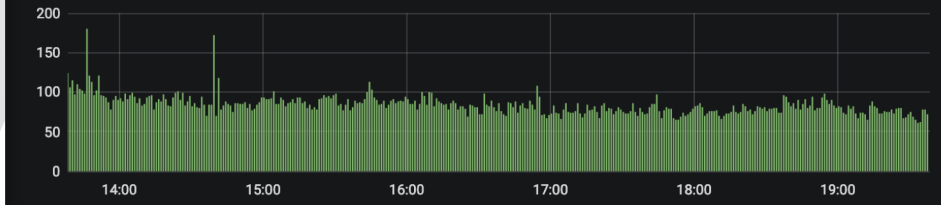
[redacted] Current



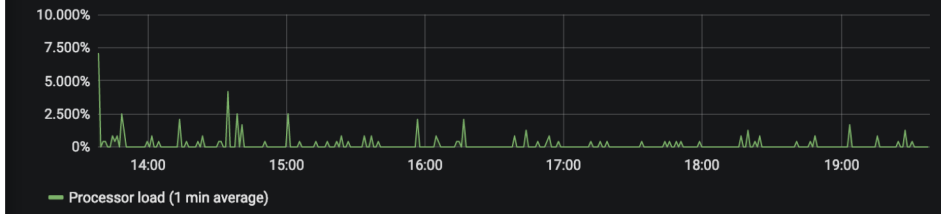
[redacted] Uptime

6 days

Connections



[redacted]



Disk Space

Metric	Current ▲
Free disk space on C: (percentage)	40.37%
Free disk space on E: (percentage)	98.21%

[redacted] Multiple External Connections — Last 1 minute

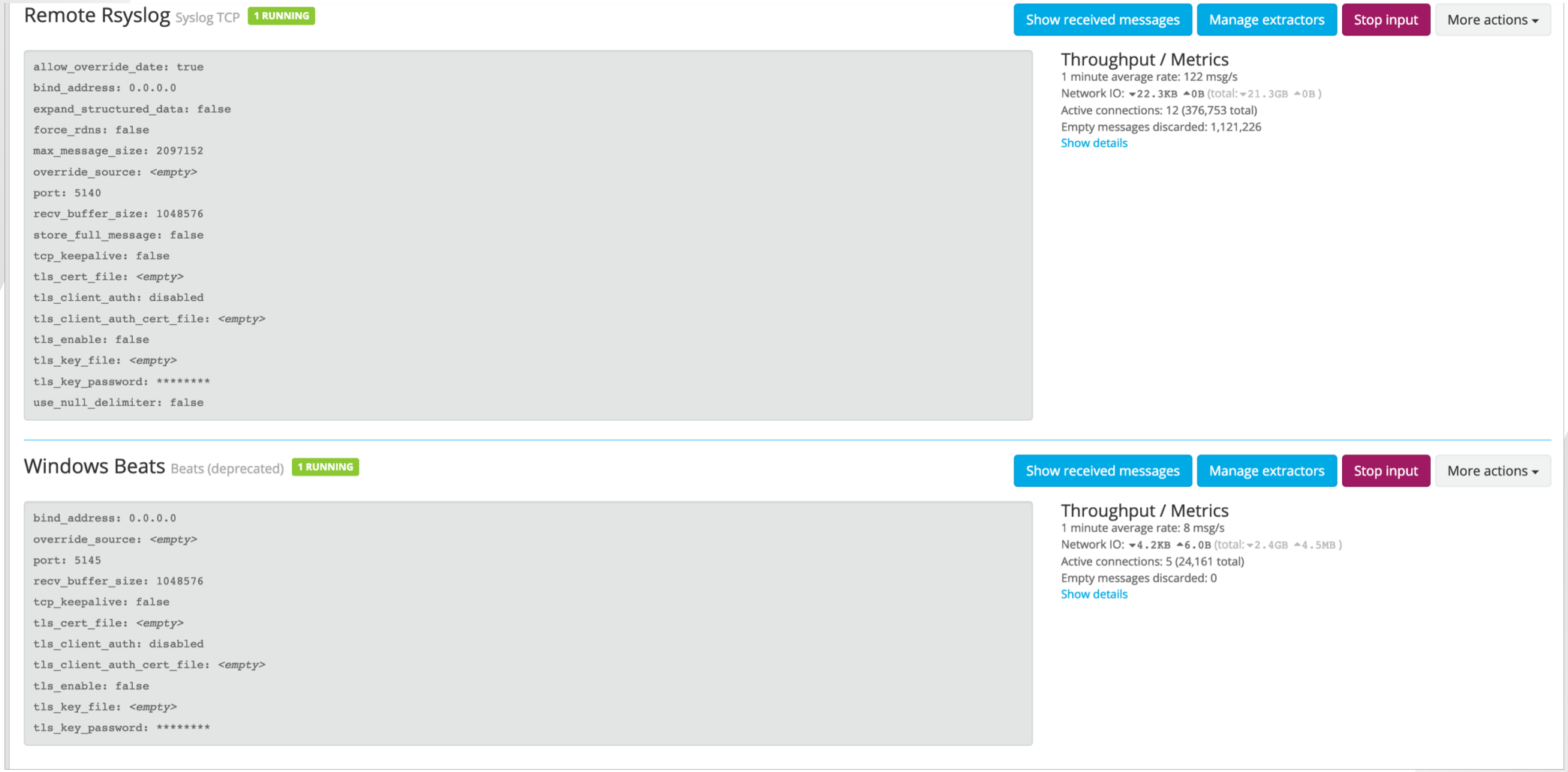
[redacted]remote_address	Time	Count ▼
12.20[redacted]	2019-02-07 19:37:53	3
173.17[redacted]	2019-02-07 19:37:53	3
70.29.[redacted]	2019-02-07 19:37:53	3
173.8[redacted]	2019-02-07 19:37:53	2
196.9[redacted]	2019-02-07 19:37:53	2
196.9[redacted]	2019-02-07 19:37:53	2
196.9[redacted]	2019-02-07 19:37:53	2
204.2[redacted]	2019-02-07 19:37:53	2

[redacted]Internal Connections — Last 1 hour

[redacted]emote_address	[redacted]remote_port	[redacted]_state	Time ▼	Count
172[redacted]	49922	Established	2019-02-07 19:37:53	1.00
172[redacted]	49972	Established	2019-02-07 19:37:53	1.00
10.2[redacted]	52420	Established	2019-02-07 19:37:53	1.00
10.2[redacted]	52408	Established	2019-02-07 19:36:53	1.00
172[redacted]	49944	Established	2019-02-07 19:35:53	1.00
10.2[redacted]	52396	Established	2019-02-07 19:35:53	1.00
172[redacted]	49930	Established	2019-02-07 19:34:53	1.00
10.2[redacted]	52383	Established	2019-02-07 19:34:53	1.00
10.2[redacted]	52371	Established	2019-02-07 19:33:53	1.00

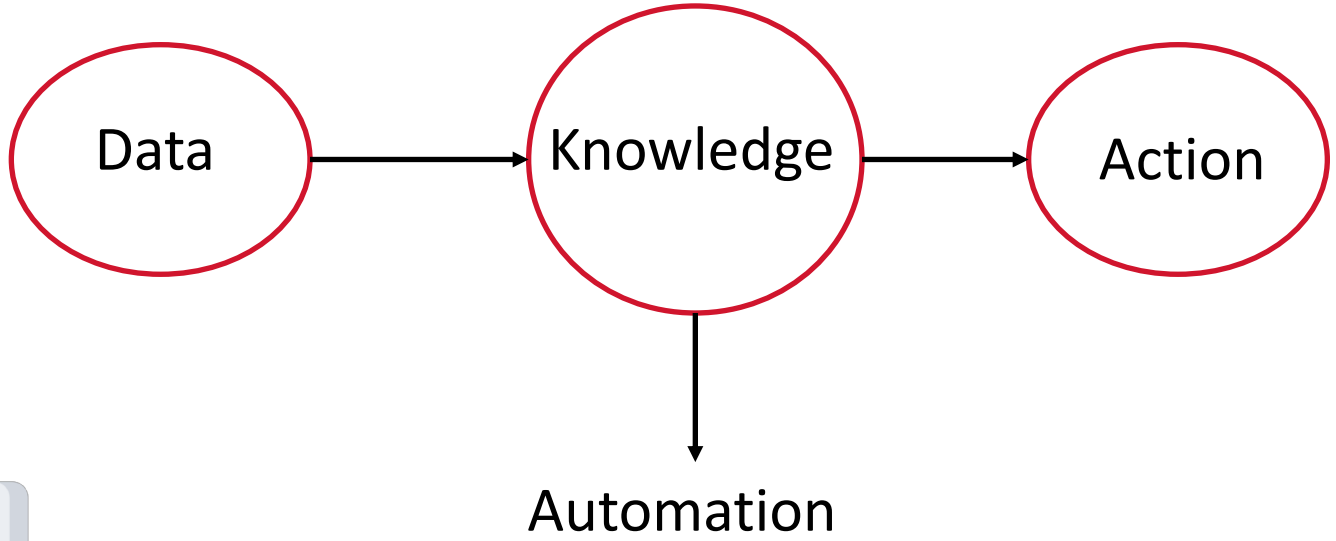
Alerts

Inputs



Meaningful Data

- Extractors.
- Pipelines.
- Code.



Extractors

- Copy Input
- Grok Patterns
- JSON
- Regex
- Delimiters
- Substrings
- Lookup Tables

55.3.244.1 GET /index.html 15824 0.043

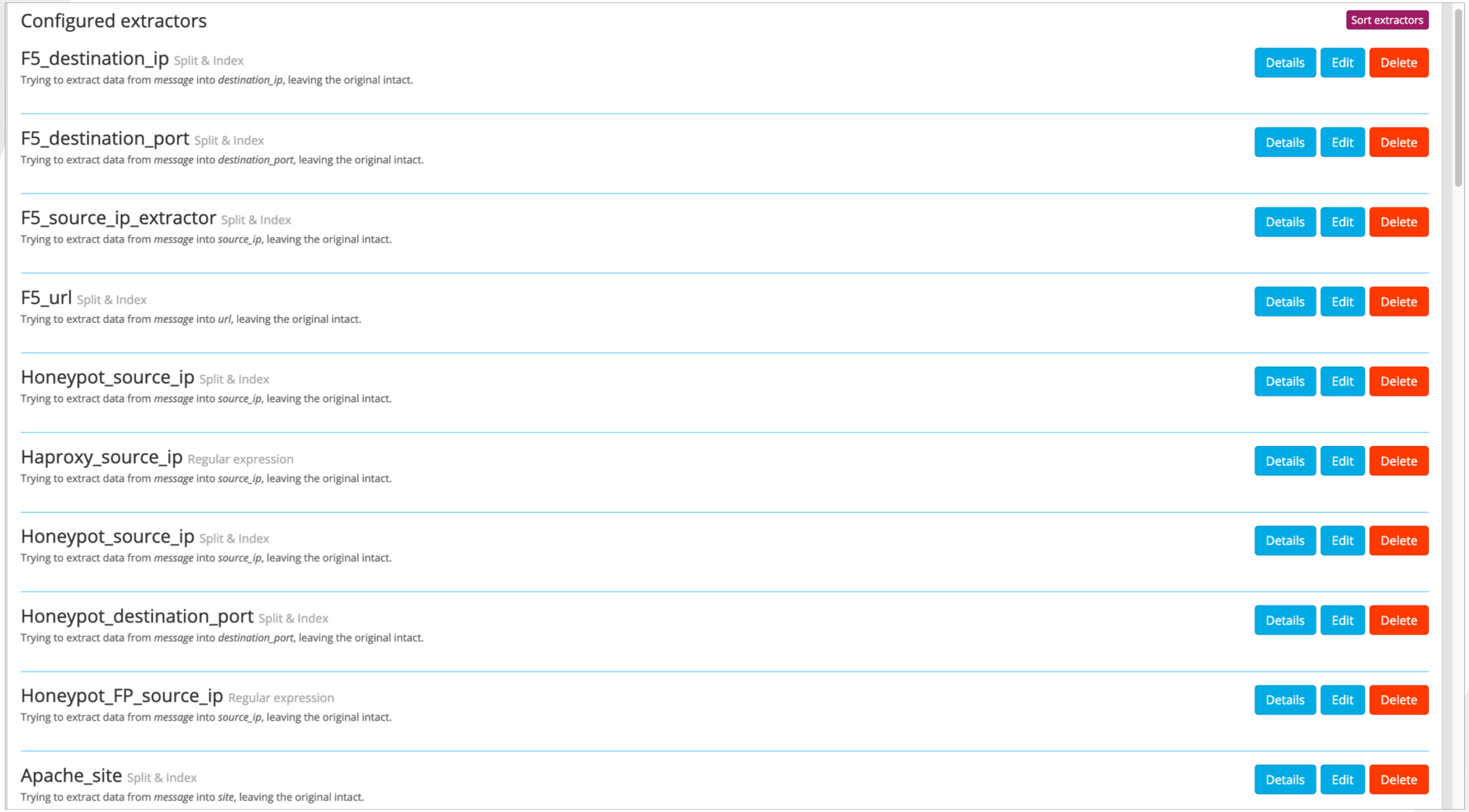
%{IP:client} %{WORD:method}
%{URIPATHPARAM:request} %{NUMBER:bytes}
%{NUMBER:duration}

Extractors: Use Case

- Identify malicious activity in Apache logs.

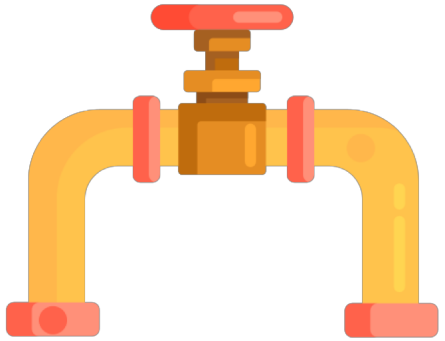
apache-access example.server
<ip address>
POST /q.php HTTP/1.1 200

Extractors



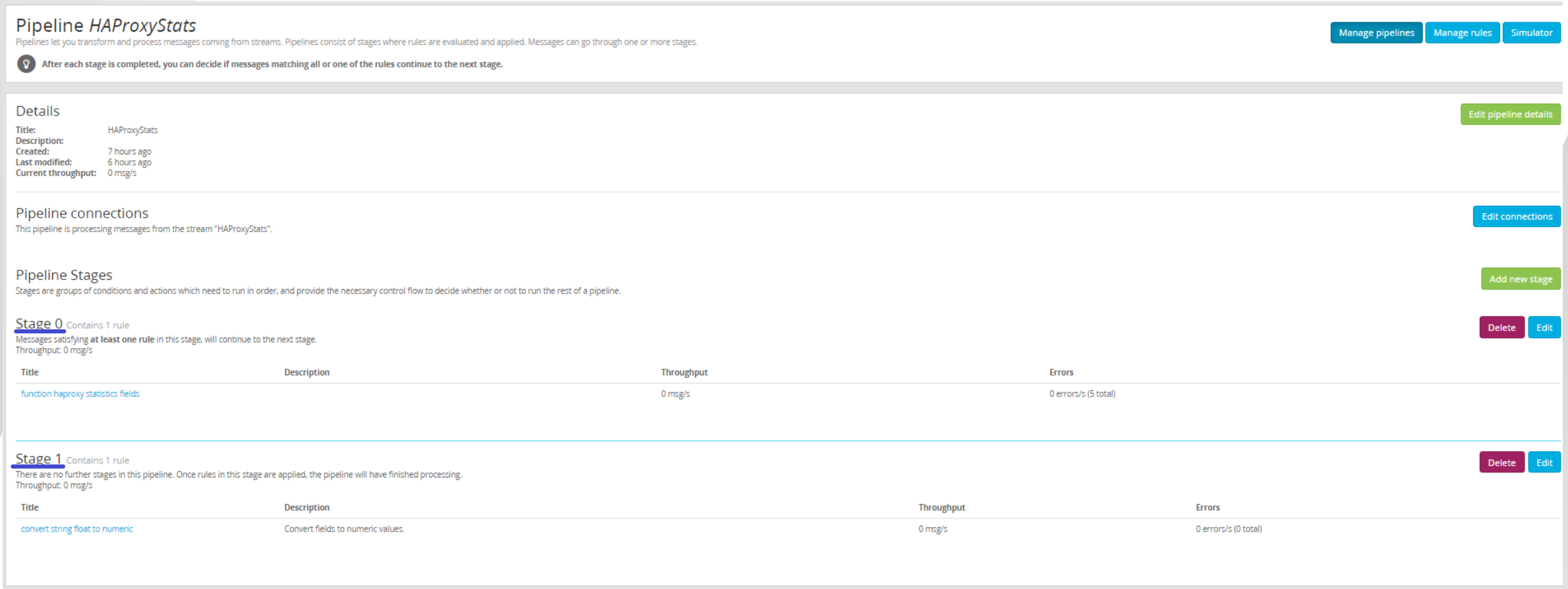
Pipelines

- Stages
- Rules



```
rule "has firewall fields"
when
        has_field("src_ip") && has_field("dst_ip")
then
        <do action>
end
```

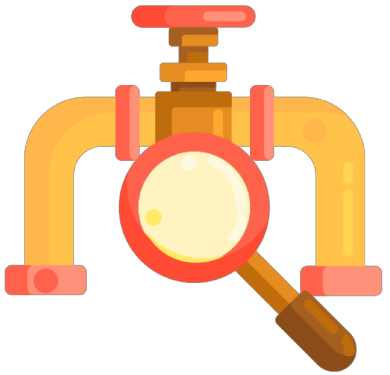
Pipelines



Haas F1 Team
OFFICIAL MACHINE TOOL

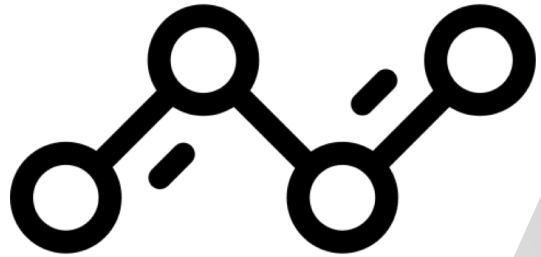
Pipelines: Use Case

- Clean “dirty” data.
- Drop noisy logs.
- Calculate hashes, match IP to CIDR, format dates, AlienVault OTX, Spamhaus, whois, and much more.



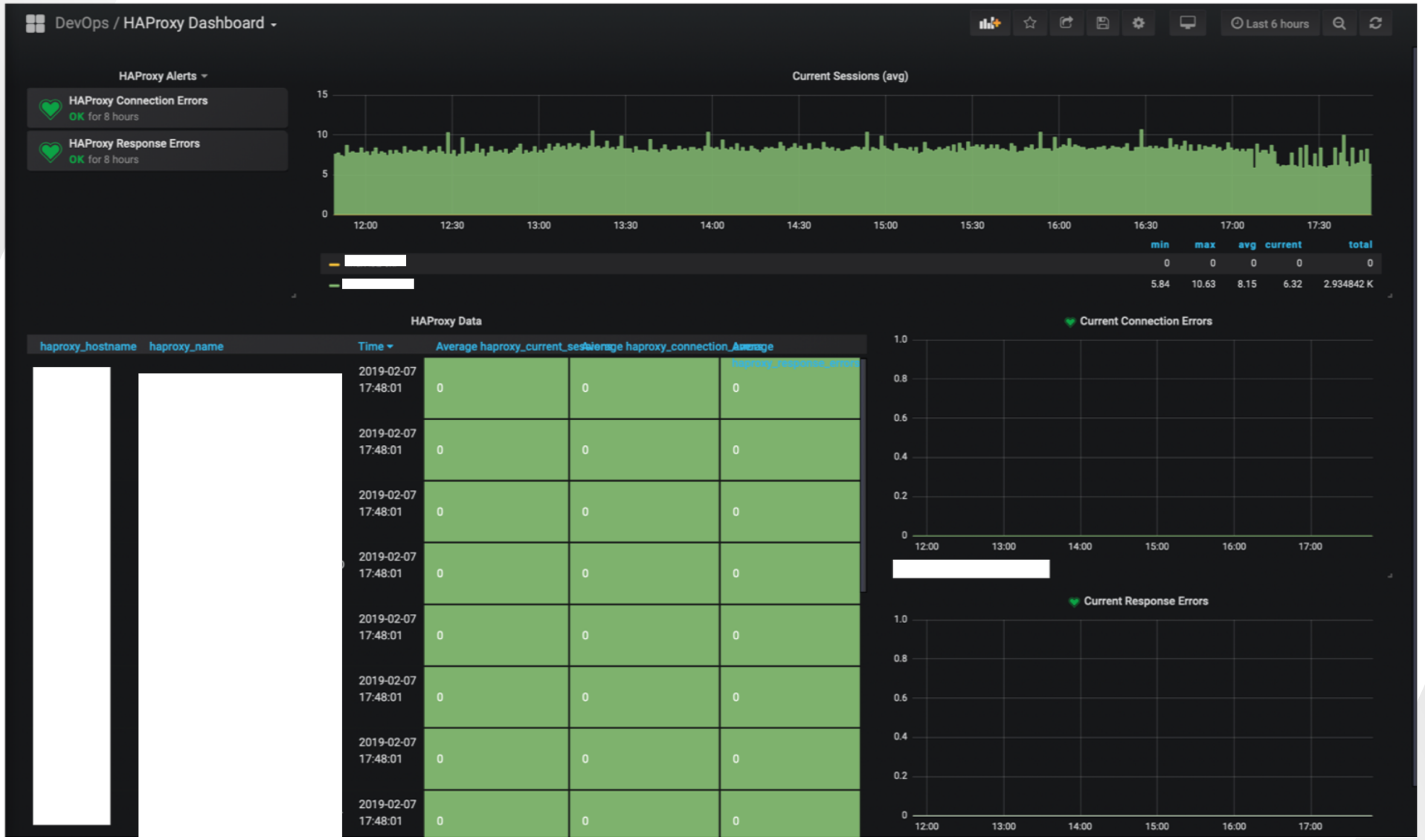
Code

- TCP connections.
- Most powerful and time consuming.
- Language considerations.



Code: Use Case

- Connectors.
- Multiple databases.
- Environment Specific.

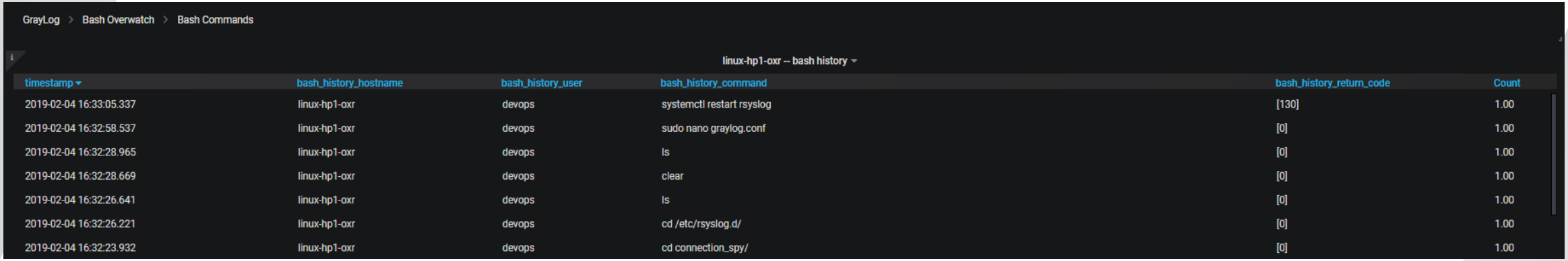


Haas F1 Team
OFFICIAL MACHINE TOOL

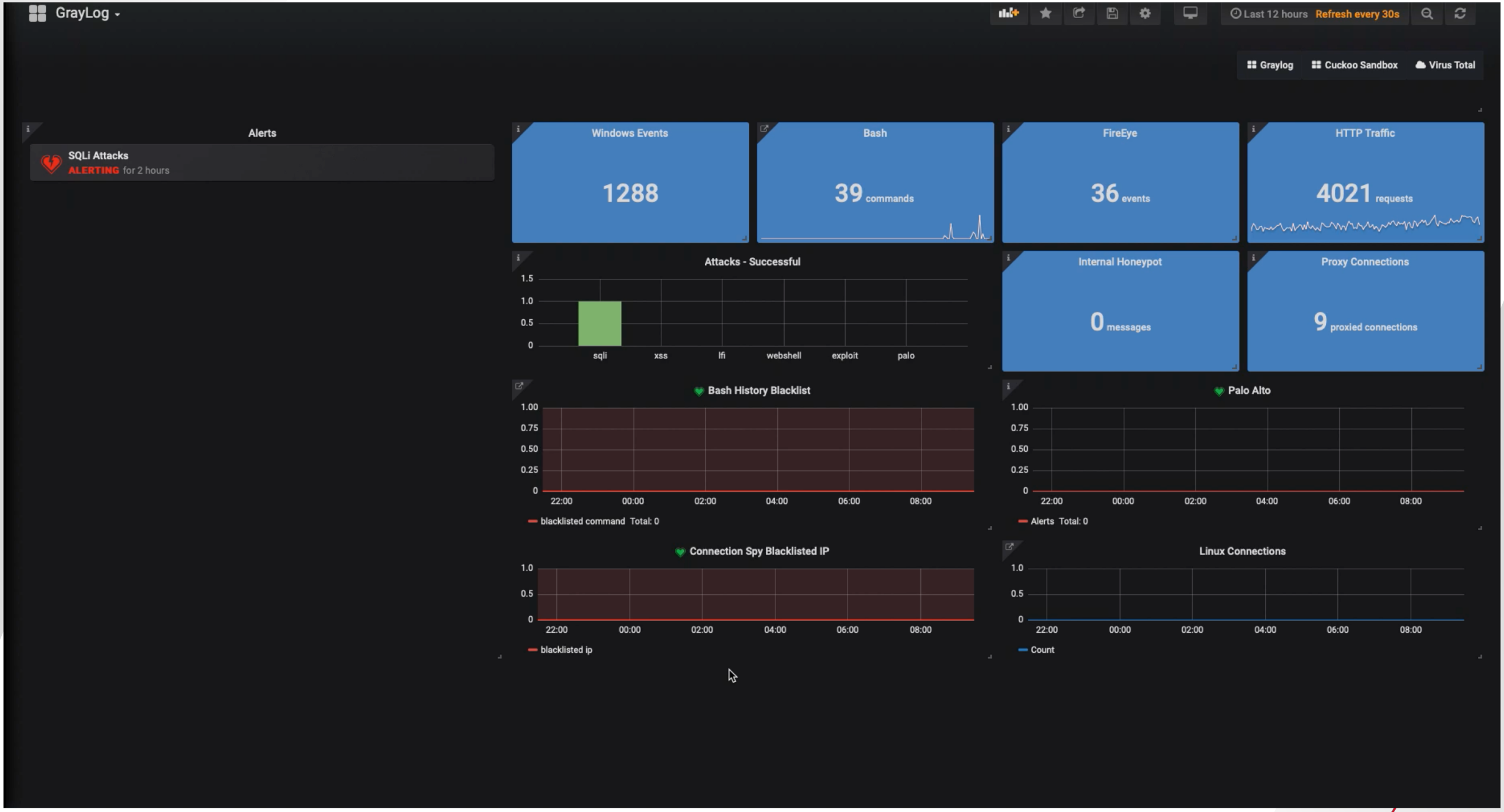
Drilldowns


GrayLog
Bash Overwatch
Bash command count fo
Drilldown
commands
04:00
08:00
12:00

Drilldowns



timestamp	bash_history_hostname	bash_history_user	bash_history_command	bash_history_return_code	Count
2019-02-04 16:33:05.337	linux-hp1-oxr	devops	systemctl restart rsyslog	[130]	1.00
2019-02-04 16:32:58.537	linux-hp1-oxr	devops	sudo nano graylog.conf	[0]	1.00
2019-02-04 16:32:28.965	linux-hp1-oxr	devops	ls	[0]	1.00
2019-02-04 16:32:28.669	linux-hp1-oxr	devops	clear	[0]	1.00
2019-02-04 16:32:26.641	linux-hp1-oxr	devops	ls	[0]	1.00
2019-02-04 16:32:26.221	linux-hp1-oxr	devops	cd /etc/rsyslog.d/	[0]	1.00
2019-02-04 16:32:23.932	linux-hp1-oxr	devops	cd connection_spy/	[0]	1.00



Alerting

- Know exactly why an alert triggers.

- Many Ways to Alert:
  - Email
  - Slack
  - SMS
  - And many more.

Appendix

- Rsyslog:
  - https://github.com/rsyslog/rsyslog
- Graylog
  - https://www.graylog.org/products/open-source
- Zabbix:
  - https://www.zabbix.com/
- Winlogbeat:
  - https://www.elastic.co/downloads/beats/winlogbeat-oss
  - https://www.elastic.co/guide/en/beats/winlogbeat/current/winlogbeat-getting-started.html
- Filebeat –
  - https://www.elastic.co/downloads/beats/filebeat-oss
  - https://www.elastic.co/guide/en/beats/filebeat/current/filebeat-getting-started.html
- ElasticSearch:
  - https://www.elastic.co/downloads/elasticsearch-oss
- Grafana:
  - http://docs.grafana.org/installation/debian/
- Icons:
  - www.flaticon.com