Scale it to a Billion

How to Build it, Keep it Safe, and Keep it Running
Scale it to a Billion

Pete Cheslock
@petecheslock - Twitter

Technical Operations at Threat Stack

https://pete.wtf
Introduction to Threat Stack

Modern Infrastructure Requires Modern Security.

✓ Audit Your Environment
✓ Continuously Monitor & Alert
✓ Investigate & Resolve
Reminder: Scale is Relative

• We are currently ingesting over hundreds of events per second

• From tens of thousands of agents

• Represents a total ingest rate of over 10 TB of raw events PER DAY
Jen: Yo, are you ready to support ~10 beta customers on a completely unautomated, unmonitored env?

Jen: 5 9s of availability.

Pete: New Phone, who dis?
The Right Way™
Threat Stack
Continuous Security Monitoring

Jen Andre, Chris Gervais
The Definitive Guide to Linux System Calls

Apr 5, 2016 • packagecloud

Tags: Linux kernel syscall

- TL;DR
- What is a system call?
- Prerequisite information
  - Hardware and software
  - User programs, the kernel, and CPU privilege levels
  - Interrupts
  - Model Specific Registers (MSRs)
  - Calling system calls with assembly is a bad idea
- Legacy system calls
Premature optimization is the root of all evil
@_lennart @petecheslock i think self-hosted metrics are going to become as archaic as running your own postfix/imap over the next few years
I'm okay with the events that are unfolding currently.

This is fine.
collectd -> write_http ->

(60 Second)

app1

app2

appN

statsd plugin
Money

Time

http://www.adamsii.com/wp-content/uploads/2015/03/time-is-money2.jpg
collectd -> write_http -> statsd plugin

(60 Second)

collectd -> write_graphite -> graphite

(10 Second)
0:00 /usr/sbin/collectdmon -P /var/run/collectd.pid -- -C /etc/collectd/collectd.conf
0:12 collectd -C /etc/collectd/collectd.conf -f
0:00 /usr/sbin/collectdmon -P /var/run/collectd-int.pid -- -C /etc/collectd-int/collectd.conf
0:28 collectd -C /etc/collectd-int/collectd.conf -f
https://github.com/hw-cookbooks/graphite

https://github.com/obfusccurity/synthesize
Metrics go in Carbon C Relay → Graphite A, Graphite B → Grafana
Want your Devs to Ops?

Build Consumable Services
Time Series is great - But we have bigger questions

• Who was the last user to login to X host and what commands did they run?

• Have any processes or users opened Y file in the last 24 hours?

• Which services have made outbound connections, and what IP’s did they connect to?
What about your S3 Buckets?

UpGuard’s blog explains how the firm came across the unprotected data:

“In the early evening of June 12th, UpGuard Cyber Risk Analyst Chris Vickery discovered an open cloud repository while searching for misconfigured data sources on behalf of the Cyber Risk Team, a research unit of UpGuard devoted to finding, securing, and raising public awareness of such exposures. The data repository, an Amazon Web Services S3 bucket, lacked any protection against access. As such, anyone with an internet connection could have accessed the Republican data operation used to power Donald Trump's presidential victory, simply by navigating to a six-character Amazon subdomain: “dra-dw”.”

https://www.upguard.com/breaches/the-rnc-files
Through 2020, 95% of cloud security failures will be the customers fault – Gartner

http://www.gartner.com/newsroom/id/3143718

Why It Will Happen
• Misconfiguration
• Mismanagement
• Human mistakes

@petecheslock
The State of OSS Security Tools?

- The ones I don’t like
- The ones I haven’t used yet
Why does auditd suck?

- Some (but not all) lines have data in key=value format
- Events can span multiple lines
- Events in the logs can be displayed out of order
- Potential for load impact on hosts

go-audit is an alternative to the auditd daemon that ships with many distros

https://slack.engineering/syscall-auditing-at-scale-e6a3ca8ac1b8
https://ossec.github.io
https://osquery.io

Performant Endpoint Visibility

osquery allows you to easily ask questions about your Linux, Windows, and macOS infrastructure. Whether your goal is intrusion detection, infrastructure reliability, or compliance, osquery gives you the ability to empower and inform a broad set of organizations within your company.

Read the deployment guide

Or start contributing!

osquery> SELECT uid, name FROM listening_ports l, processes p WHERE l.pid=p.pid;
SIEM = Security Information and Event Management

SIM = Security Information Management

SEM = Security Event Management
SIEM = Security Information and Event Management

SIM = Security Information Management

SEM = Security Event Management
Handling the Flood of Security Events

- SEM designed for real-time analysis to take immediate action
- SIM is used for trend analysis and compliance reporting
WHO | WHAT | WHEN
Why Should I Monitor Non-Production?

- Do you have a shared access control between Dev & Prod?
- Same passwords keys in Dev & Prod?
- Can you 100% say you are NOT testing with Customer data in Dev?
- Are your users undertaking poor operational practices?
- Are your users evading CI/CD systems?
10:52 AM  incoming-webhook  BOT

 Threat Stack
  apt-get run with: apt-get update openssl
  Severity
    Warn (2)
  Alert Details
    View details
  Source
    Host

10:53 AM  Sam Bisbee  that's doing the upgrade i requested from them

Server
  threatstack-web01

Org
  Threat Stack Prod
<table>
<thead>
<tr>
<th>Time</th>
<th>User</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>9:15 PM</td>
<td><strong>incoming-webhook</strong></td>
<td><strong>BOT</strong></td>
</tr>
<tr>
<td>9:15 PM</td>
<td><strong>Threat Stack</strong></td>
<td>CloudTrail Activity: Route53 DNS Record Change ChangeResourceRecordSets by i-aa661331</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Critical (1)</td>
</tr>
<tr>
<td></td>
<td>Alert Details</td>
<td>View details</td>
</tr>
<tr>
<td></td>
<td>Source</td>
<td>CloudTrail</td>
</tr>
<tr>
<td>9:15 PM</td>
<td><strong>Threat Stack</strong></td>
<td>CloudTrail Activity (CreateAPICall): CreateGrant by i-aa661331</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Warn (2)</td>
</tr>
<tr>
<td></td>
<td>Alert Details</td>
<td>View details</td>
</tr>
<tr>
<td></td>
<td>Source</td>
<td>CloudTrail</td>
</tr>
<tr>
<td>9:16 PM</td>
<td>Pete Cheslock</td>
<td>that’s all from me rolling the upgraded (downsized) stats system</td>
</tr>
</tbody>
</table>
Is this you?

Yes

No
SecOps & ChatOps

Integrate your security alerts into your existing communication tools.
SEE SAY SOMETHING SOMETHING
SEE SAY SOMETHING SOMETHING
Safe Access to Production
“Every time someone logs onto a system interactively, they compromise everyone's knowledge of that system”

– Mark Burgess
Trust but Verify

- Reduce surface area by not allowing remote connections directly from the WAN (*hint* - use VPNs and Bastion hosts)
- Understand why users have to log into systems, then automate those reasons away.
  - Allow Sec Ops to contribute to Configuration Mgmt.
- Require Per-human Usernames
- Don’t rely on Security though Obscurity
Tech of the 90s

THREAT STACK

TODAYS SCALE!
Open Source Tools

• https://github.com/threatstack/ts-ldap
Open Source Tools

• https://github.com/threatstack/ts-ldap

• https://github.com/threatstack/authkeys
Open Source Tools

• https://github.com/threatstack/ts-ldap
• https://github.com/threatstack/authkeys
• https://github.com/threatstack/deputize
Start Small

Identify High Risks
The best security culture is collaborative, not prescriptive.
DevOps

Start Your Security Assessment

Audit your cloud infrastructure security in minutes.

Thank You