Protecting $1 Trillion Everyday

How the Bank of England has evolved from a reactive to a proactive SOC

Jonathan Pagett | Bank of England

October 2018 | Version 1.0

JONATHAN PAGETT

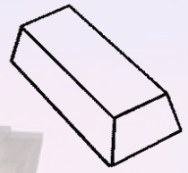
Security Operations Centre
Bank of England

splunk> .conf18

Who are the Bank of England?

Founded 1694

splunk> .conf18



Gold reserves

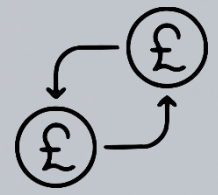
Monetary stability

Financial stability

Print banknotes

Run payments services

Provide “risk free” banking services



Payments

Analytics

Cyber

Technology that sits at the heart of the UK financial sector

Bank of England

in numbers….

$1T

Daily payments

1/3

UK GDP everyday

4,000

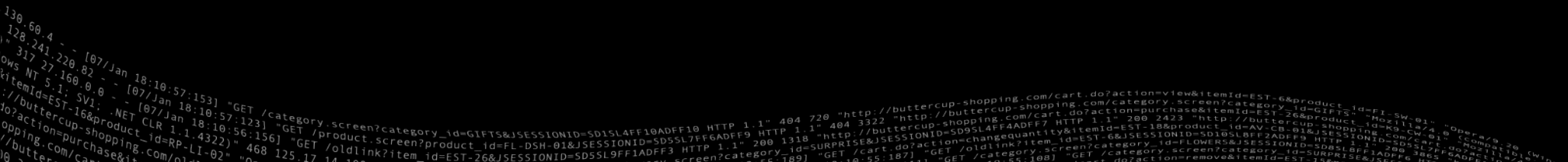
Staff

10,000

Endpoints

8

SOC staff



Detect and respond to cyber-attacks against the Bank of England

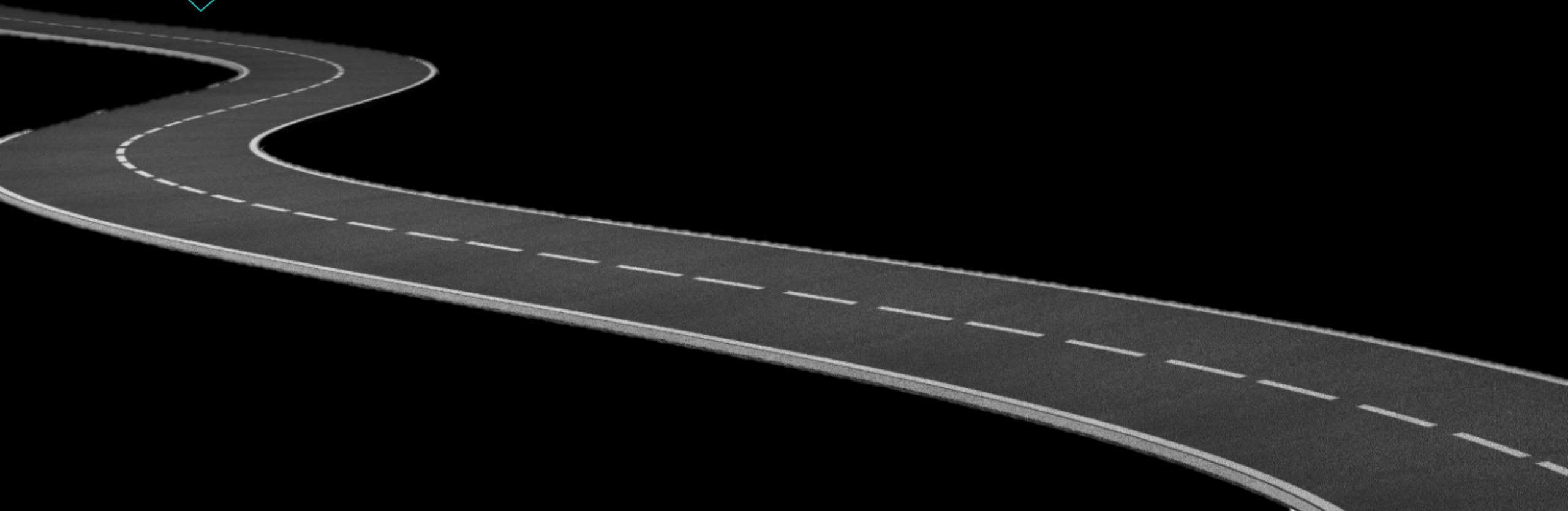
splunk> .conf18

The Journey

Where was the SOC in 2015?

2015 - reactive

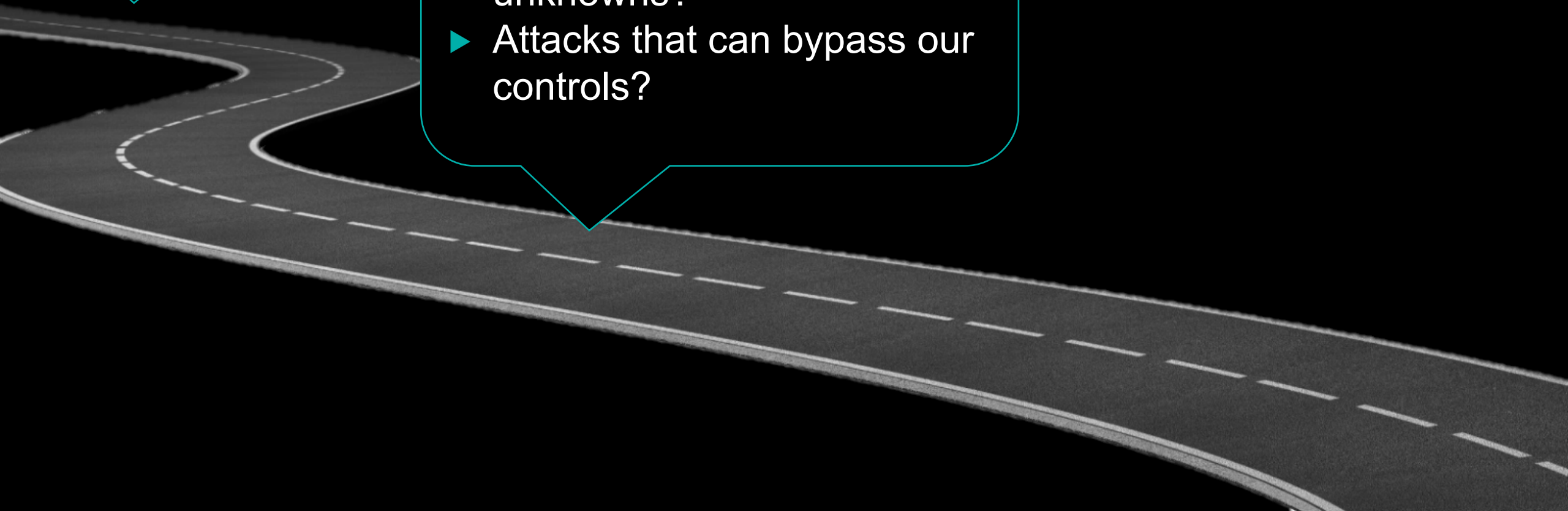
- Reactive to known threats
- Reliant on our security controls to detect attacks



The Need for Change

2015 - reactive

- Reactive to known threats
- Reliant on our security controls to detect attacks



2016 - proactive

- What about the known unknowns?
- Attacks that can bypass our controls?

Operating Model First – Technology Second

2015 - reactive

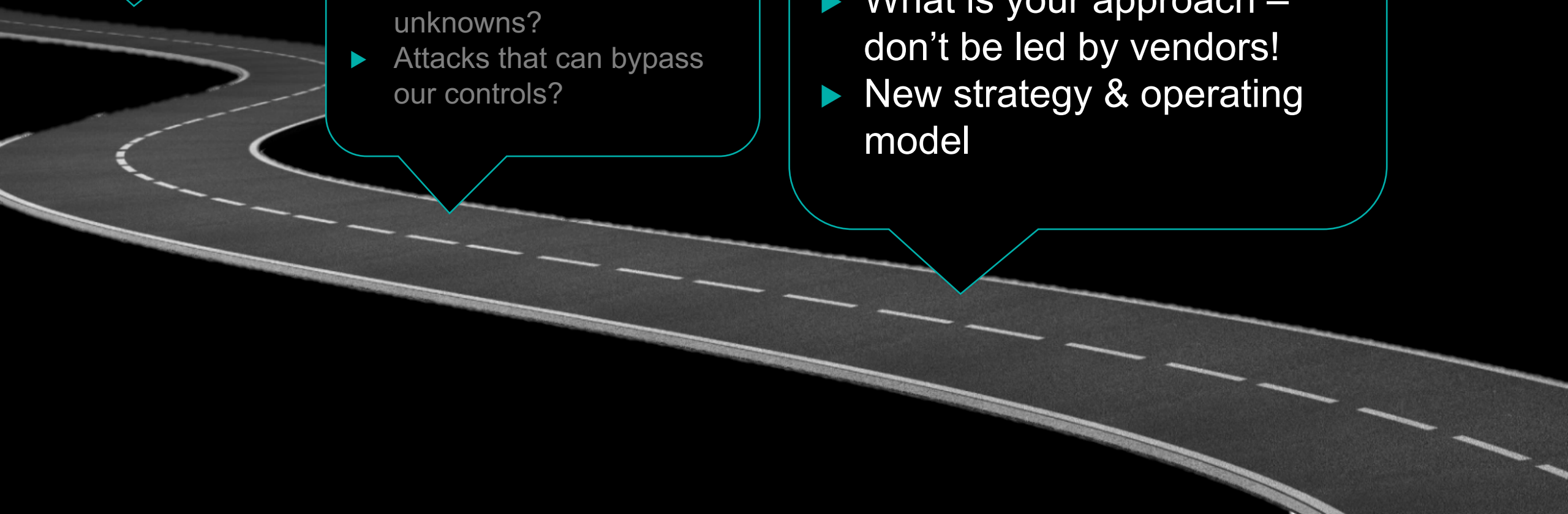
- Reactive to known threats
- Reliant on our security controls to detect attacks

2016 - proactive

- What about the known unknowns?
- Attacks that can bypass our controls?

2016

- What are we doing again?
- What is your approach – don't be led by vendors!
- New strategy & operating model



The Strategy

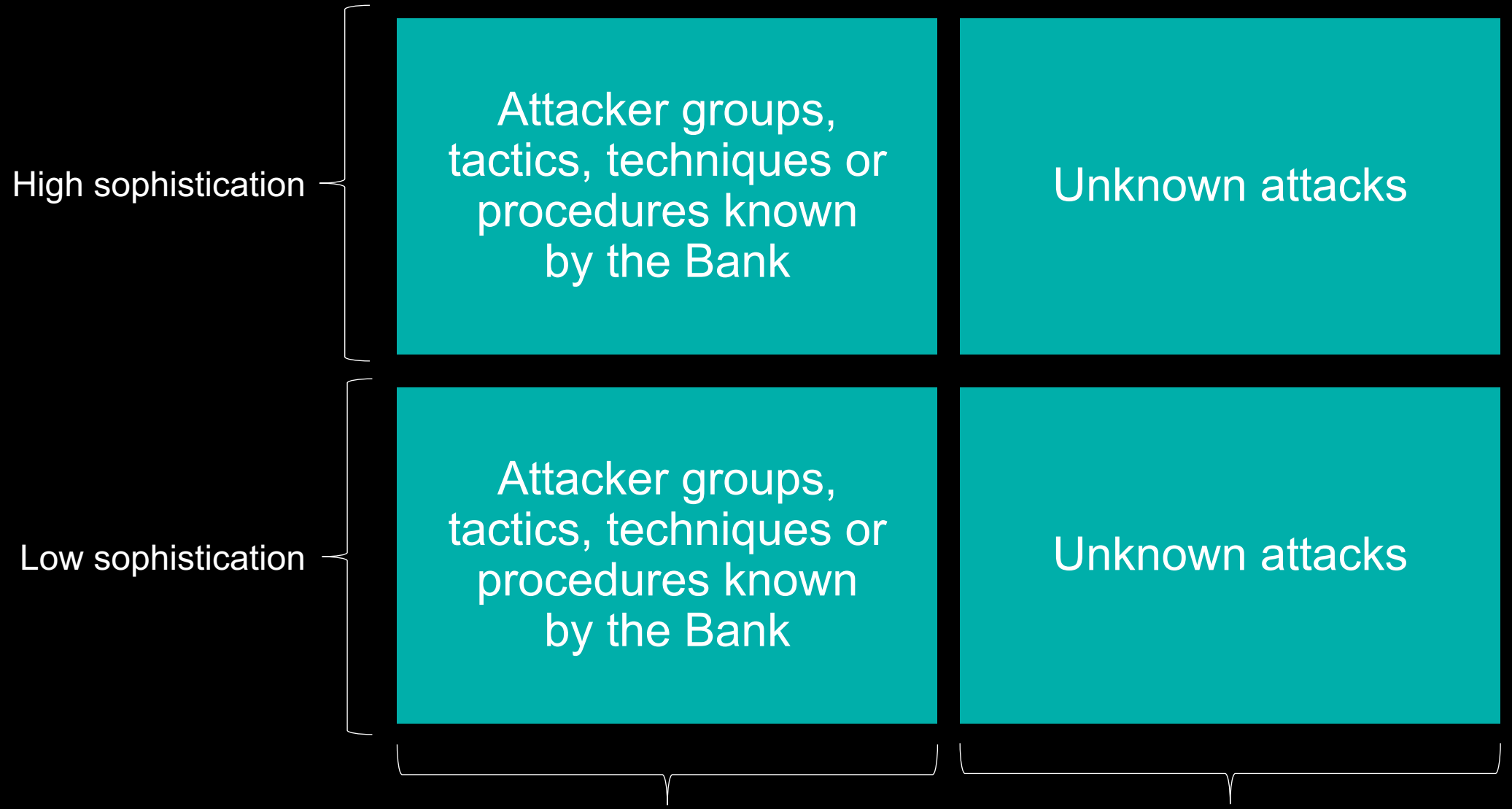
Bank of England Monitoring Strategy

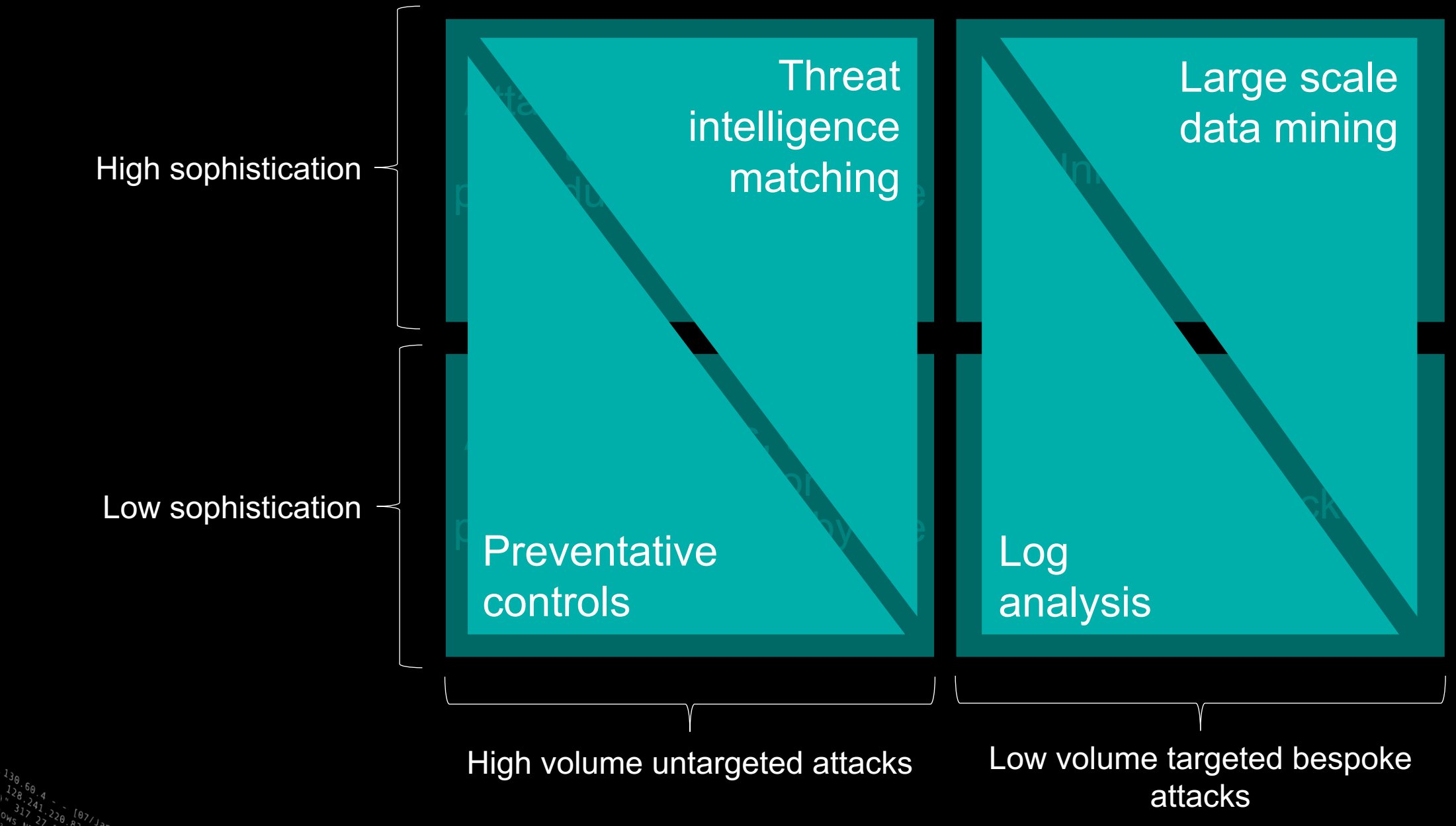
Our approach

Attacker groups, tactics, techniques or procedures known by the Bank

Unknown attacks

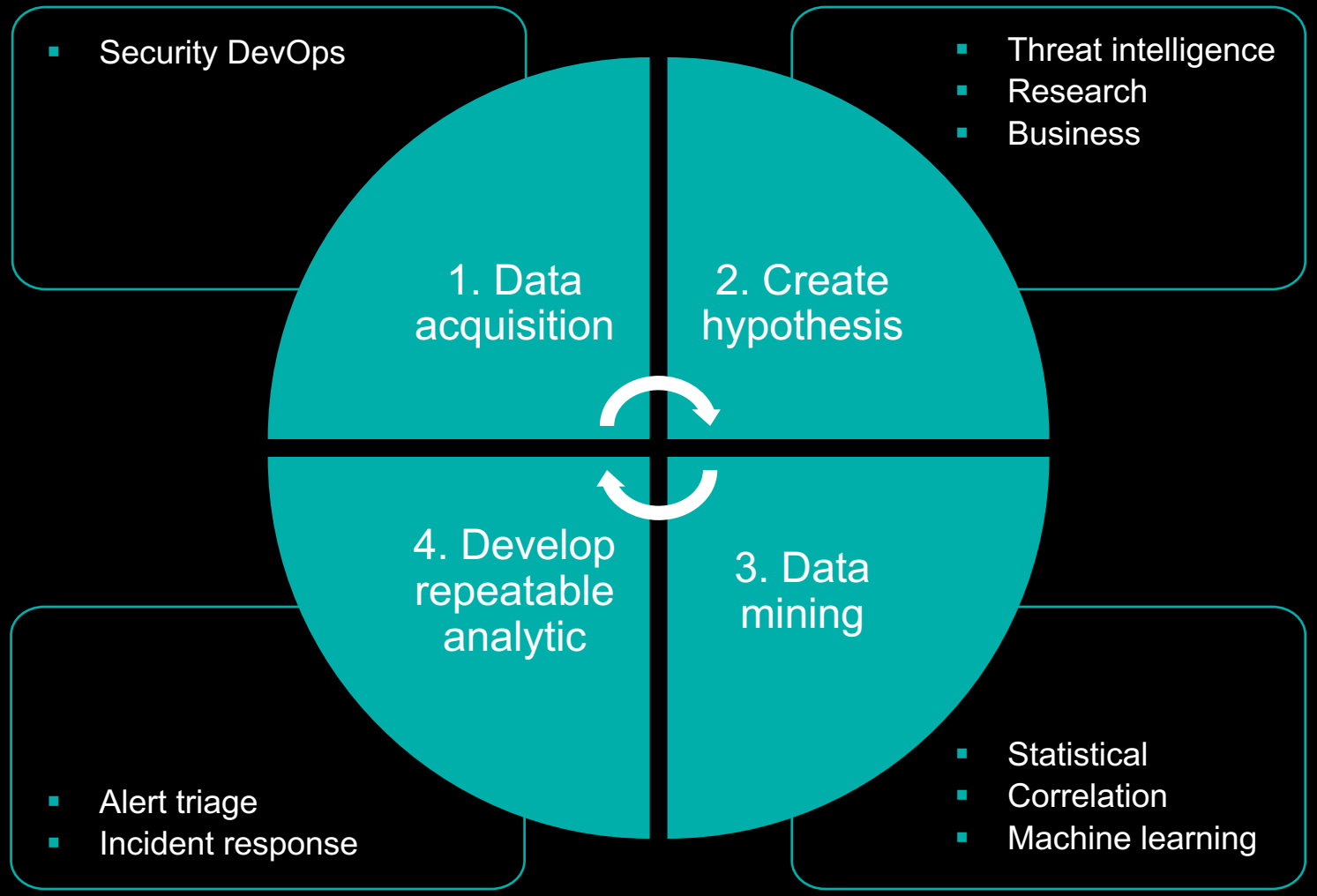
splunk> .conf18





The Operating Model

- Research and intelligence based
- Continual improvement at heart
- Data and adversary led
- 273 analytics developed
- Supported by team structure



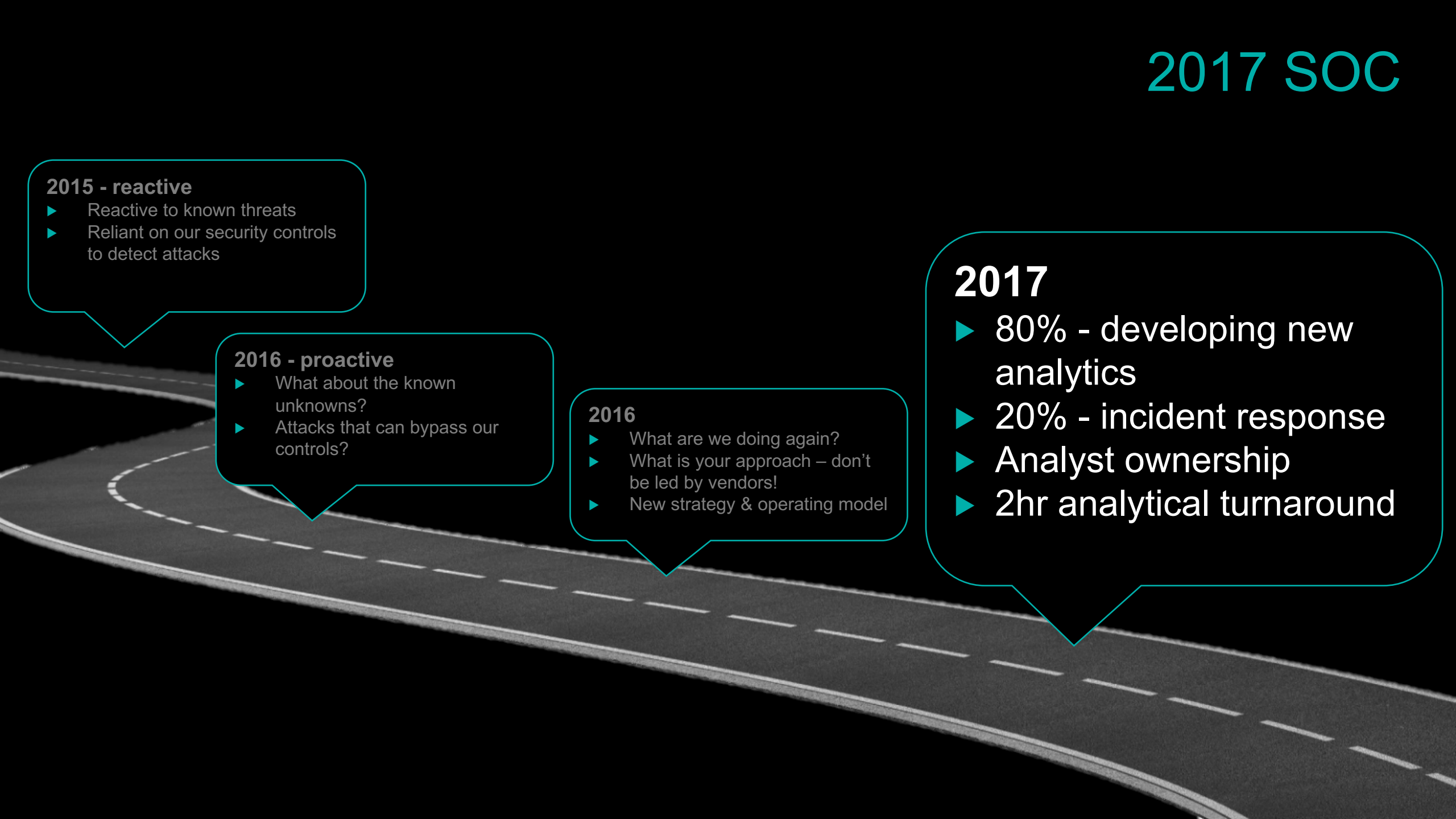
Splunk and our Operating Model

Why we chose Splunk – our top 3

- Fast iterative search development – test hypothesis and get instant results
- Wide range of functions within SPL (Mathematical, time, statistical, text etc.)
- I want to employ security skills, not system engineers

splunk> .conf18

2017 SOC



2015 - reactive

- Reactive to known threats
- Reliant on our security controls to detect attacks

2016 - proactive

- What about the known unknowns?
- Attacks that can bypass our controls?

2016

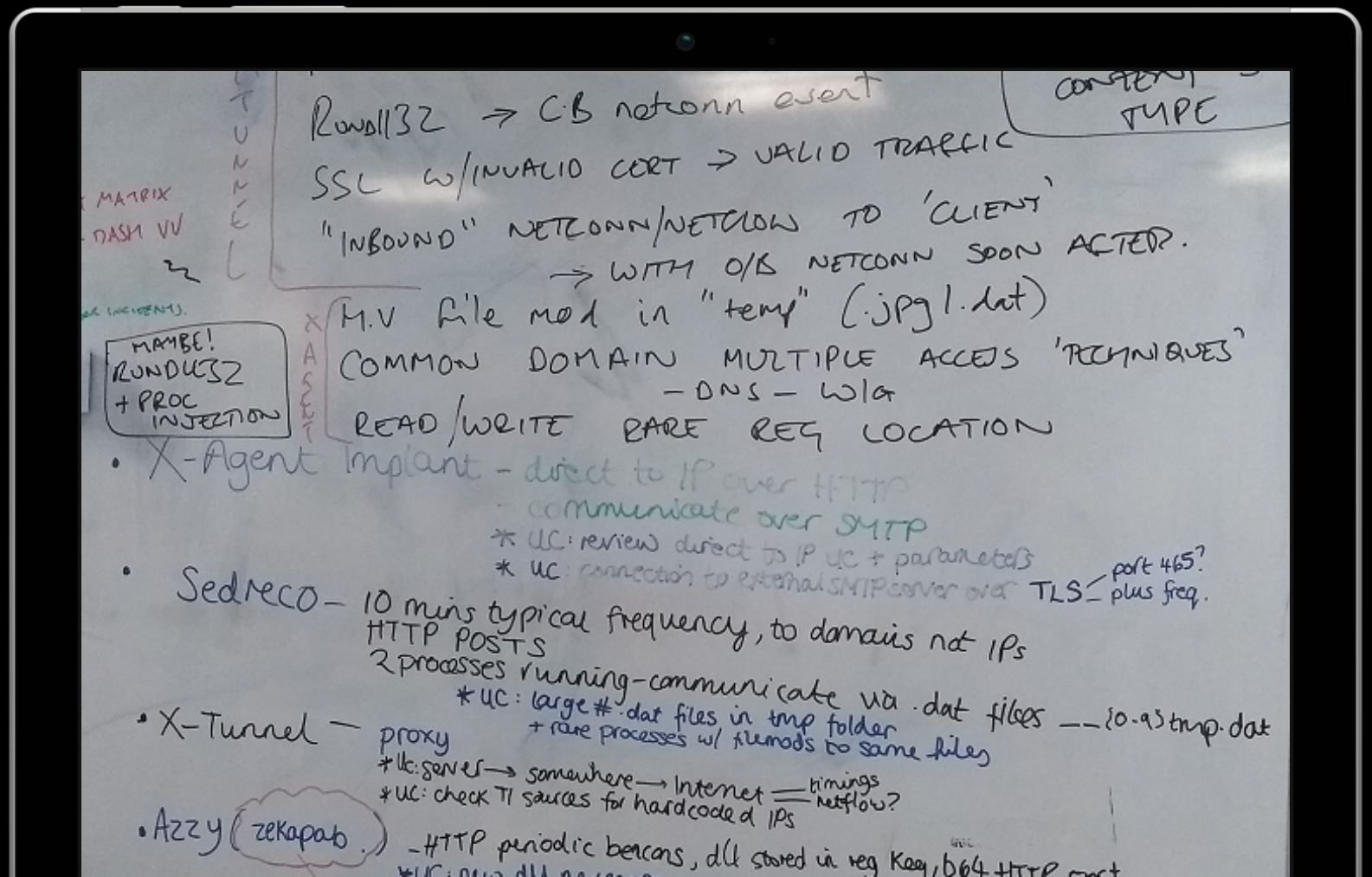
- What are we doing again?
- What is your approach – don't be led by vendors!
- New strategy & operating model

2017

- 80% - developing new analytics
- 20% - incident response
- Analyst ownership
- 2hr analytical turnaround

How We Approach Developing Analytics

Hackathons



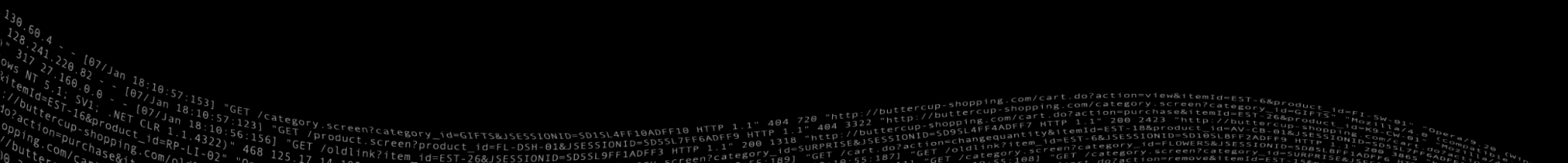
- **adversary** focused
- **data** focused
- **system** focused

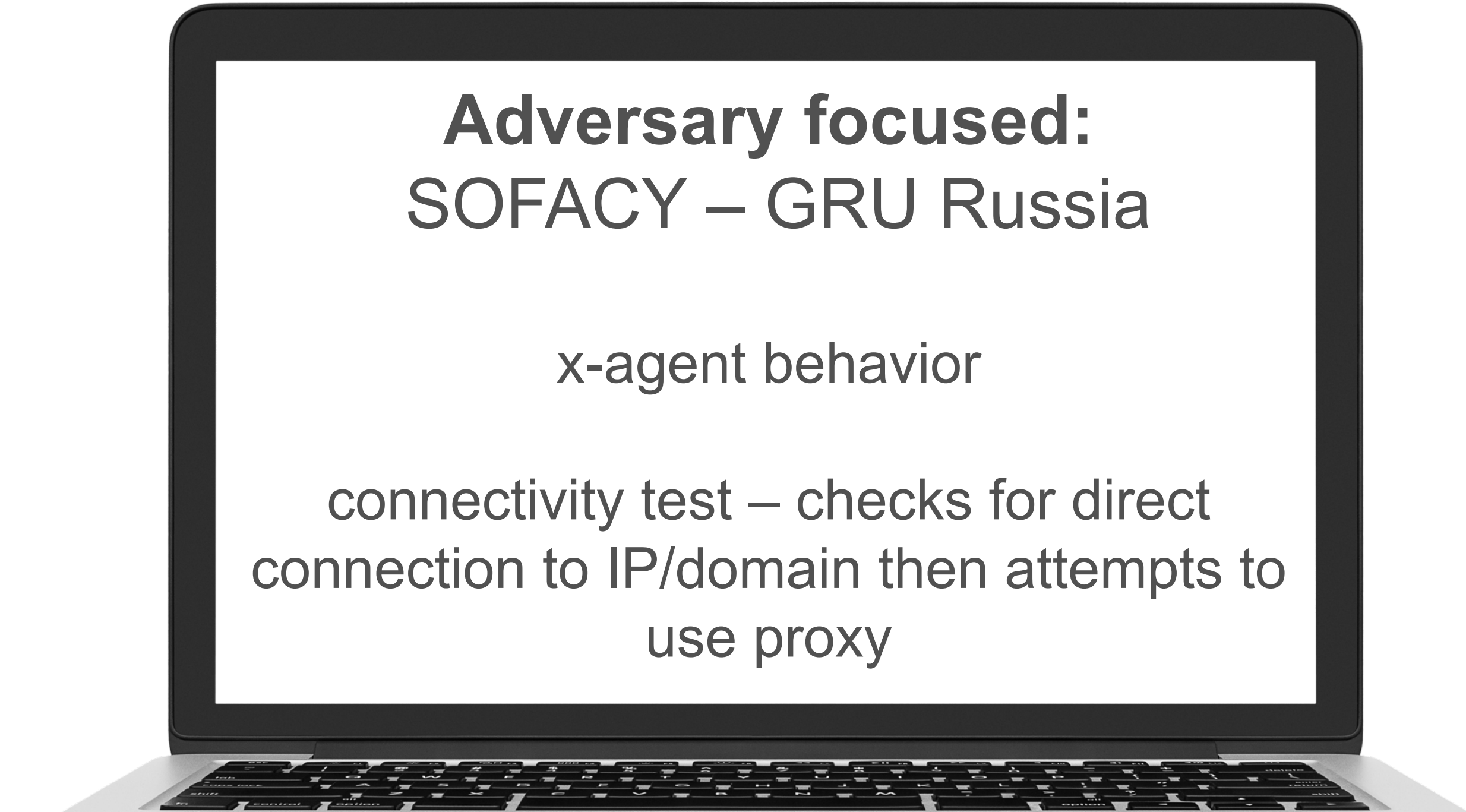
splunk> .conf18

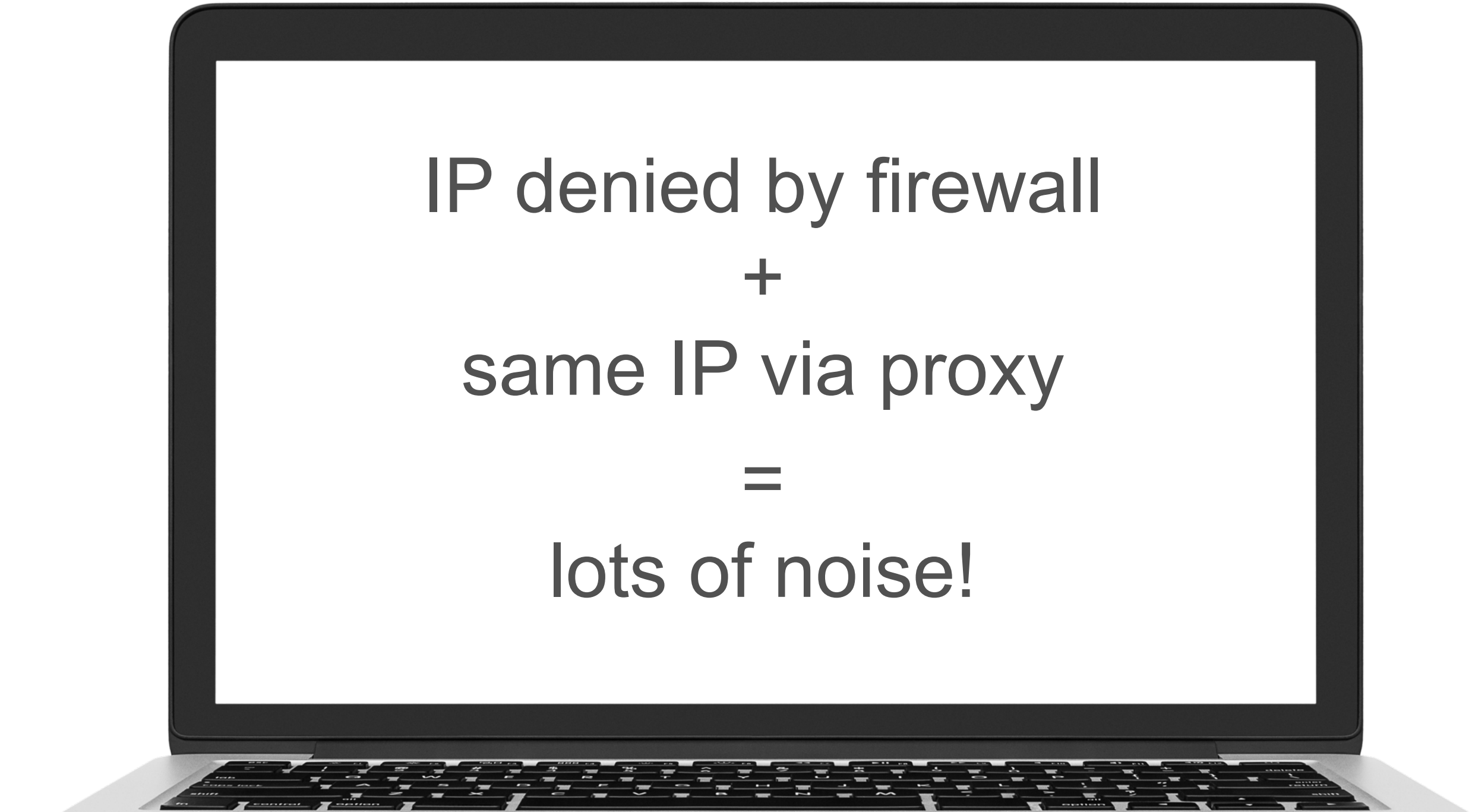
How We Approach Developing Analytics

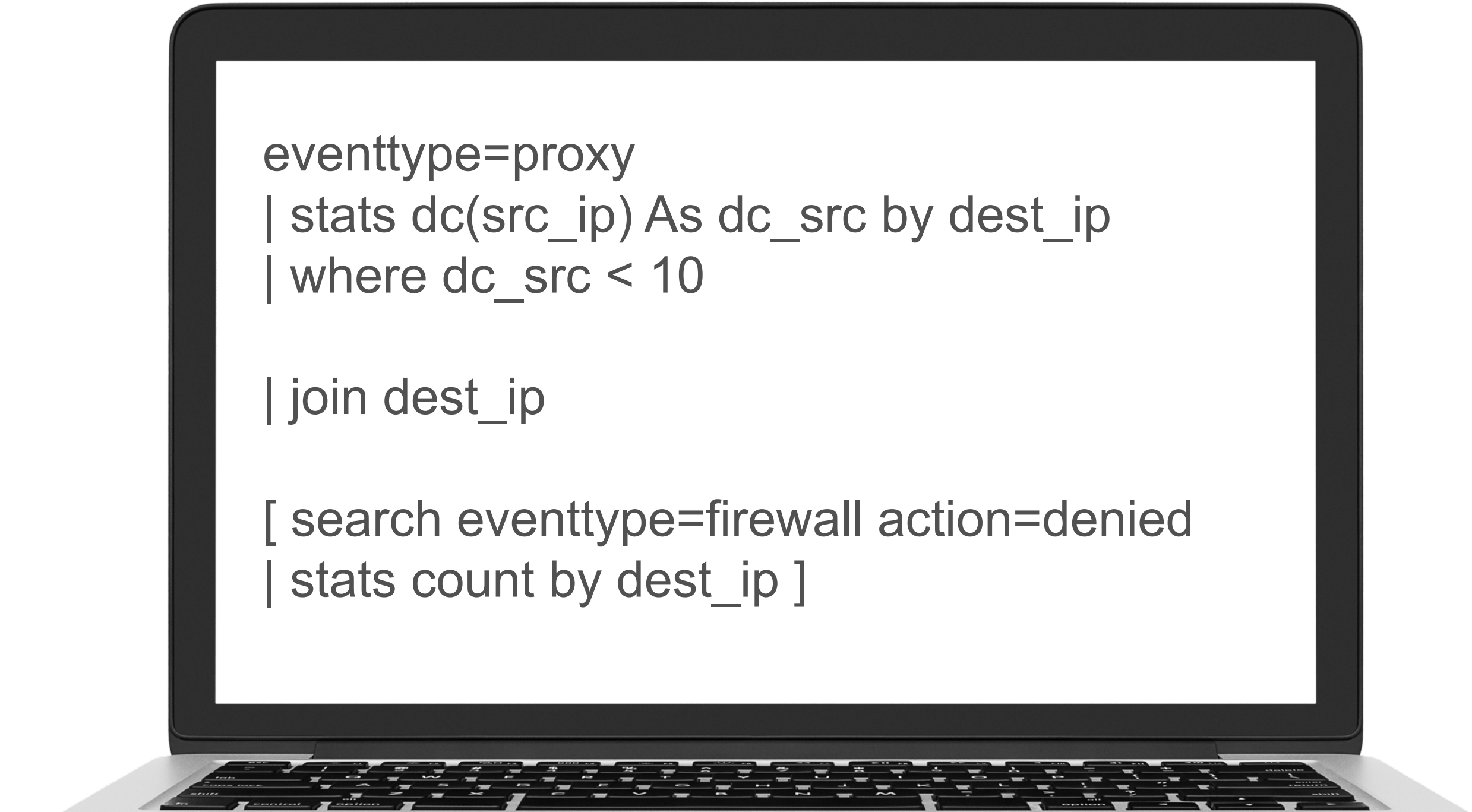
Other considerations

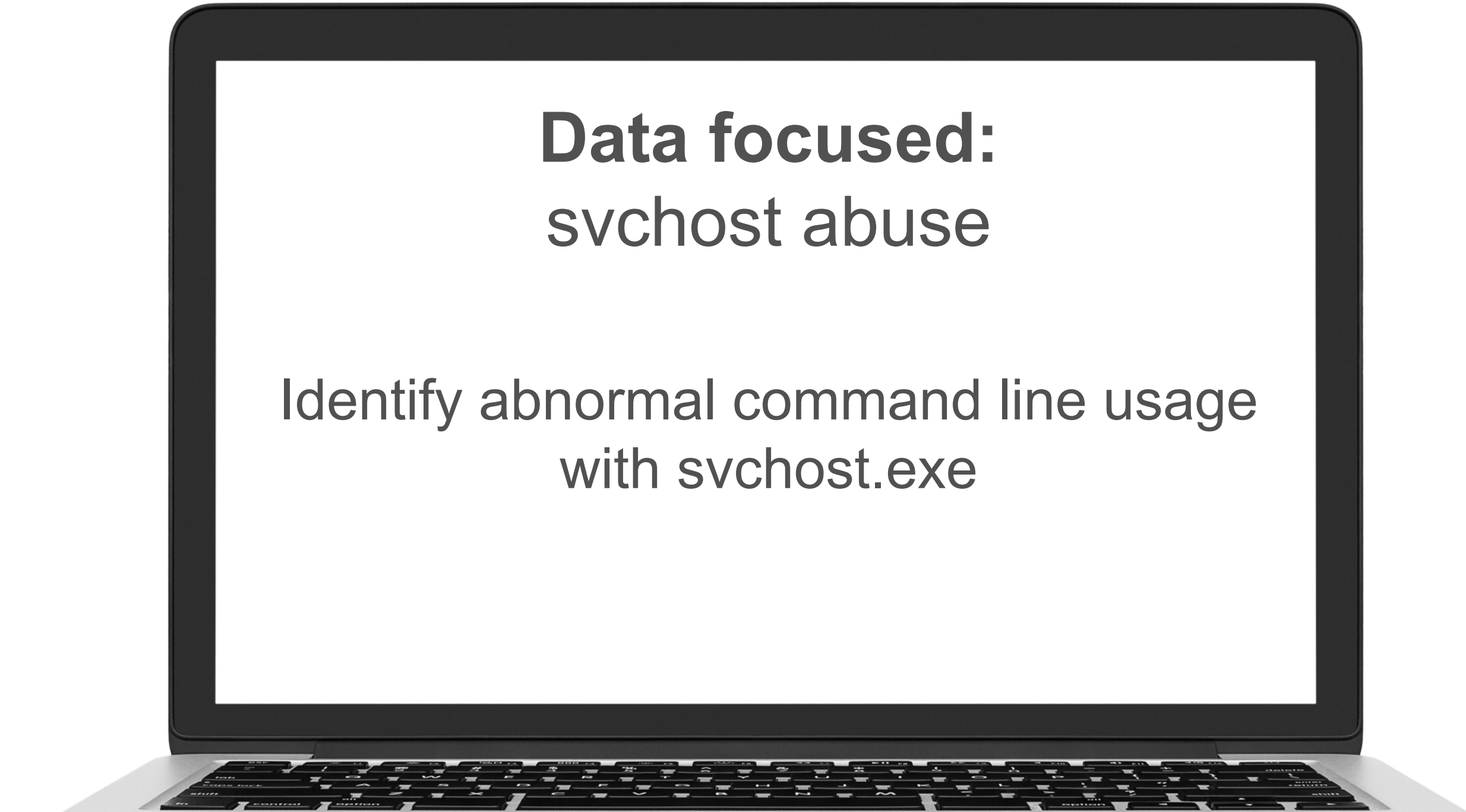
- Detect the **operation** not the attack
  - Think of the whole kill chain!
  - MITRE ATT&CK framework
- Consider incident response / alert triage plan
  - How are you really going to respond to this?

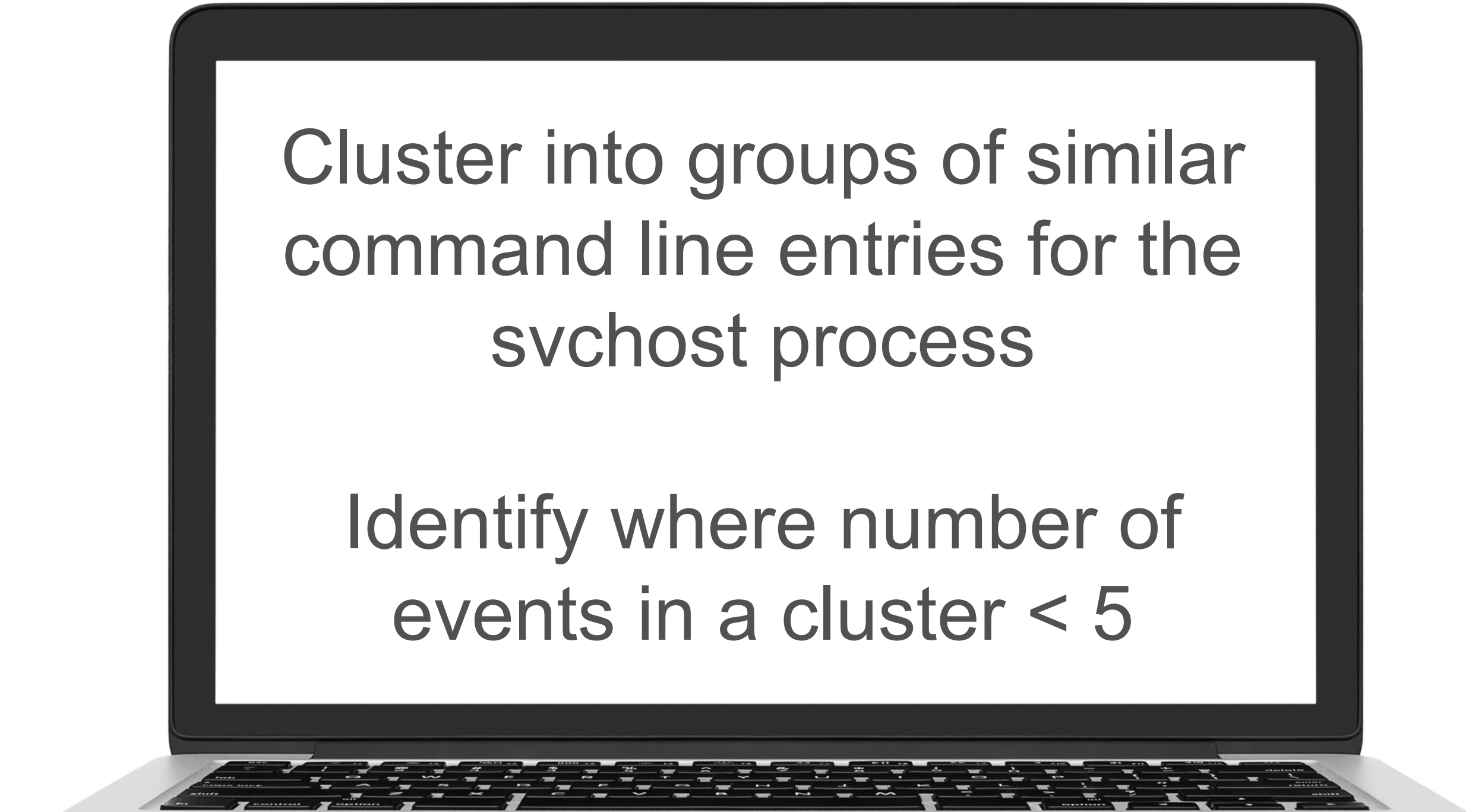


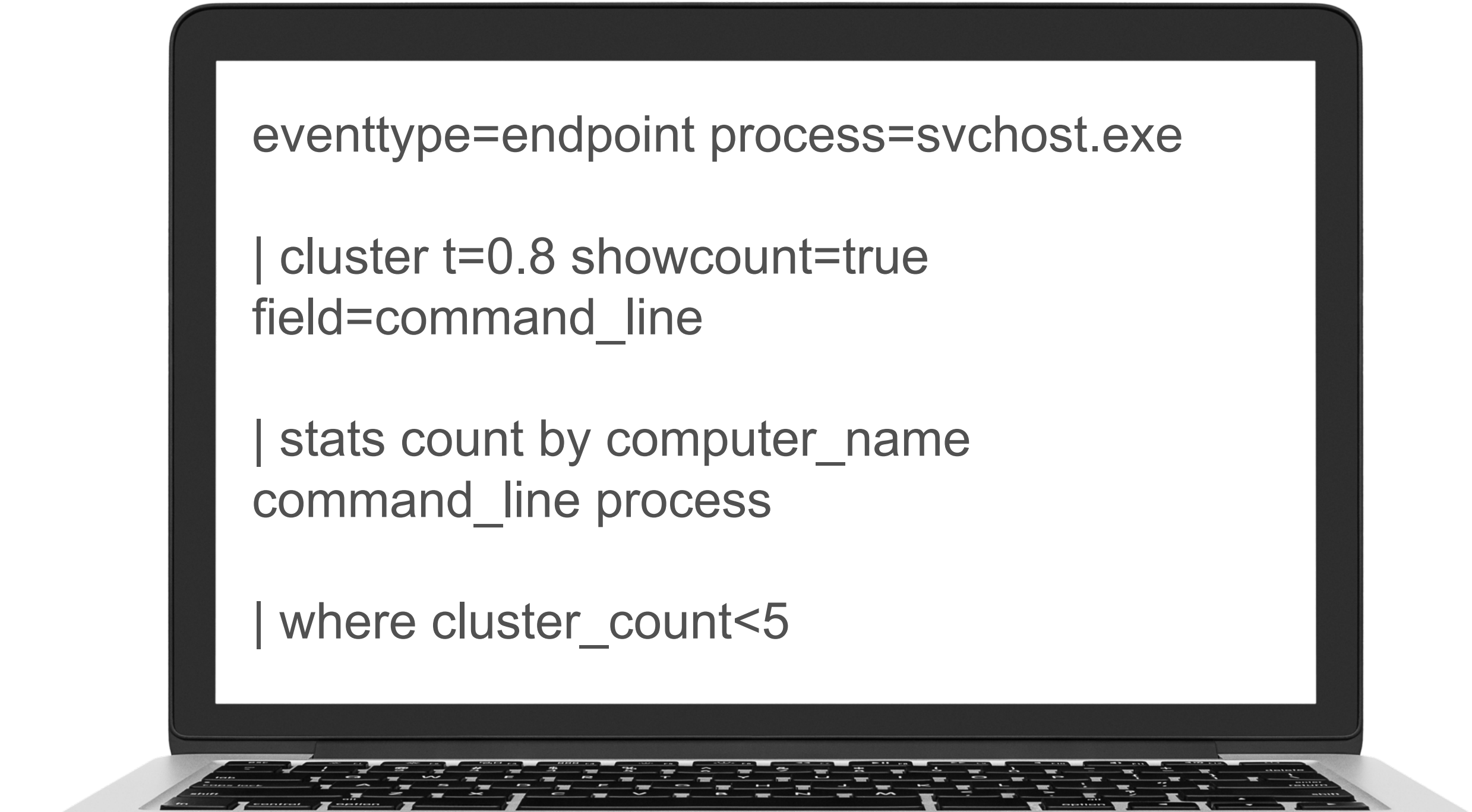

Adversary focused:
SOFACY – GRU Russia
x-agent behavior
connectivity test – checks for direct connection to IP/domain then attempts to use proxy


IP denied by firewall
+
same IP via proxy
=
lots of noise!


eventtype=proxy
| stats dc(src_ip) As dc_src by dest_ip
| where dc_src < 10
| join dest_ip
[search eventtype=firewall action=denied
| stats count by dest_ip]


Data focused:
svchost abuse
Identify abnormal command line usage
with svchost.exe


Cluster into groups of similar command line entries for the svchost process
Identify where number of events in a cluster < 5


eventtype=endpoint process=svchost.exe
| cluster t=0.8 showcount=true field=command_line
| stats count by computer_name command_line process
| where cluster_count<5

What I Wish I Knew in 2015

splunk> .conf18

What Works?

1. Show me the data - endpoint or bust
2. Empowerment - excellent analysts - rounded skill sets - training
3. Business involvement
4. A visible/tangible security capability – PR for security – Bank of Bangladesh

What Doesn't Work?

1. Threat intelligence - too Indicator of Compromise (IoC) focused
2. Shortage of skills - £££

Key Takeaways

1. Don’t be driven by vendors. Only you can know your adversaries, your environment and your business. Vendors cannot. Invest in your people.

2. If you're not constantly developing new ways of detecting attacks, your monitoring is getting worse every day.

3. Involve your business. They know the real pain points (with some guidance from you).

Thank You

Don't forget to rate this session in the .conf18 mobile app