Getting started with SecOps

Practical tips for building - or being - the blue team of your dreams.

Mikko Koivunen

TurkuSec 10.03.2022

Hello, who’s this?

Recent activities:

- I work as a security consultant at Knowit.
- Technical hobbies like Microsoft Sentinel development at secopslab.fi
- Family life, gardening, making music, kummalpualjokke.fi 

How I got started in security?

- BBS scene in the ‘90s introduced me to things like Phrack, 2600…
- After school went to work in IT: helpdesk -> infrastructure -> security.

On the menu today

- So you are doing IT? Good for you.
- How can you also start doing security, in a somewhat formalized way?
- Selected ideas for individuals, teams or organisations.

What is Security Operations ?

- The daily work of keeping systems secure, detecting problems and responding when things happen.
- The classic triangle: people, processes and technology.
- Is it the same as SOC? Yes, no, sometimes.

If you want to be good at it:

Consider it a **service** that needs people, leadership, measuring and continuous development.

What has changed in SecOps?

- In the olden days, **the SOC** was something independent and isolated. Not interested in prevention, focusing on detection & response.
- Today we need a collaborative approach with minimal process blockers:

> *“think QA [find and fix bugs], not helpdesk [wait for issues and handle them]”*
>
> *-Anton Chuvakin*

- Focus should be on people and skills, not tiers.
- A consistent set of core processes is needed, but allow room for creativity.
- Modernization is not the same as ”automation”, but if you can automate, do it.

How do you get started?

- The usual start is to have a virtual team - a collaborative effort with people from different roles but with interest in security.
- Make it a “Center of Expertise”, that provides leadership, support and is open for dialogue with everyone.
- When your organisation grows, make sure SecOps grows organically with the same pace.

Get good at the basics

- Maintaining security policies.
- Maintaining access policies.
- Keep up with assets, patching and vulnerabilities.
- Demand quality from your vendors and partners.
- Not glamorous, but critical.

Work with others

- Work with management:
  - Usually, more money is needed.
  - Get on the same page about communications, mandates, criticality…
- Work with end users:
  - Make sure they know you do monitoring.
  - Cultivate a low treshold for contact, both ways.
  - Don’t scare people.

Heatmap your security capabilities

- Plenty of public resources available, about what processes, tools and tech are common and available.
- Map your findings to what you have now.
- If something is missing, understand if it’s really needed.
- You don’t have to do everything.

Do we have / Do we need?

“Vulnerability assessment” etc

“SIEM” “Incident response process” etc

”Technical control X” ”Security product Y”

Know your security toolkit

- What tools do you have that can detect threats and generate alerts?
- What tools do you have to report on your security posture?
- What data do you have for doing custom threat detection?
- How can you get the findings and alerts to one place?

Build custom detections

- Detection engineering takes time and practice.
- So does managing a SIEM.
- Do it by all means, but understand the resource requirements.
- My suggestion is to look at SaaS options, so you can focus on the content instead of the engine.

Understand your data

- Some data is high-value for detection.
- Some is not - but can be high-value for investigation.

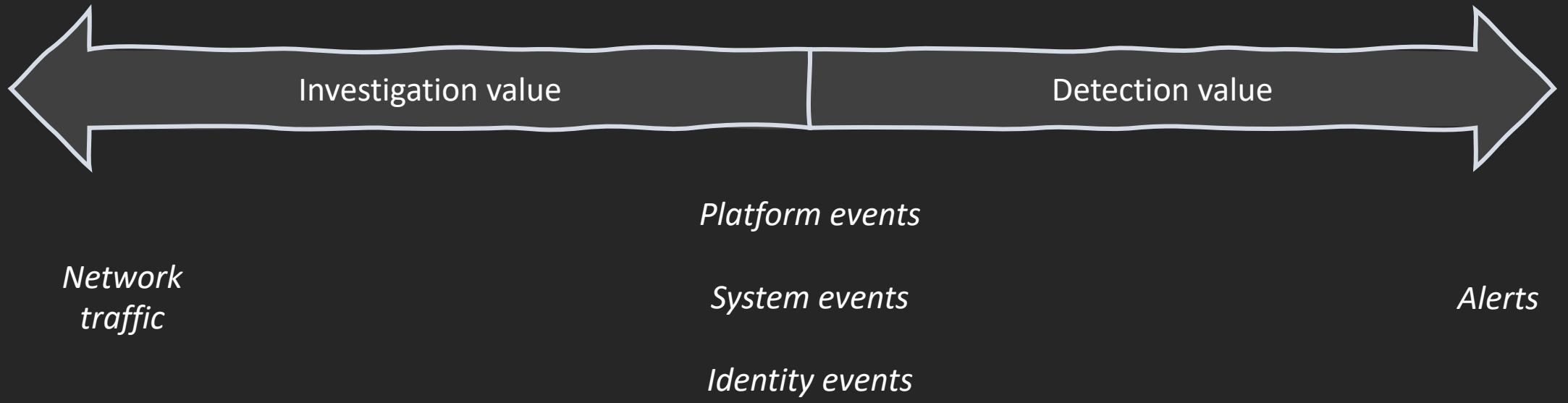


Figure out what happens after hours?

By default:

- If you do IT operations 8-16, you also do security operations 8-16.
- If an incident happens on a Saturday → management's problem.

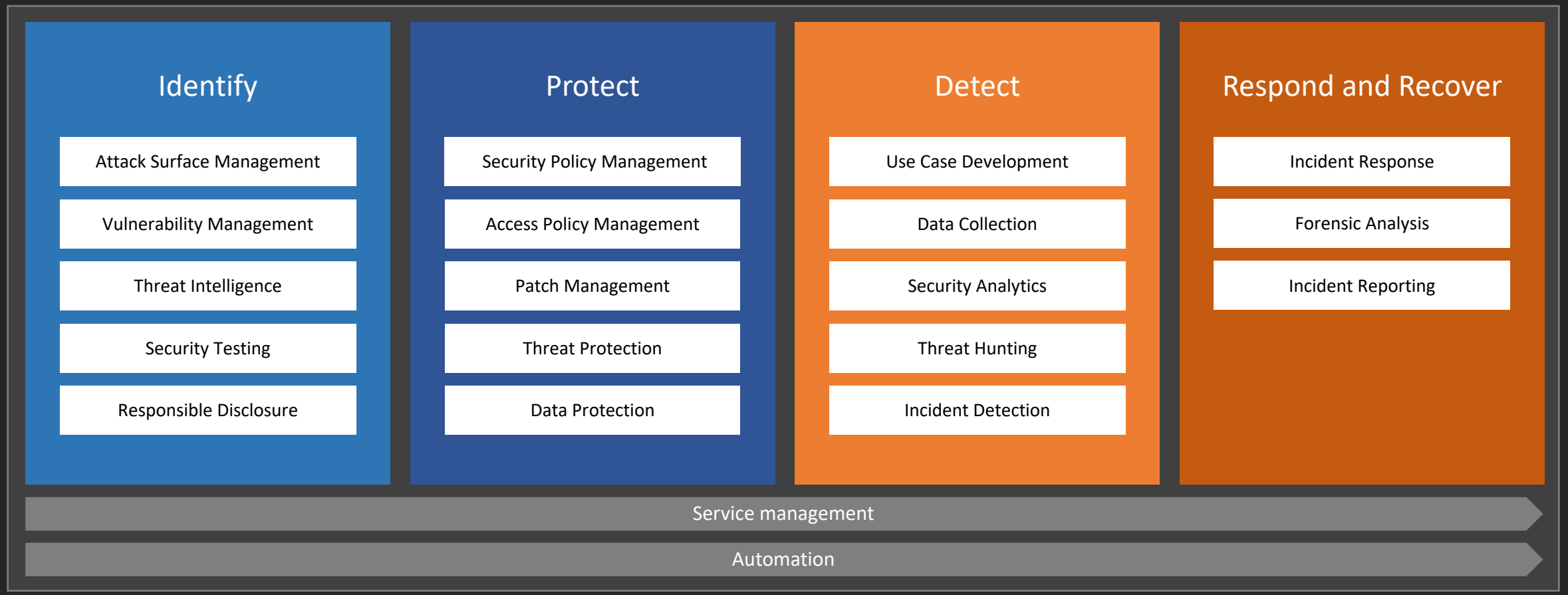
If you want to start working 24/7:

- Start with generic IT on-call rotation.
- Onboard security responsibilities to that.
- Consider more advanced options later.

What about MSPs?

- Don’t “buy a SOC” before you have basic capability to do most of this work by yourself.
- When incidents happen, you want in-house decision making.
- On the other hand… Don’t be afraid to buy services to help where you **know** you lack resources.
- You can also just buy consultancy to help you develop your in-house capabilities, instead of outsourcing the work itself.

What do you end up with?



https://github.com/mikoiv/secops-standard-model/