Building an INCIDENT RESPONSE function

WHO AND WHY?

Michalis Kamprianis

MBA, MSc

1.

The Organization ***know the cards***

We cannot
change the cards
we are dealt,
just how we play
the hand

Randy Pausch

Fundamental information

- **Business needs and requirements**
- Maturity (of the security function)
- Organizational Structure
- Organizational Culture
- Risk Appetite
- Financial and other Constraints

Strategic and Tactical decisions

Strategic

- The Scope
- Team autonomy
- Response schedule
- Operating Model

Tactical

- Tools and toolsets
- Detailed playbooks

2.

The Scope

What do we care about?

Sample scope definition

Priority

- Application(s)
  - On premises
  - Cloud
- Endpoints

Non priority

- Users
- Network

Risk Appetite
Security Maturity

Is anyone helping you? Examples

Early Incident Notification

- Outsourced network management
- Cloud service providers
  - SaaS
  - PaaS

Actual Response

- Internal IT teams
- External Incident Response vendors

3.

Team Autonomy

Can you make a difference?

CSIRT as part of SOC

Advantages

- Easier staffing
- Less resources
- Deeper knowledge
- No analysis fatigue
- Development opportunities

Disadvantages

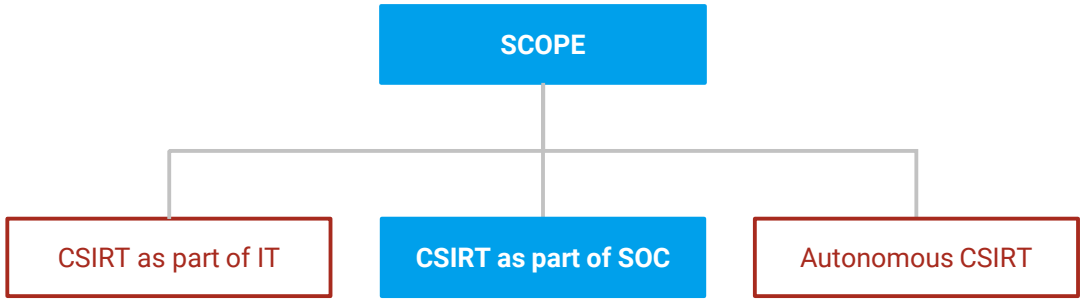
- Different mindset
- Lack of focus
- Wider knowledge
- Work Overload

CSIRT as an IT function

- Security Response versus IT Response
- Response versus Operations
- Priorities and staffing
- Very different mindset
- Easier playbooks
- Better coordination / or not

Org. Structure
Security Maturity
Constraints

Decision Tree



4.

Response Schedule

There’s a fire!
Now what?

Continuous versus “Working hours”

Model 24x7

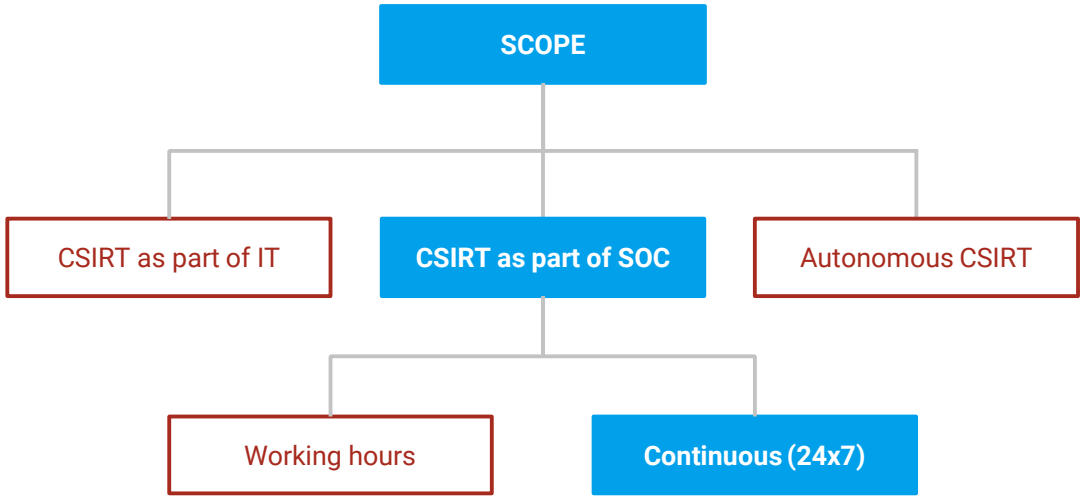
- How much delay is acceptable?
- Who else can receive notifications?
- Budget?
- Other 24x7 teams?

Model “working hours”

- What is the damage of delay?
- Who is our attacker?
- Where are our in-scope systems?

Risk Appetite
Security Maturity

Decision Tree



5.

Operating model

Where is my CSIRT?

In house or MSSP?

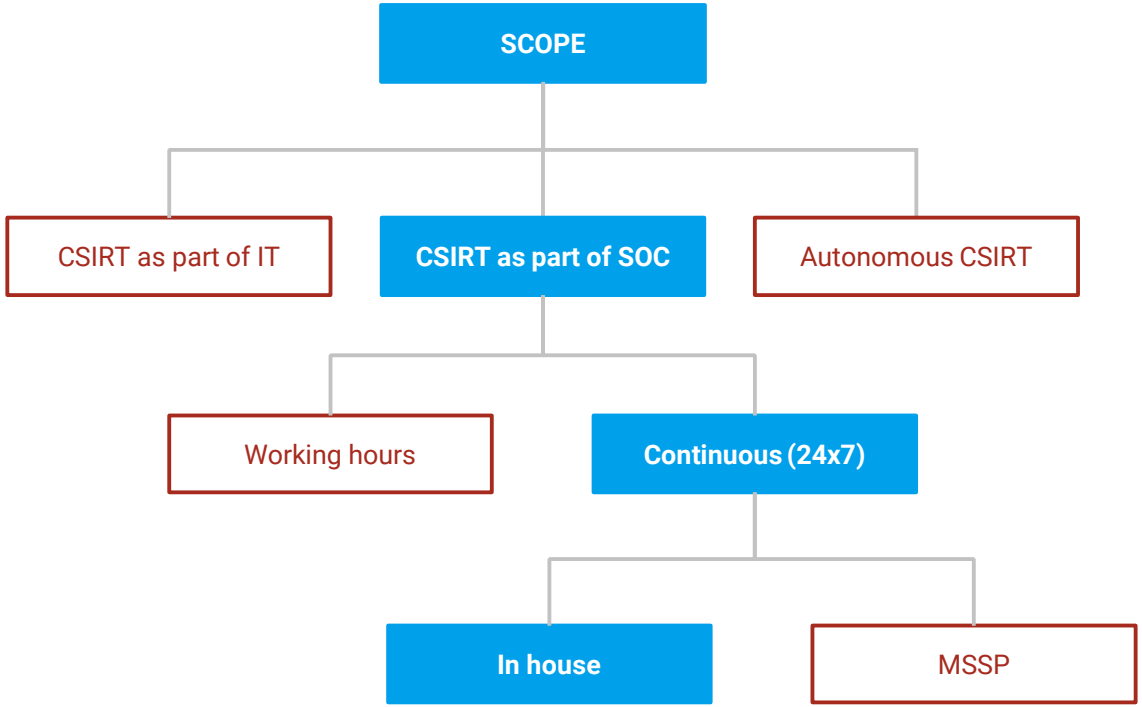
In house

- Flexible architecture
- Build knowledge
- Easier communication
- Long deployment time
- Prone to errors

MSSP

- MSSP Architecture and products
- Stable resource supply
- Established playbooks
- Typical vendor relationship
- Quick start

Decision Tree



5.1

Decisions decisions

Where is my CSIRT?

Follow the sun or centralized?

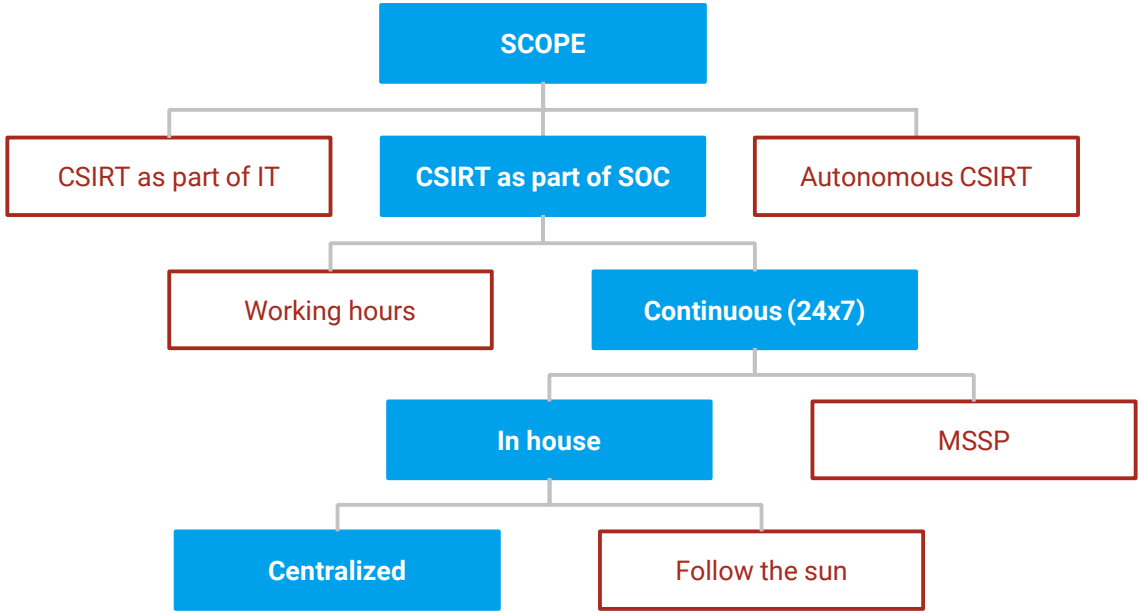
Follow the sun

- Easier staffing
- More costly
- Less efficient handover
- Easier communication with business

Centralized

- Talent shortage
- Cheaper resources
- Simpler HR processes
- Better handover
- Easier communication within CSIRT

Decision Tree



THANKS!

Any questions? Ask me now or

On Twitter: @kamprianism

By email: michalis.kamprianis@gmail.com

At my blog: https://kamprianis.eu/michalis/i.think

On LinkedIn: https://www.linkedin.com/in/michaliskamprianis