Algorithms vs Hackers

Göran Sandahl, CTO and Co-founder Unomaly.

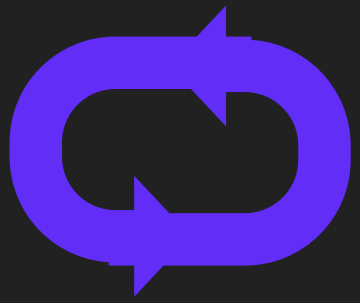
unomaly

Background

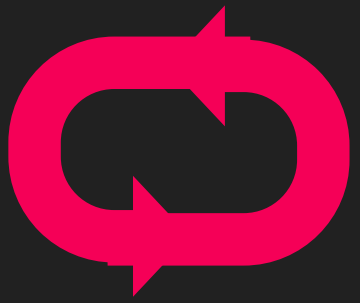
This slide deck was used in a presentation held at SUSEC on Oct 19 2017. Invited by Niklas Niktin @ Karlstads Universitet, currently users of Unomaly.

unomaly + 

Us



Our systems



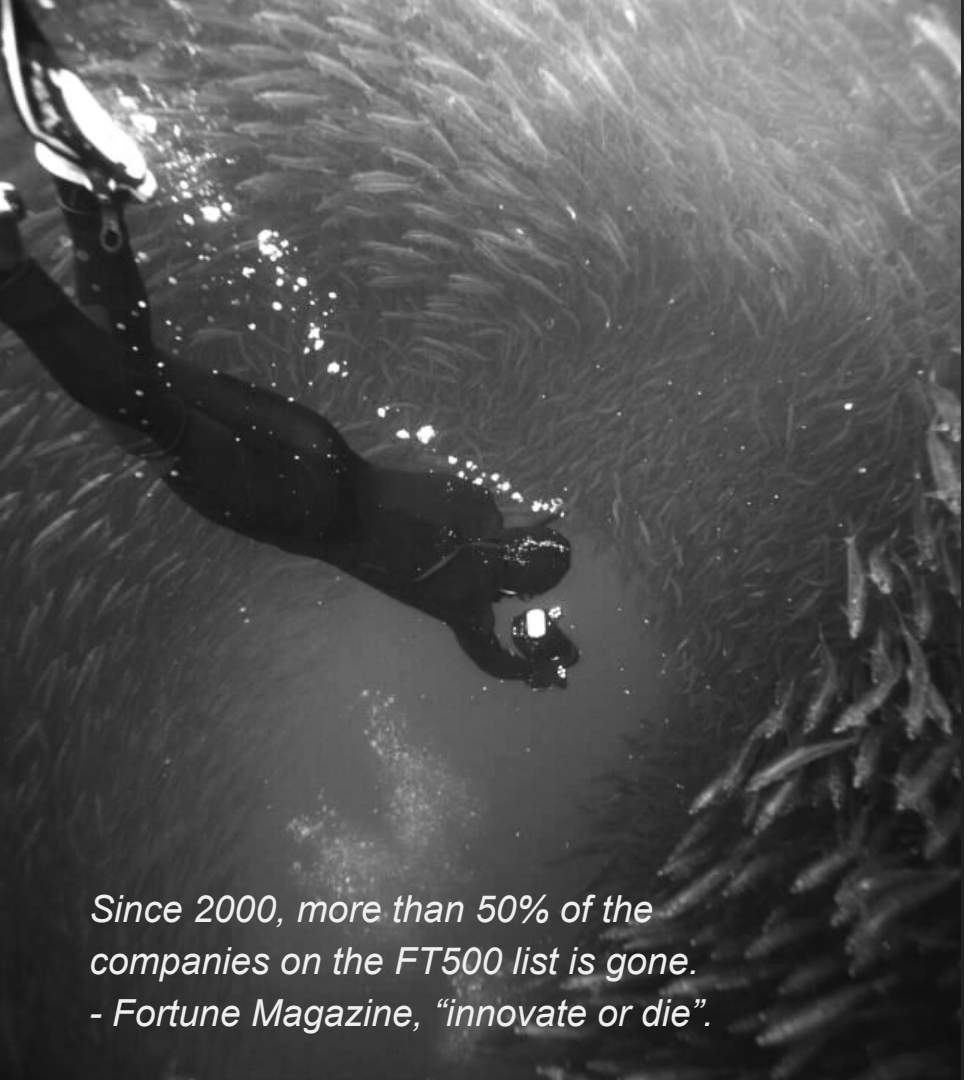
Hackers

The digital transformation

Physical **Software**

Data poor → Data rich → Data driven

Data? Big data Machine intelligence



The transformation is brutal...

8/10 digital transformation projects fails. 90% of all big data initiatives doesn’t return its money.

Struggle to maintain high availability

40% of all incidents have unknown root causes, 20% of organizational time spent on troubleshooting,

Slow rate of change due to bureaucracy

R&D spending all time high, but little correlation between spending and results.

Breaches are all time high

67% of all incidents remains undetected until third party detect, after 7 weeks.

Increasing compliance pressure

GDPR, ISO27001, PCI etc.

Winners are enormously successful.

“Netflix has used analytics to position itself as the clear leader of the pack. It has done this by constantly evolving their use of data.”

14 x more changes
8 times more projects, 6 times more applications, ⅓ of unplanned work.

1/2 of failure rate and 10x faster fixes to severe incidents

⅓ of audit preparation effort and fewest number of repeat audit findings

5 x more likely to detect a breach
and 5 times less likely for breach to result in loss.

https://puppet.com/resources/whitepaper/state-of-devops-report

What’s the difference?

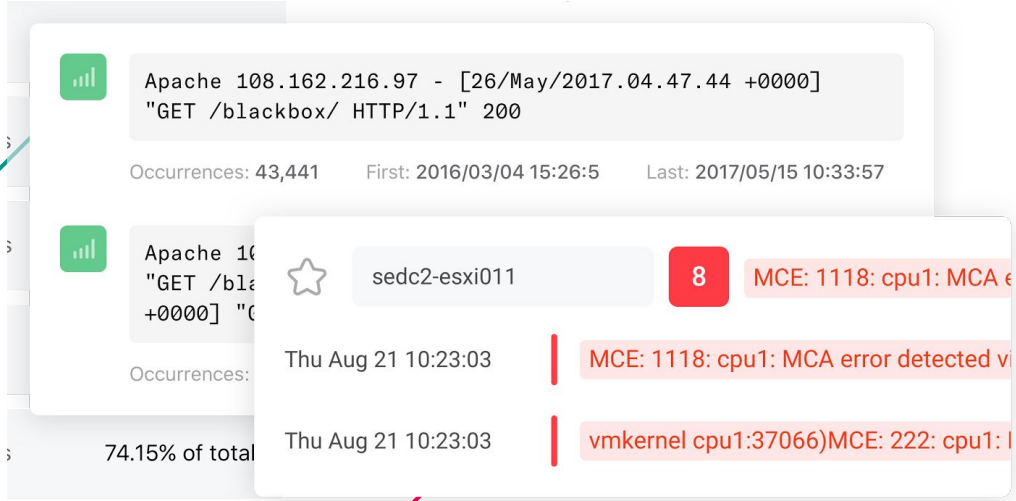
	The old team	The new team
Believes in	Past experience, rules.	Future developments, data.
Approach to data	**Use data to answer questions.**	**Use data to question answers.**
Acts when	Something is defined as important.	Something is different, new, unknown.
Controls risk by	Implementing controls and policies.	Detects, responds and changes.
Gets good at	Fighting fires, running projects	Learning, acting, changing.
Organized as	Separation by duty, siloed expertise.	Autonomous, cross-functional teams
Leadership	**Technology averse.**	**Technology adoptive.**

An algorithmic definition of relevance.

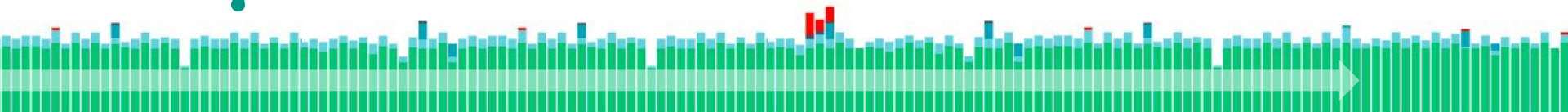
Go from “known to be bad” to “progressively interesting”.

1. All data, in favor of “important data”
2. Systematic analysis, in favor of expert analysis
3. Unbiased and raw, in favor of pretty and easy to understand.
4. Value now, in favor of value later.

Machine learning acts as a memory of everything

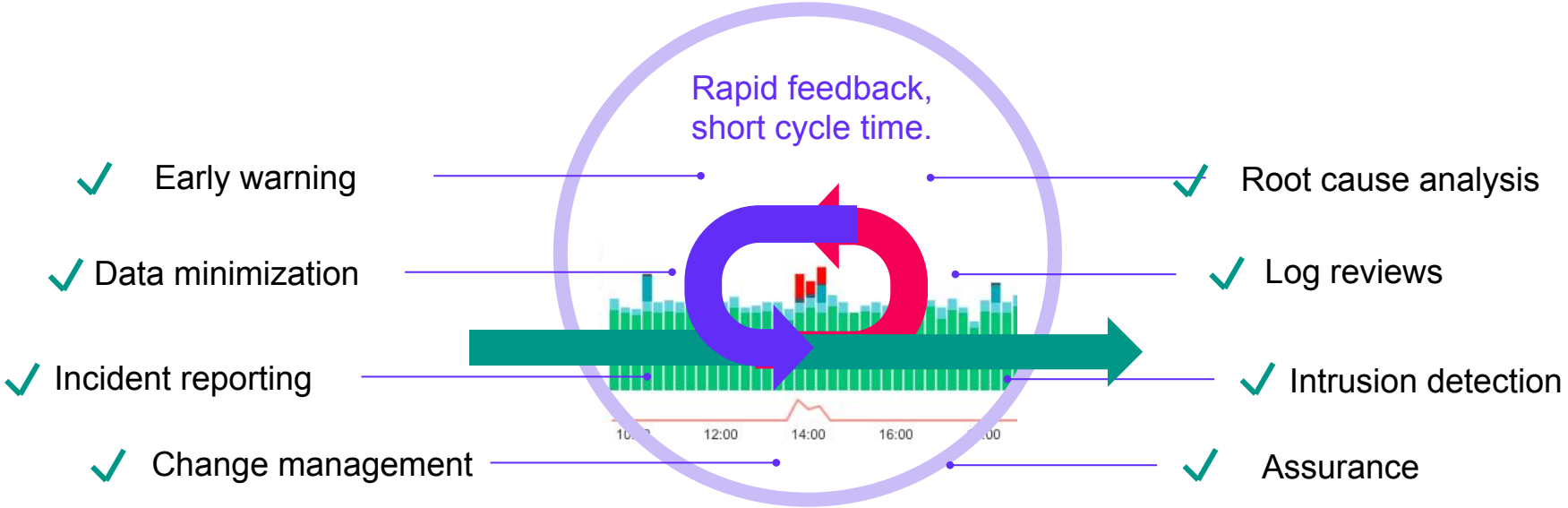


Anomaly detection acts as a realtime news feed



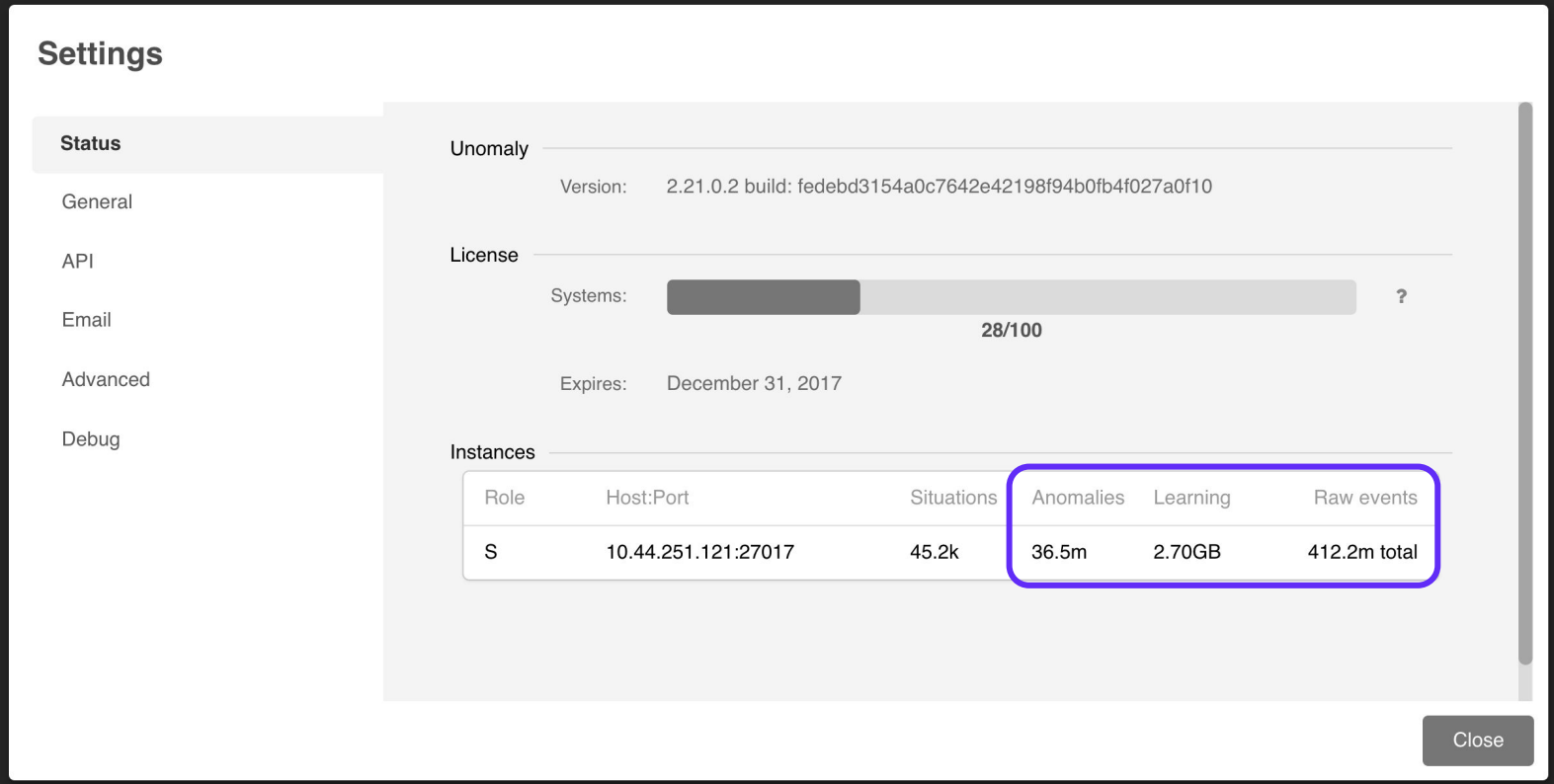
How an organization can work

Autonomously act on continuous, small and timely insights. Work in in small iterations, pulls resources as needed.



Examples

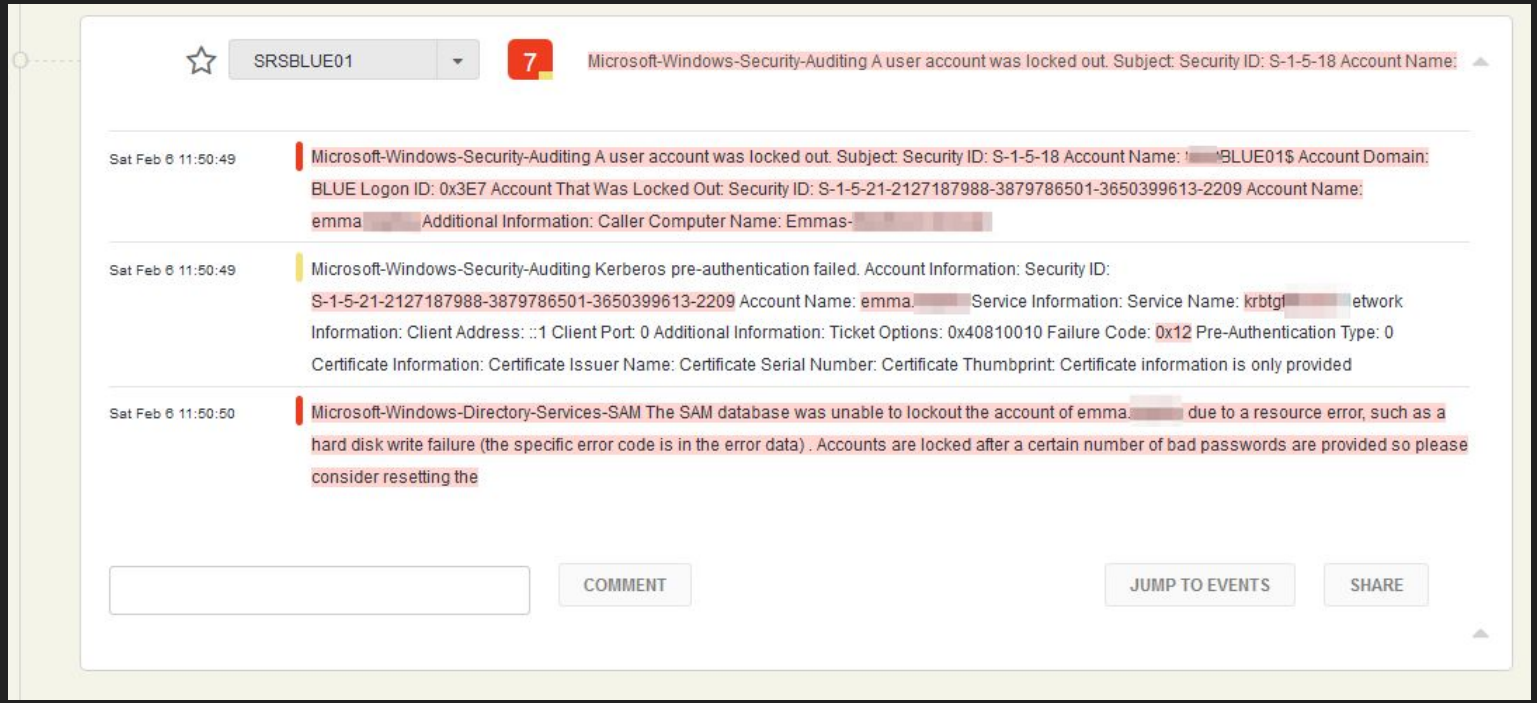
Data minimization



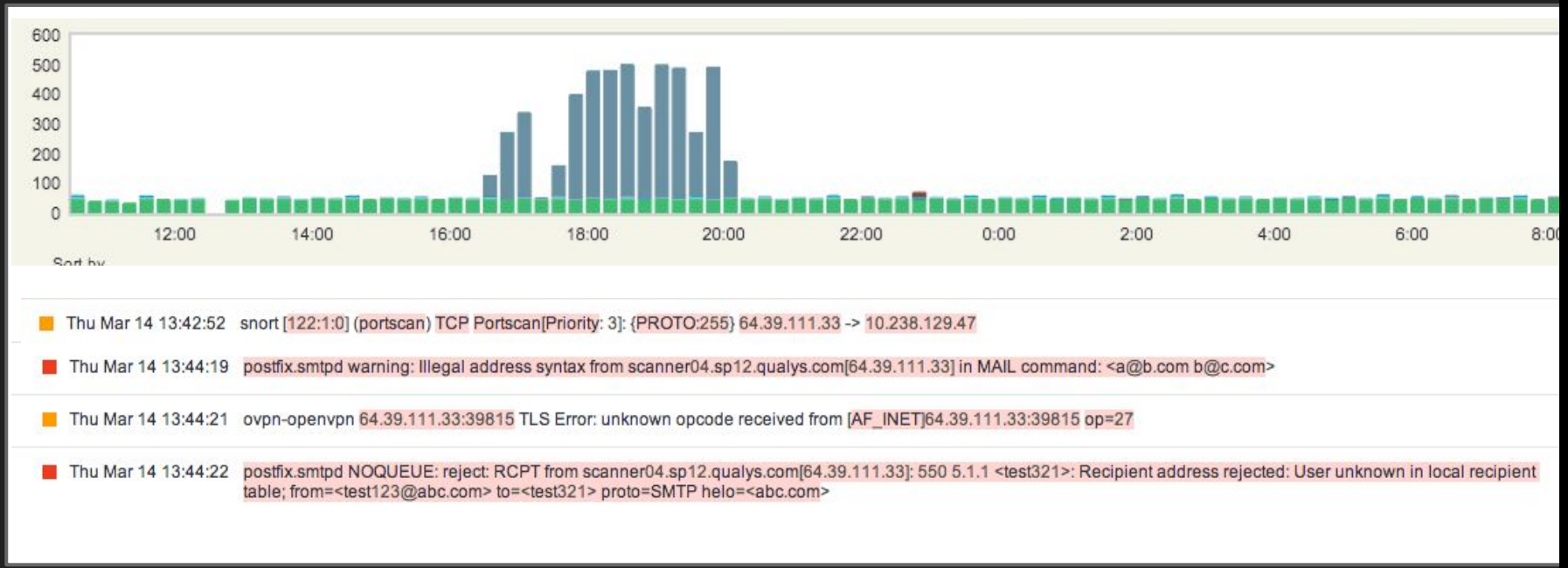
Early warning

Intrusion detection

Investigations



Testing


600
500
400
300
200
100
0
12:00
14:00
16:00
18:00
20:00
22:00
0:00
2:00
4:00
6:00
Thu Mar 14 13:42:52 snort [122:1:0] (portscan) TCP Portscan[Priority: 3]: {PROTO:255} 64.39.111.33 -> 10.238.129.47
Thu Mar 14 13:44:19 postfix.smtpd warning: Illegal address syntax from scanner04.sp12.qualys.com[64.39.111.33] in MAIL command: <a@b.com b@c.com>
Thu Mar 14 13:44:21 ovpn-openvpn 64.39.111.33:39815 TLS Error: unknown opcode received from [AF_INET]64.39.111.33:39815 op=27
Thu Mar 14 13:44:22 postfix.smtpd NOQUEUE: reject: RCPT from scanner04.sp12.qualys.com[64.39.111.33]: 550 5.1.1 <test321>: Recipient address rejected: User unknown in local recipient table; from=<test123@abc.com> to=<test321> proto=SMTP helo=<abc.com>

Summary

- Normally, organizations are distanced their systems while hackers are not.
- Algorithms provides a new interface to systems and their data.
- Operating by small signals (vs large signals) is transformative to a team.
- A lot of the work we normally do can be done differently, simpler, sometimes even automatically “as we go”.
- It’s a focus on technology, people, process.

- If interested to learn more
  - Email goran@unomaly.com
  - Or go to unomaly.com, Get started.

Demo

Test Unomaly for 30 days

- 1 hour installation and 2 hours data integration.
- Algorithmically analyze 100% data from a platform.
- Light training and workflow session for one team.
- Presentation of findings in a report:
  - Issues that today go undetected, but should be monitored in the future.
  - What your systems are actually doing, and where you have existing issues.
  - Proof that incidents creates anomalies and that it will, universally, speed up root cause analysis.
  - How little that is required by your organisation to get this important capability.

Example report