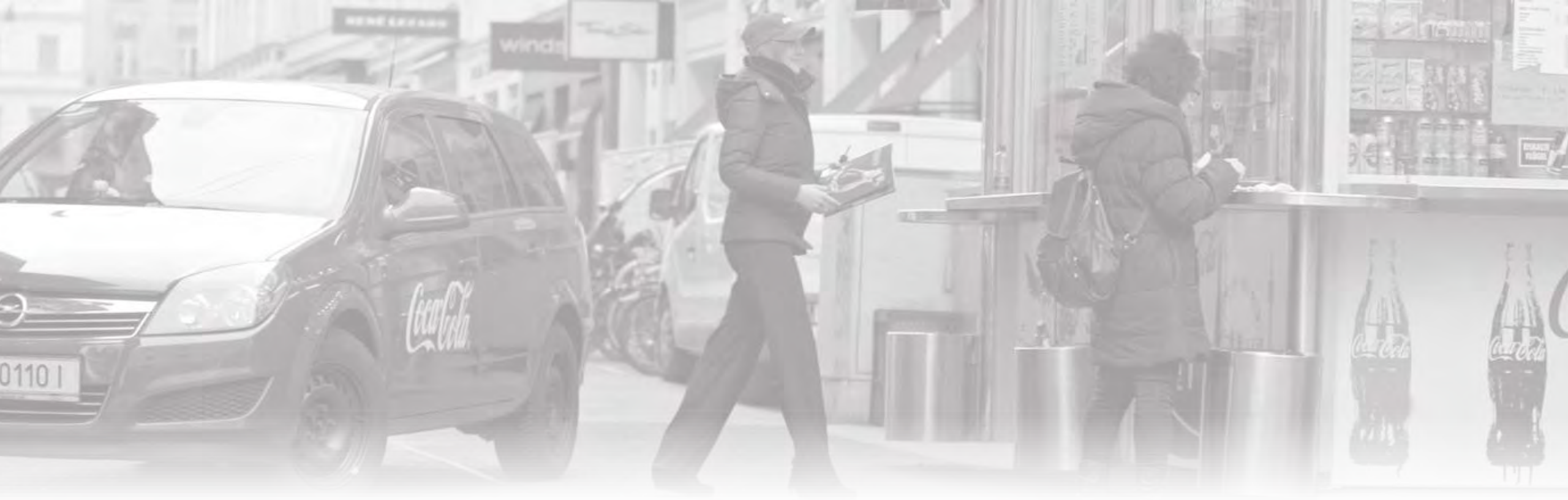
Ingredients for Successful Security Operation Centers

6th INFORMATION SECURITY CONFERENCE

George Kanellopoulos

- ☐ What is a Security Operations Center ?
- ☐ Why anyone needs a SOC?
- ☐ How to setup a successful SOC?

Are you ready to respond to a major cyber security breach if it happens to your company?



Faster cyber attack detection, response, & recovery through threat intelligence, security event monitoring and incident response processes

Talent

Get the right people who know what they are doing and have done it multiple times before

Intelligence

Aim to build a SOC that is intelligent, and relevant to your specific environment

Prioritize

Focus on attack use cases which are ‘alive’, have high potential business impact and are easy to implement

Technology

Analytics, Forensics, Incident Response,
Ticketing, SIEM, Threat Intelligence,
Vulnerability management, ...

Patch Management, Security Architecture,
Risk Management, Awareness

Automate

Aim for pre-defined, automated ticketing and response actions (APIs, Scripts)

Time-to-fix monthly trends

Attacks constantly evolve, an obsolete SOC will respond to obsolete attacks

SOC Ingredients

1. Talent 88gr
2. Intelligence 42gr
3. Prioritize 23gr
4. Technology 14gr
5. Integrate 9gr
6. Automate 12gr
7. Measure 8gr
8. Refresh 49gr

Thank you