

Detect & Respond

10 common pitfalls

that will sabotage the effectiveness
of your security program

Frode Hommedal

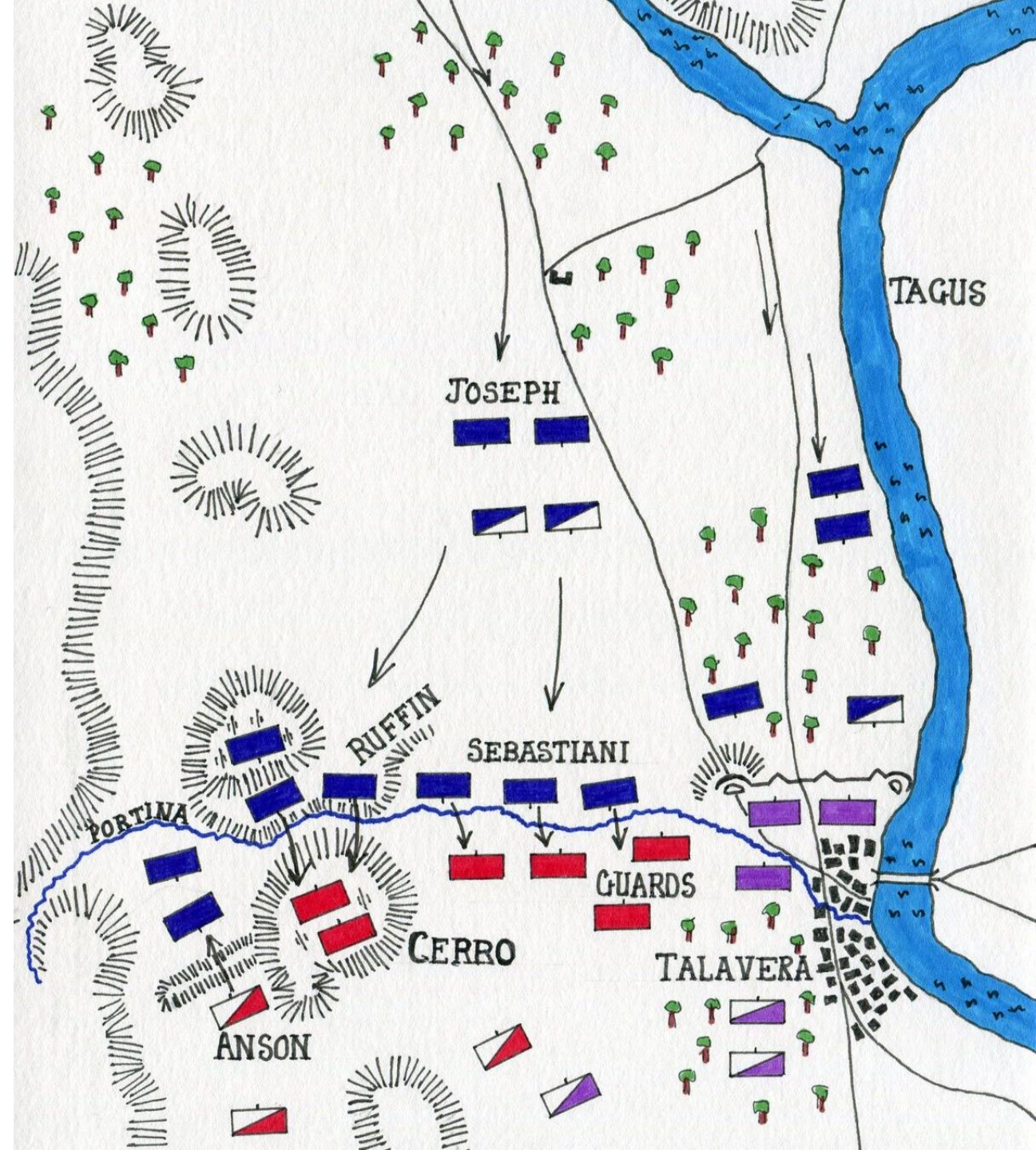
Technical Director
PwC.no/Cyber
ISF – August 2019



When designing a strategy for detection and response there are numerous pitfalls you can fall into.

This presentation will highlight some of them.

[Based on my own experience and discussions with peers]



A person with a shaved head, wearing a dark plaid shirt, is seen from behind, looking out a window with white horizontal blinds. The person's right arm is raised, touching the blinds. The scene is brightly lit from the window, creating a high-contrast silhouette effect.

“

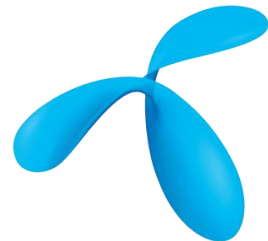
If you fall into too many of these, your security program will likely be **ineffective at protecting your organization** from internal and external threats.

#whoami

**Technical analyst turned
strategic advisor within
the field of detection and
response and ... security.**



NORWEGIAN
NATIONAL SECURITY
AUTHORITY



telenor



Pitfall #1

Guessing risk, not basing it on asset valuation and threat and vulnerability assessments.

“

Risk comes from not knowing what you're doing. – Warren Buffett



Pitfall #2

Not creating an actual security strategy.

“

*Strategy without tactics is the longest route to victory, tactics without strategy is **the noise before defeat**.* – Sun Tzu



Pitfall #3

Not clearly defining the scope and mission of your SOC and CSIRT.

“

*I learned that **focus is key**.
Not just in your running
a company, but in your
personal life as well.*

– Tim Cook

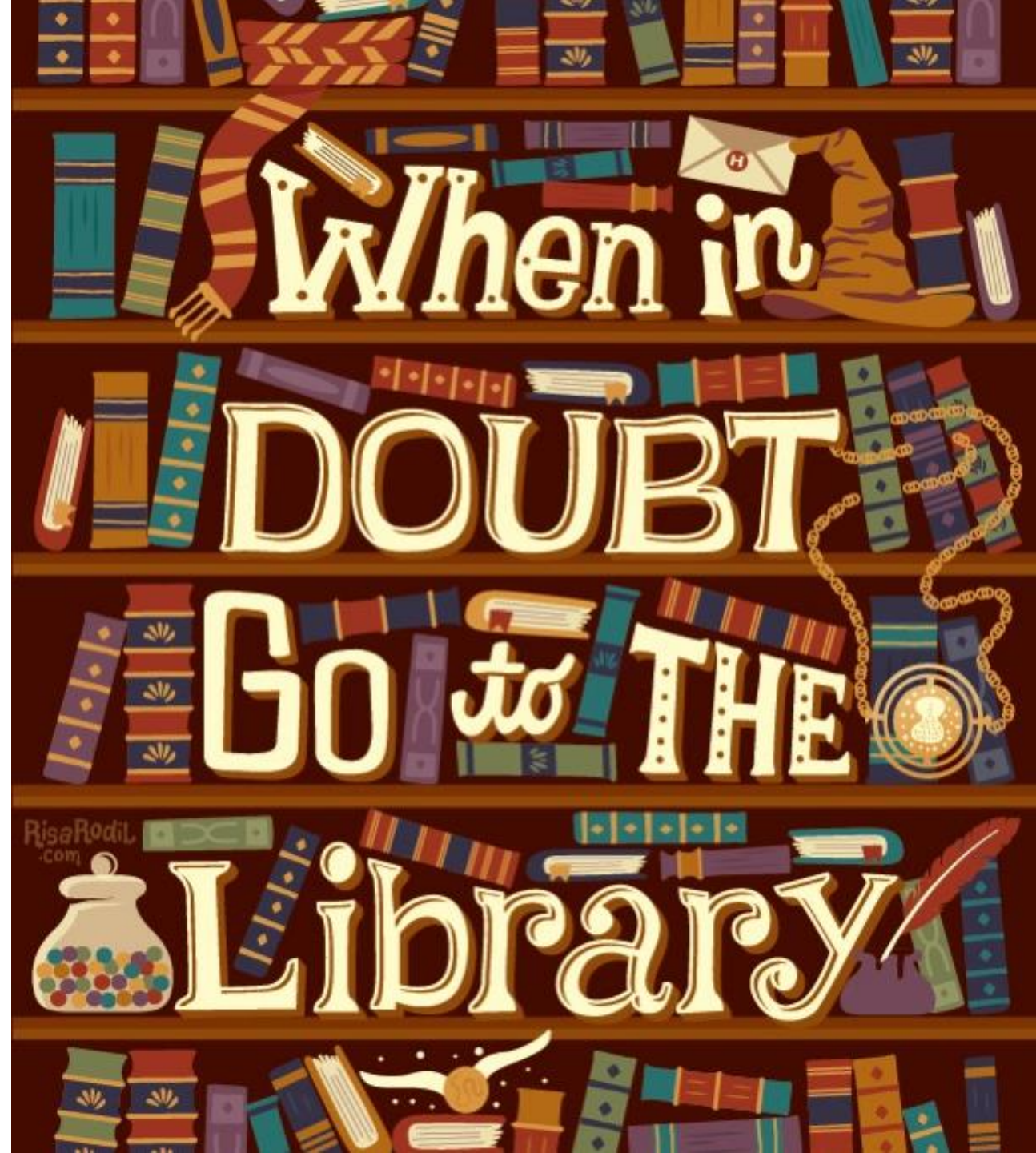


Pitfall #4

Not investing in centralized logging.

“

*The only thing that you
absolutely have to know,
is the **location** of the
library.* –Albert Einstein



Pitfall #5

Not continuously investing in data quality.

“

*Information is a source of learning. But **unless** it is organized, processed, and available to the right people in a format for decision making, it is **a burden, not a benefit.***

– William Pollard



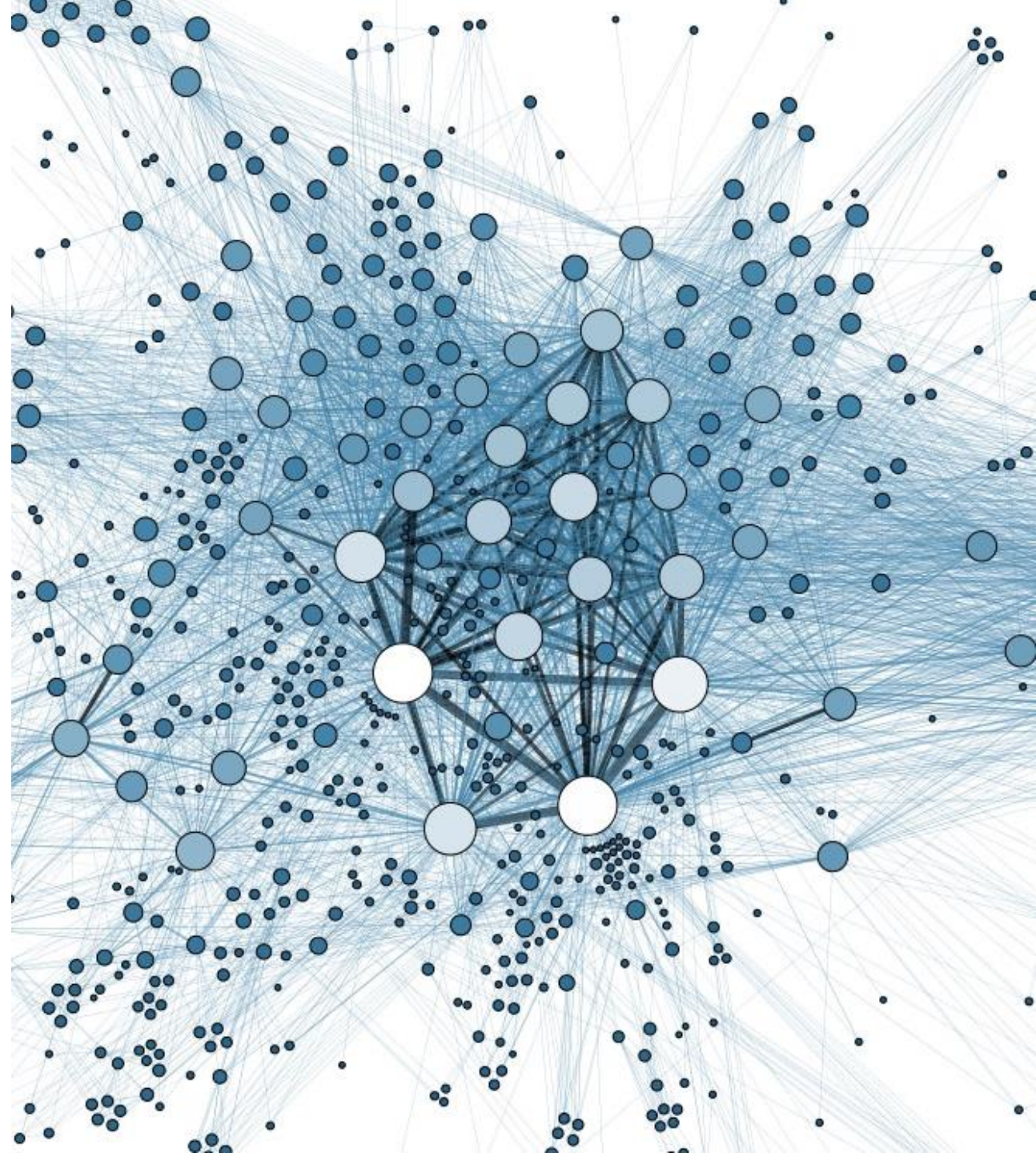
Pitfall #6

Blindly trusting that vendor detection logic will discover your threats.

“

*You can use all the quantitative **data** you can get, but you still have to **distrust** it and use your own intelligence and judgment.*

– Alvin Toffler



Pitfall #7

Not integrating all your security solutions in one centralized cockpit.

“

Efficiency is the foundation for survival.

Effectiveness is the foundation for success.

– John C. Maxwell



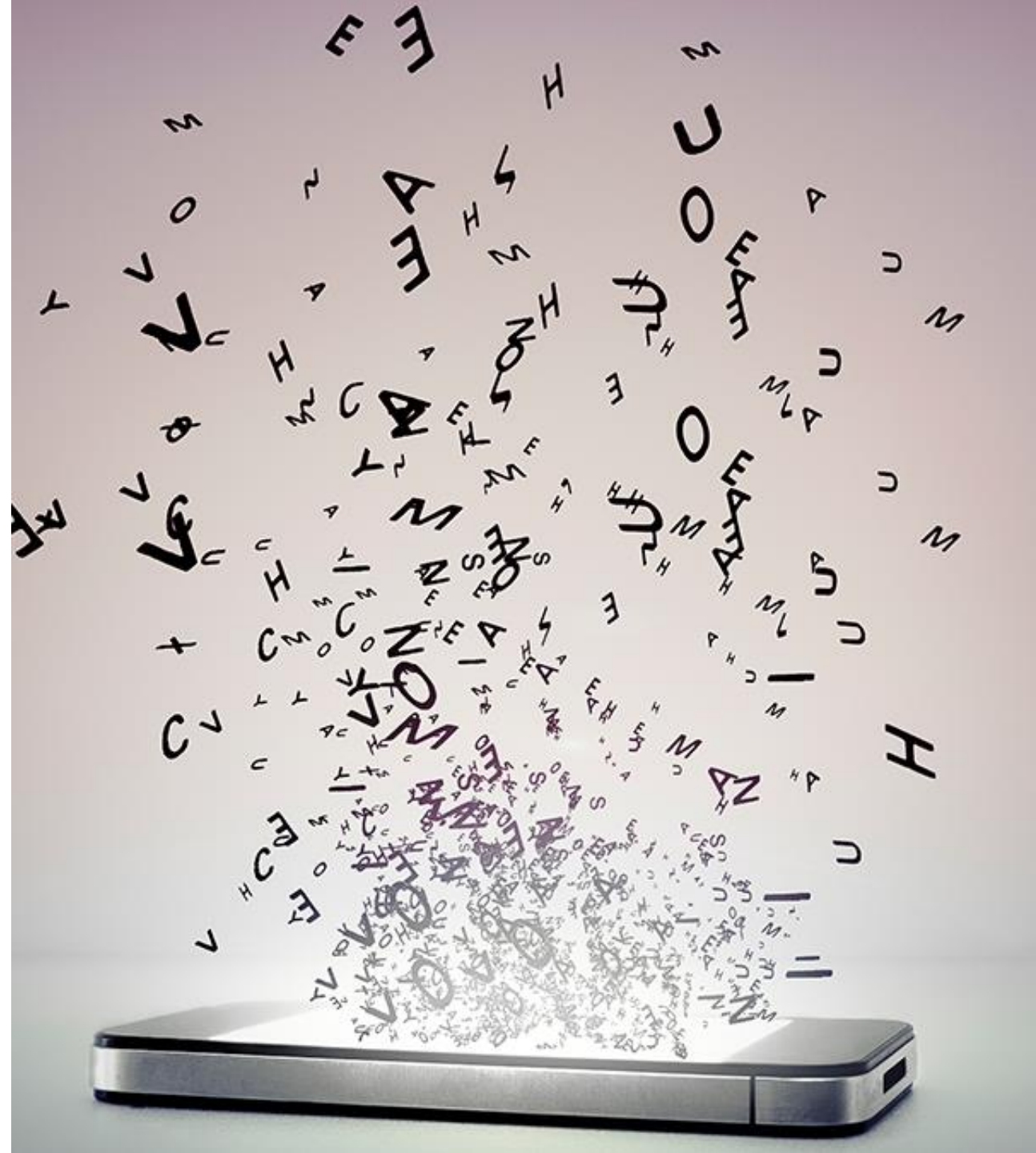
Pitfall #8

Failing to take the necessary time to seek out available knowledge.

“

*Learning is **not attained by chance**, it must be sought for with ardor and attended to with diligence.*

– Abigail Adams



Pitfall #9

Not systematically learn from the insights offered by your SOC and CSIRT.

“

*No one can whistle a symphony. It takes a whole **orchestra** to play it.*

– H.E. Luccock



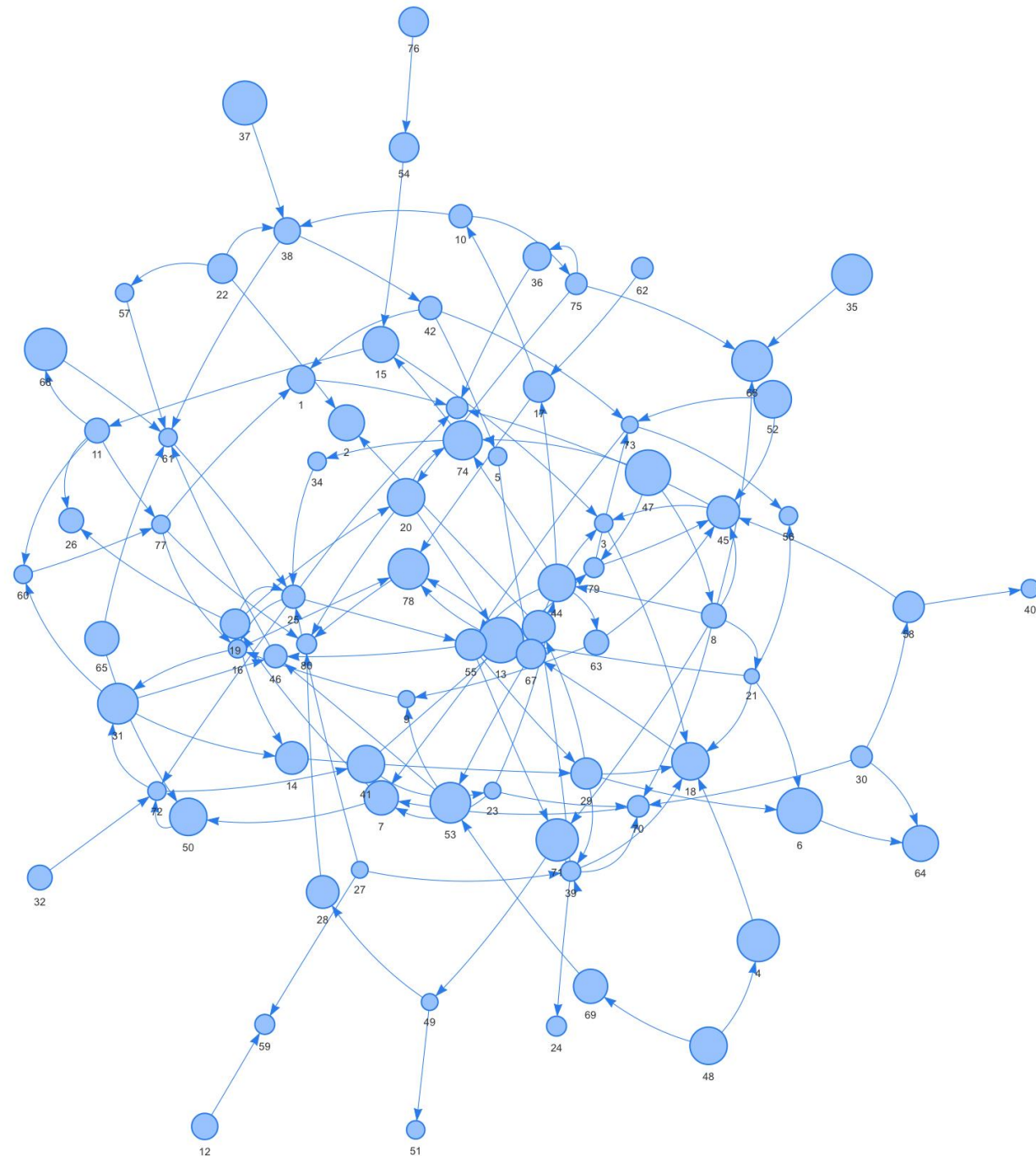
Pitfall #10

Not thinking in terms of dependencies.

“

*Defenders think in **lists**.
Attackers think in **graphs**. As long as this is true, attackers win.*

– John Lambert



Thank you

Frode Hommedal

Technical Director

ISF – August 2019

pwc.no/Cyber

Feel free to reach out if you have
any **questions** or **comments**.

frode.hommedal@pwc.com

© 2019 PwC. All rights reserved. Not for further distribution without the permission of PwC. “PwC” refers to the network of member firms of PricewaterhouseCoopers International Limited (PwCIL), or, as the context requires, individual member firms of the PwC network. Each member firm is a separate legal entity and does not act as agent of PwCIL or any other member firm. PwCIL does not provide any services to clients. PwCIL is not responsible or liable for the acts or omissions of any of its member firms nor can it control the exercise of their professional judgment or bind them in any way. No member firm is responsible or liable for the acts or omissions of any other member firm nor can it control the exercise of another member firm’s professional judgment or bind another member firm or PwCIL in any way.