Forging Ahead Post Calamity

Photo: Camerist (https://noun.ly/file)

Hi,
I'm "Konst" (Konstantin) Tchernov

Consultant – Site Reliability Engineering

https://konst.kiwi/

Names, industries and identifying characteristics have been changed for privacy.

Welcome to

Incident 01: Zero-Day

Meet Sidney

“Many apps in the stamp-collecting industry are vulnerable to remote attacks.”

– *https://very-well-known-tech-news.com/*

Front page.

“Remote exploit in the StampStack Framework”

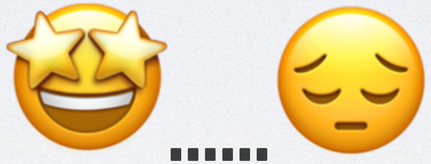
– *https://famous-security-researchers.org/*

With code samples to execute the exploit.

Silver lining: code samples.

Same-day:

Sidney identified a quick-fix that could be applied.



Problems

- Google / Apple will still flag old StampStack versions.
- Legacy apps:
  - Older StampStack framework version.
  - The apps were not as actively maintained.

Long Word documents were written.

Many PowerPoint meetings were held.

Finger pointing.

Time was counting down.

“*Skunkworks*” team.

Problem was patched before stakeholder agreement was reached.

Incident 01: the Good

- Quick initial fix.
- Skunkworks for a long-term fix.
- Upgraded StampStack to the latest version.
- Training sessions with devs.

Incident 01: the Bad

- Skunkworks for a long-term fix.
- Somewhat hushed up internally.
- Limited learning.

Incident 01: the Ugly

- Cross-team blame.
- Blaming the framework.
- Processes not fixed.
- People left.

Postmortems: learning from failure

Prevent same or similar failures.

Postmortems are blameless

Side-effects to blame

“THEY are the ones at fault.”

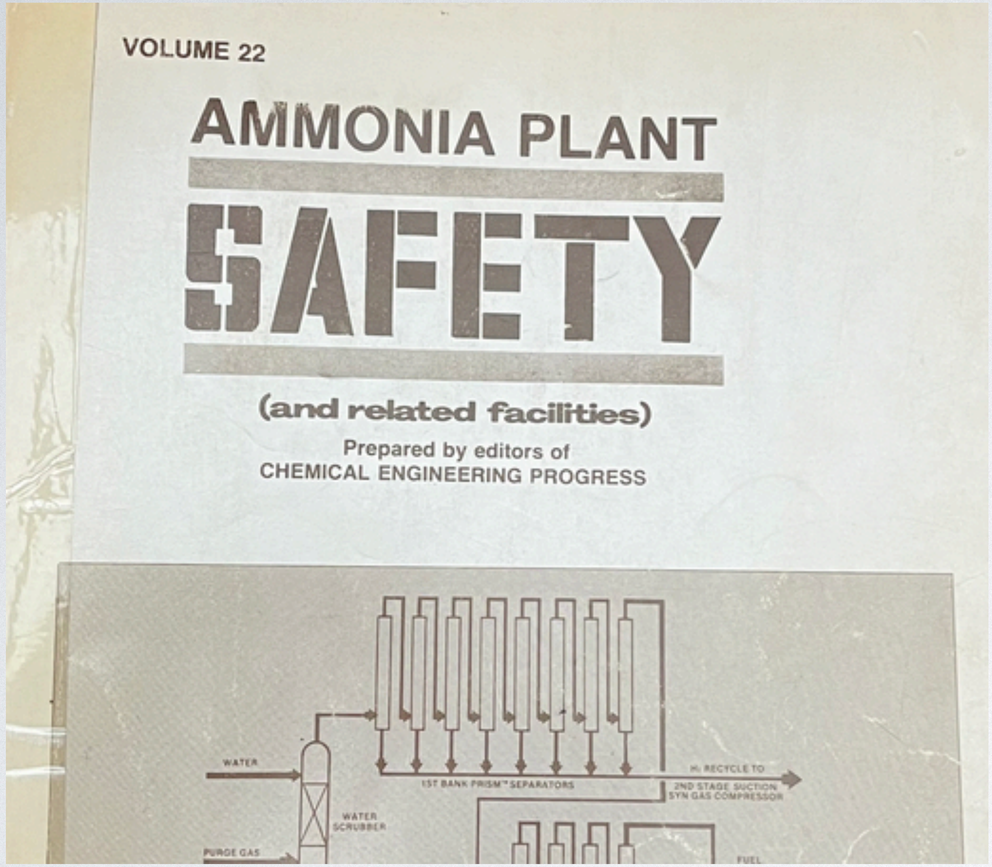
“WE warned management about this months ago.”

"Make sure it is in an email so that we cover our arses.”

Inquisitions or Witch Hunts.

General document structure:

1. Problem summary
2. Impact analysis - e.g. # of customers, duration, severity
3. Timeline of events
4. Contributing factors
5. Mitigations - action items with owners



Synthesis Start-Up Heater Failure

The fire at Monsanto's ammonia plant resulted from a rupture in one of the two synthesis start-up heater coils. The failure was caused by the localized overheating because of insufficient flow through the heater. There were no injuries to personnel.

F.G. Kokemor
Monsanto Co., Luling, La.

Credit: Kelly Shortridge (Fastly)
https://kellyshortridge.com/
https://hachyderm.io/@shortridge

Events Leading To The Failure

At approximately 4:30 p.m. on February 6, 1979, the start-up heater was lit to begin synthesis converter catalyst warm up following a unit shutdown due to a power failure. Fuel pressure to the four (4) burners was 2 psig (13.79×10^3 Pa). The start-up heater inlet and outlet valves were opened and the pressure was equalized in the synthesis loop at 900 psig (6.2053×10^6 Pa). At approximately 7:30 p.m., motor operated valves 5 and 6 were opened (Fig. 2) and firing of the start-up

Credit: Kelly Shortridge (Fastly)
https://kellyshortridge.com/
https://hachyderm.io/@shortridge

Now, what we have been finding is that the best approach to take is really the design one, and I'm sure you've gone for the correct approach on flow. I think if you consider only metallurgy, and make sure you put in stainless steel, then no matter that temperatures you reach, you should be safe.

If you depend only on well-trained operators, you may fail. I think you really must depend on the design approach and don't depend much at all on the operation.

You also said you had temperature trips checked two weeks previously, but you didn't mention them again. Presumably that evidence was destroyed in the fire?

Credit: Kelly Shortridge (Fastly)
https://kellyshortridge.com/
https://hachyderm.io/@shortridge

~~root cause~~

“Saying that a system suffered an outage because of a bug is like saying that a person died because of a cut.”

– Dr. Lorin Hochestein (Netflix)
https://hachyderm.io/@norootcause

Welcome to

Meditation on Steroids.

Incident 02: Russian Hacker

“I have your customer details.
My Bitcoin wallet is open for donations.”

– Vladimir from Russia

Emailing as: ceos.name@zeni.ly

Stabilise first.

Stabilise:

1. Confirm the problem.
2. Block the exploit — quick fix.
3. Fix email config.
4. Look for similar bugs in the API.

Days after:

1. Looked through ***access logs*** for:
    A. Scope of the breached data.
    B. Signs of similar behaviour going back 6 months.
2. *New* PEN testing company to do a targeted test.
3. Scheduled a postmortem.

Postmortem

How did this happen?

Junior Jeff

Senior Anna

BUG written → Peer Review (PR) → Demo

Demo → Manual tests → Automated tests → Regular PEN Test

Regular PEN Test → Web Application Firewall (WAF) → Monitoring & Alerting

How did this happen?

Lack of ~~experience~~ support.

Lack of standard patterns.

Rushed? Did not think of security?

No security training

BUG written

Peer Review (PR)

No critical review

Demo

Regular PEN Test

Automated tests

Manual tests

Don't cover security

Only automated scanning? Limited time paid for?

Web Application Firewall (WAF)

Monitoring & Alerting

Tuned to avoid false positives?

Not security focused?

“SHIP SHIP. SHIP.  ”

– The Boss

Example Mitigations:

- Cover security in automated tests.
- Security training for devs and testers.
- More sophisticated WAF🔥🧱 rules.
- Audit trail + alerts for admin tasks.
- Call out time pressure to execs.

Share the postmortems.

What next?

What about your team?

Has the team stabilised?

Devs will focus on tech mitigations.

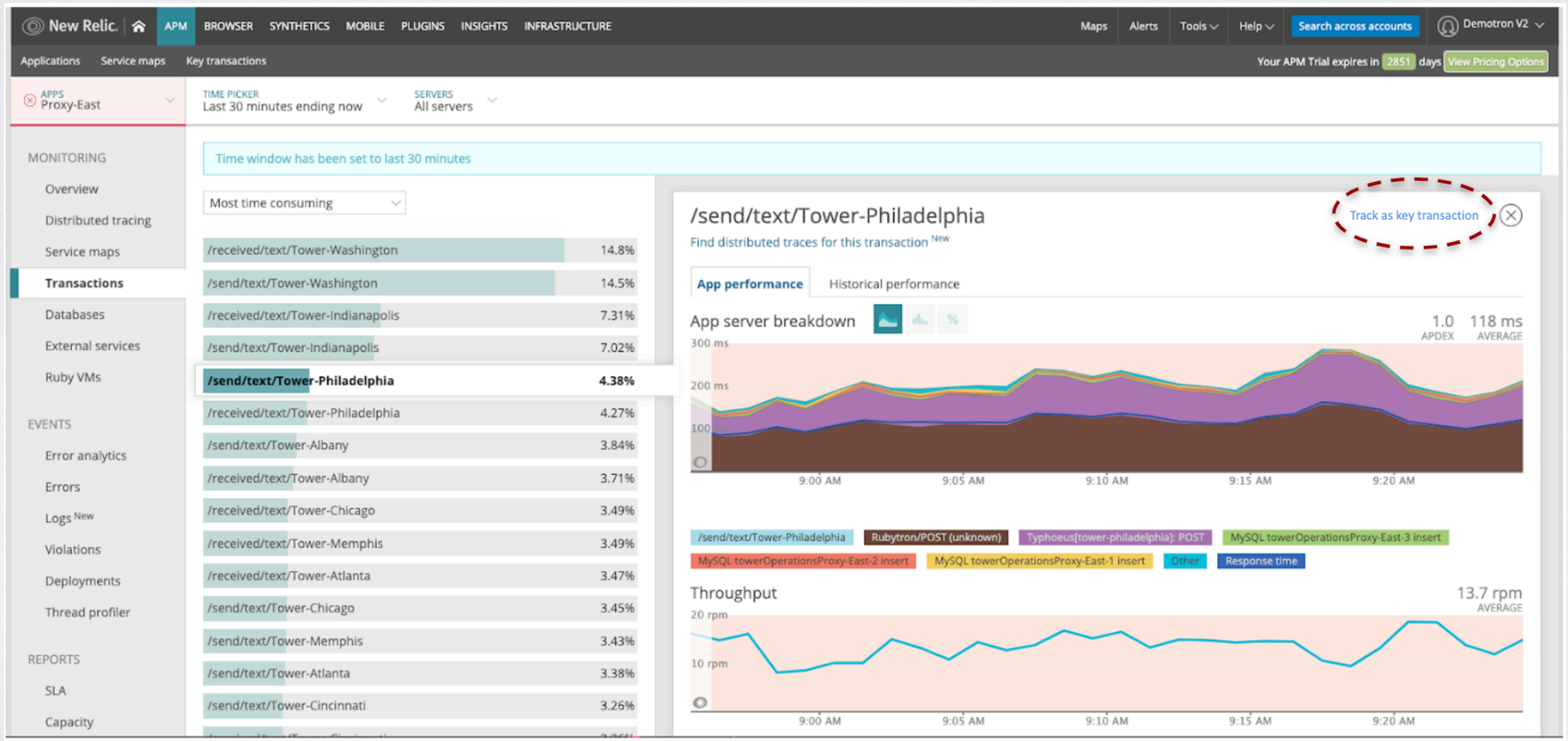
The “lone developer” is outdated.

https://noun.ly/owl

Make the team around you better.

Shared learning

Run through troubleshooting or postmortem research steps together.



Mob Session – OWASP Juice Shop

Check in on people

Grab a ☕ / 🧋 / 🍩

Or virtual version

Prevent operator error, but don’t forget the operators.

Post mortem structure and examples:

1. Google SRE Workbook – Postmortem Culture: Learning from Failure – https://noun.ly/sleet

2. Atlassian Postmortem template – https://noun.ly/rise

3. AWS re:Invent 2022 – Handling Log4Shell – https://noun.ly/watch

Comments or Questions?

Konstantin “Konst” Tchernov

https://konst.kiwi/

Slides: https://noun.ly/slash