

# Algorithms vs Hackers

Göran Sandahl, CTO and Co-founder Unomaly.



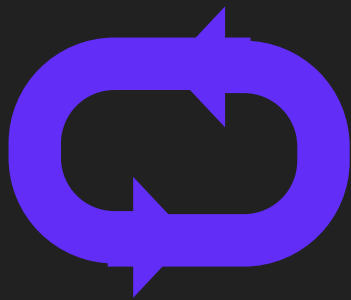
# Background

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



Data?

Big data

Machine intelligence



*Since 2000, more than 50% of the companies on the FT500 list is gone.  
- Fortune Magazine, "innovate or die".*

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,  $\frac{1}{3}$  of unplanned work.

**$\frac{1}{2}$  of failure rate and  
10x faster fixes to  
severe incidents**

**$\frac{1}{3}$  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.**



# What's the difference?

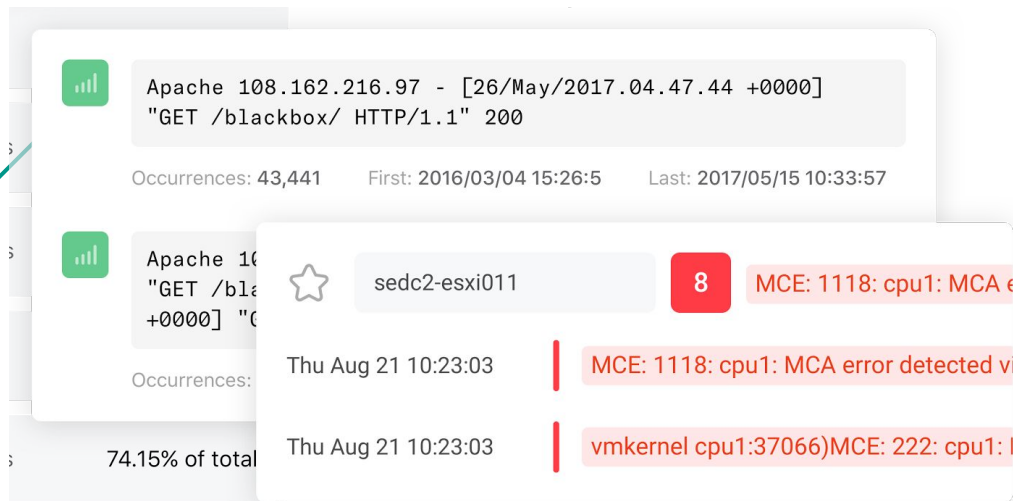
|                         | The old team                          | The new team                          |
|-------------------------|---------------------------------------|---------------------------------------|
| Believes in             | Past experience, rules.               | Future developments, data.            |
| <b>Approach to data</b> | <b>Use data to answer questions.</b>  | <b>Use data to question answers.</b>  |
| 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    |
| <b>Leadership</b>       | <b>Technology averse.</b>             | <b>Technology adoptive.</b>           |

# 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

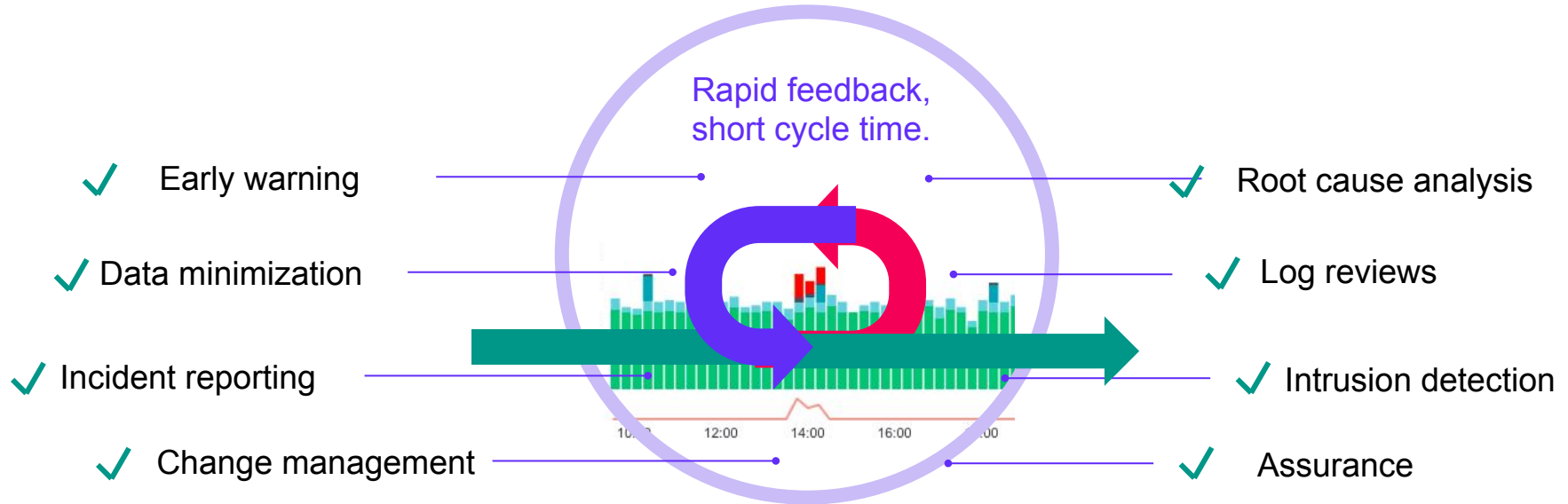


Anomaly detection acts as a realtime news feed



# How an organization can work

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



# Examples

# Data minimization

## Settings

### Status

General

API

Email

Advanced

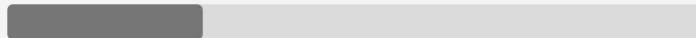
Debug

### Unomaly

Version: 2.21.0.2 build: fedebd3154a0c7642e42198f94b0fb4f027a0f10

### License

Systems:



28/100

?

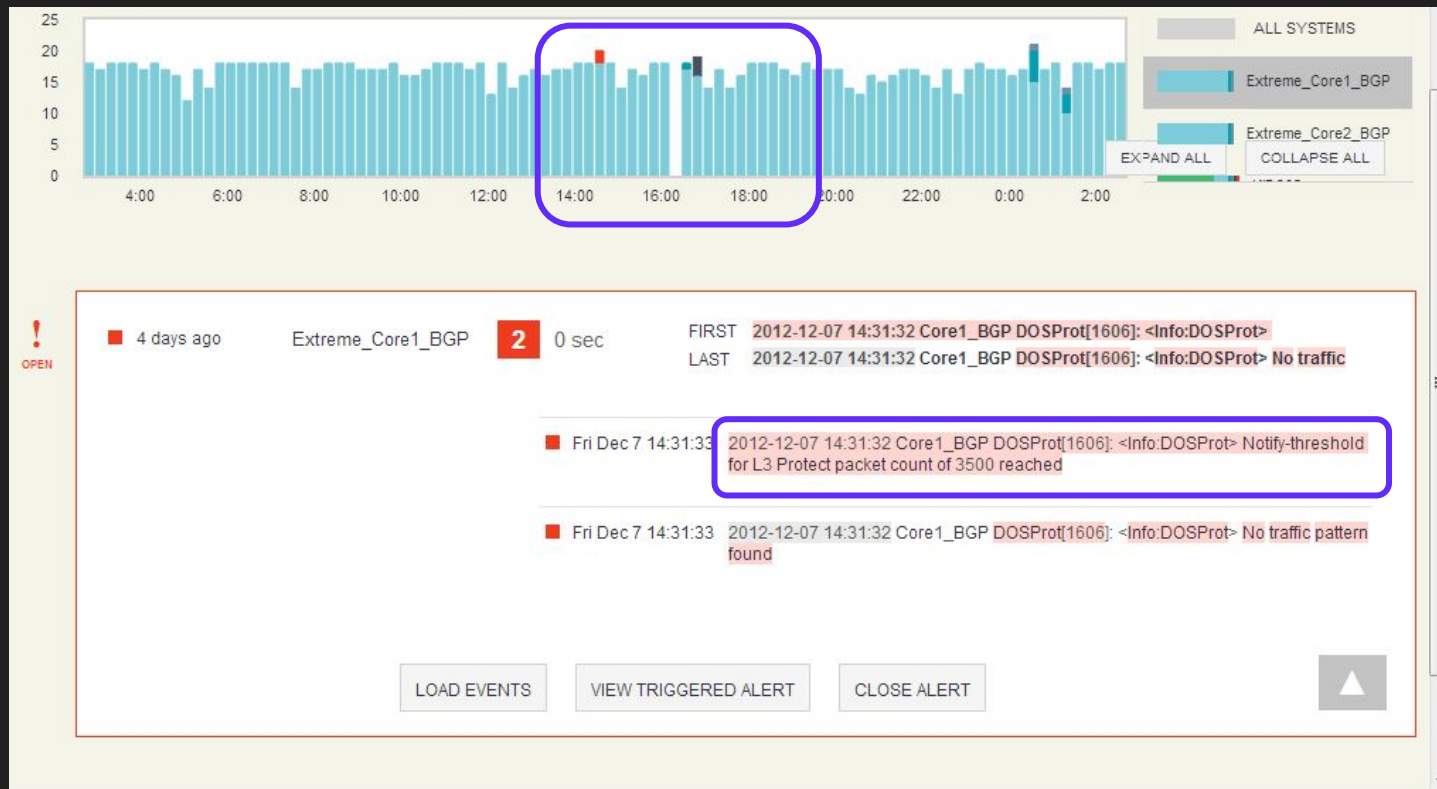
Expires: December 31, 2017

### Instances

| Role | Host:Port           | Situations | Anomalies | Learning | Raw events   |
|------|---------------------|------------|-----------|----------|--------------|
| S    | 10.44.251.121:27017 | 45.2k      | 36.5m     | 2.70GB   | 412.2m total |

Close



# Early warning





# Intrusion detection

|                    |   |
|--------------------|---|
| Mon Jun 27 4:34:18 | sshd input_userauth_request: invalid user rwa [preauth]                       |
| Mon Jun 27 4:34:18 | kernel [86129010.233243] RPC: fragment too large: 0x00430100                  |
| Mon Jun 27 4:34:20 | sshd Failed password for invalid user rwa from 38.132.117.108 port 35308 ssh2 |
| Mon Jun 27 4:34:22 | kernel [86129014.261332] RPC: fragment too large: 0x56818106                  |



# Investigations

 SRSBLUE01 

 Microsoft-Windows-Security-Auditing A user account was locked out. Subject: Security ID: S-1-5-18 Account Name: 


---

Sat Feb 6 11:50:49

 Microsoft-Windows-Security-Auditing A user account was locked out. Subject: Security ID: S-1-5-18 Account Name: 'SRSBLUE01\$ Account Domain: BLUE Logon ID: 0x3E7 Account That Was Locked Out: Security ID: S-1-5-21-2127187988-3879786501-3650399613-2209 Account Name: emma Additional Information: Caller Computer Name: Emmas-


---

Sat Feb 6 11:50:49

 Microsoft-Windows-Security-Auditing Kerberos pre-authentication failed. Account Information: Security ID: S-1-5-21-2127187988-3879786501-3650399613-2209 Account Name: emma Service Information: Service Name: krbtgt network Information: Client Address: ::1 Client Port: 0 Additional Information: Ticket Options: 0x40810010 Failure Code: 0x12 Pre-Authentication Type: 0 Certificate Information: Certificate Issuer Name: Certificate Serial Number: Certificate Thumbprint: Certificate information is only provided

---

Sat Feb 6 11:50:50

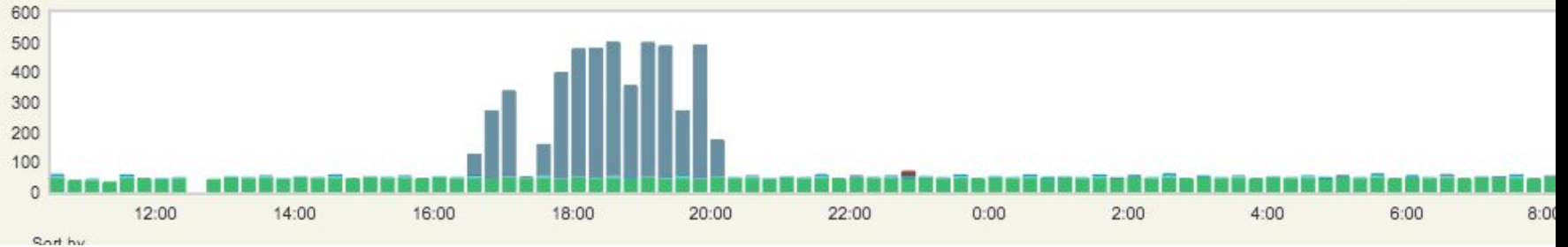
 Microsoft-Windows-Directory-Services-SAM The SAM database was unable to lockout the account of emma due to a resource error, such as a hard disk write failure (the specific error code is in the error data). Accounts are locked after a certain number of bad passwords are provided so please consider resetting the

COMMENT

JUMP TO EVENTS

SHARE

# Testing



- 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](mailto:goran@unomaly.com)
    - Or go to [unomaly.com](https://unomaly.com), Get started.



Demo

unomaly

# 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



unomaly

## Executive summary

Unomaly analyzed more than 4.1 billion events during 2 months and reduced the data with 99,99999%. It uncovered significant unknown issues existing in the infrastructure.

## Issues

- I/O problems in storage area.
- Critical failures in routers.
- Fatal errors on hardware.
- Manipulation attempts.



apollo

Dustin

