Partially funded by U-2010, an Integrated Research Project
of the 5th Call in the 6th European Research Framework Program

HoneyBot

Decoy Devices for Security Monitoring in Emergency & Mobile Network

Alexandre Dulaunoy, SES ASTRA

Security Monitoring in Emergency & Mobile Networks

Problem statement :

Emergency networks have to **run** before we can secure and monitor them

Decoy Devices

Decoy devices are used to fool the attackers

But also exists in computer network security to discover attackers on large-scale networks

Decoy Devices

(low-interaction honeypot)

"In computer network security,
a honeypot is a trap set to detect, deflect,
or in some manner counteract attempts at
unauthorized use of information systems."

A Technique of Security Monitoring

HoneyBot

Leverage of honeypot technology in emergency and mobile network

Limited false-positive and information overload
"only a target for suspicious activities"

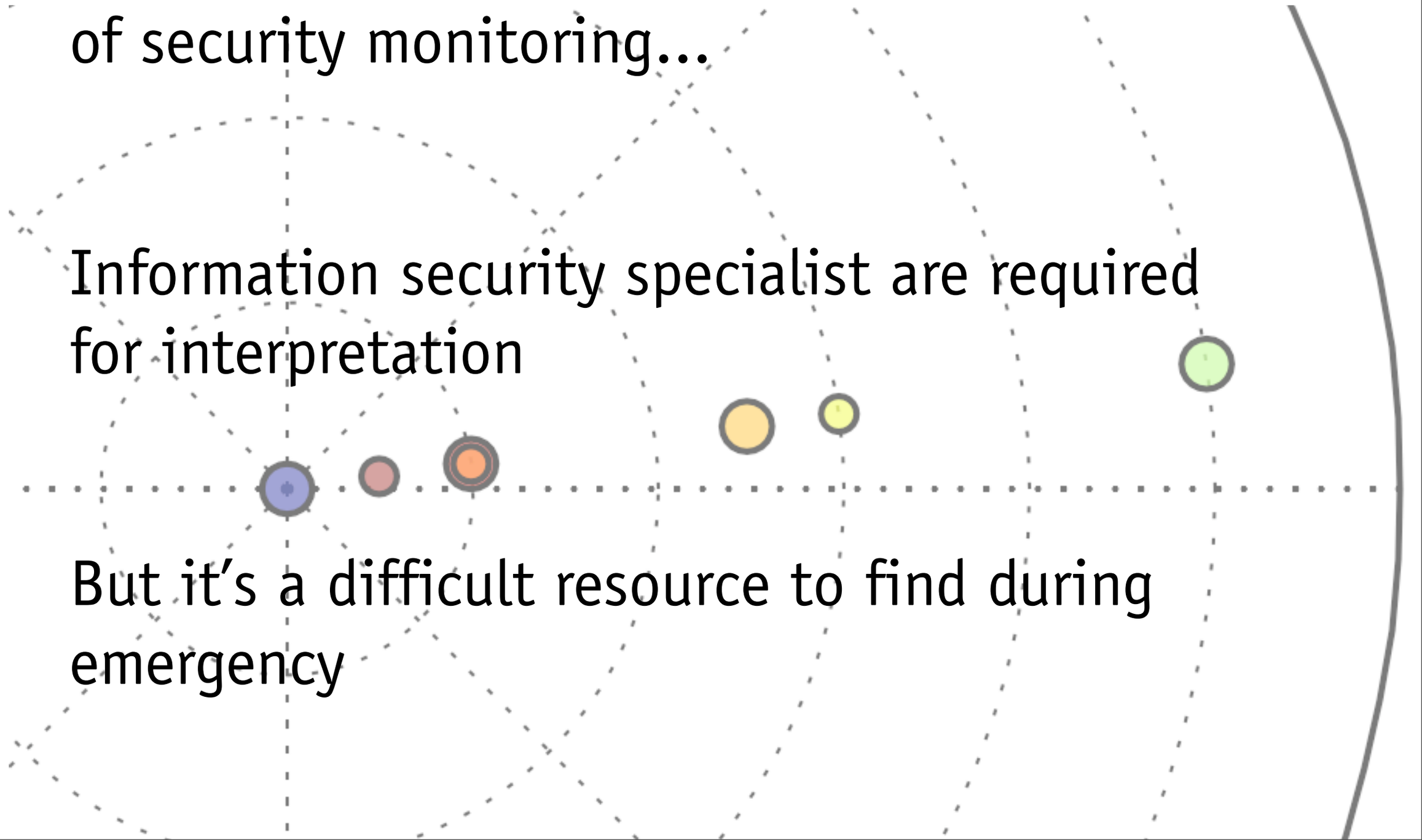
Fast deployment and fast monitoring
"plug&forget"

HoneyBot Devices are unmanned during operation

Monitoring

Security Visualization to The Rescue

Gathering suspicious activities is only a part of security monitoring...

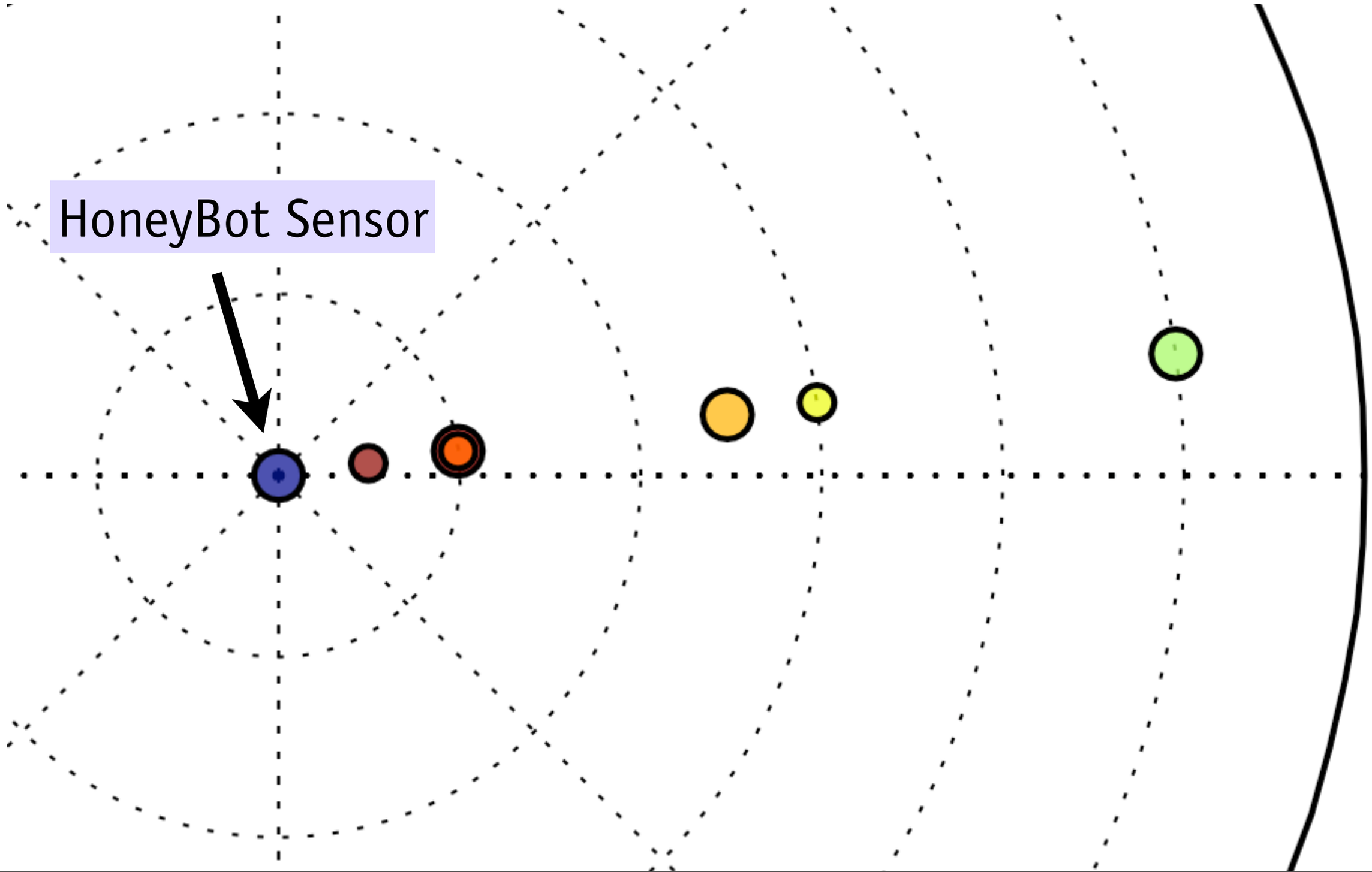


Information security specialist are required for interpretation

But it’s a difficult resource to find during emergency

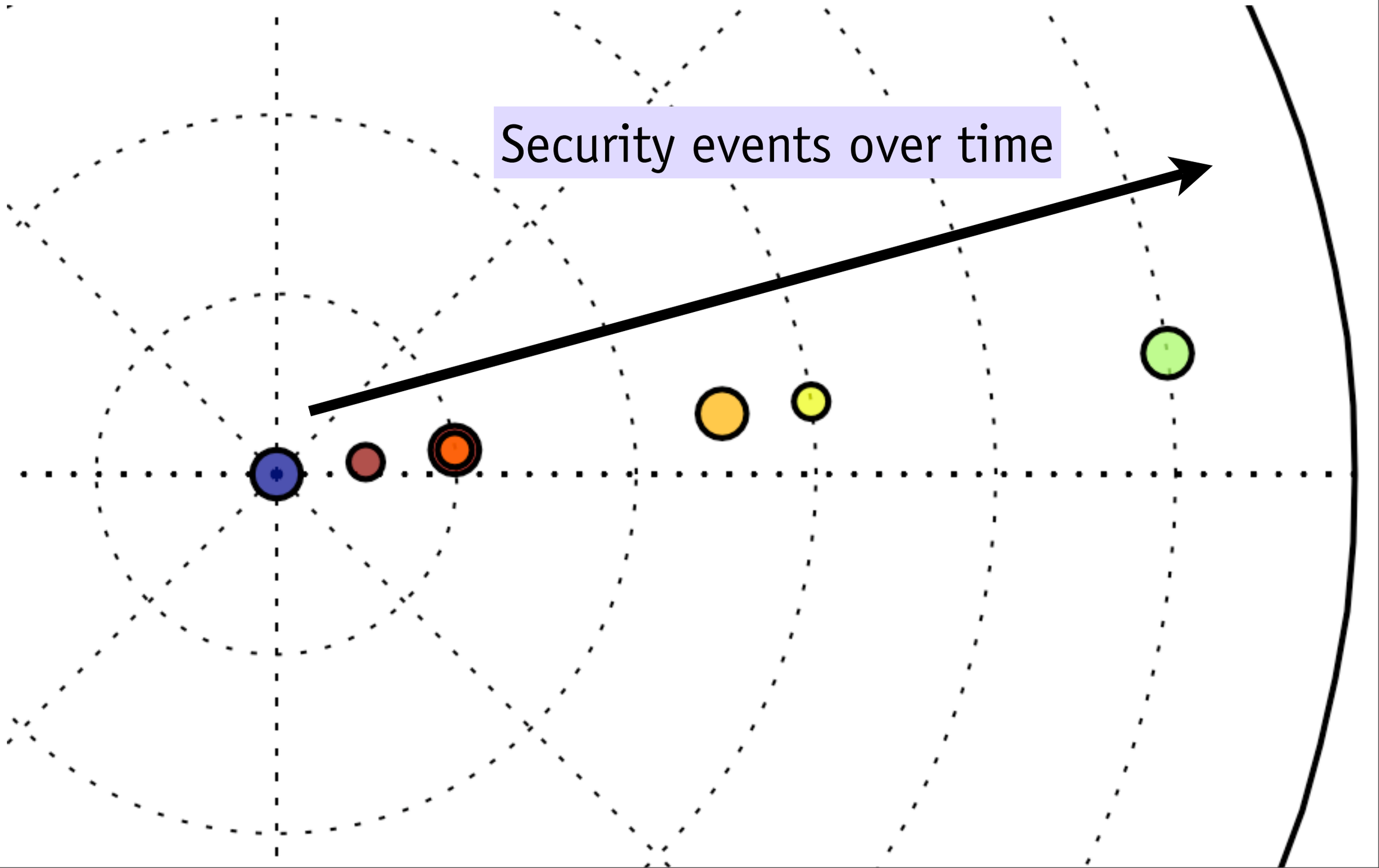
Monitoring

Security Visualization to The Rescue



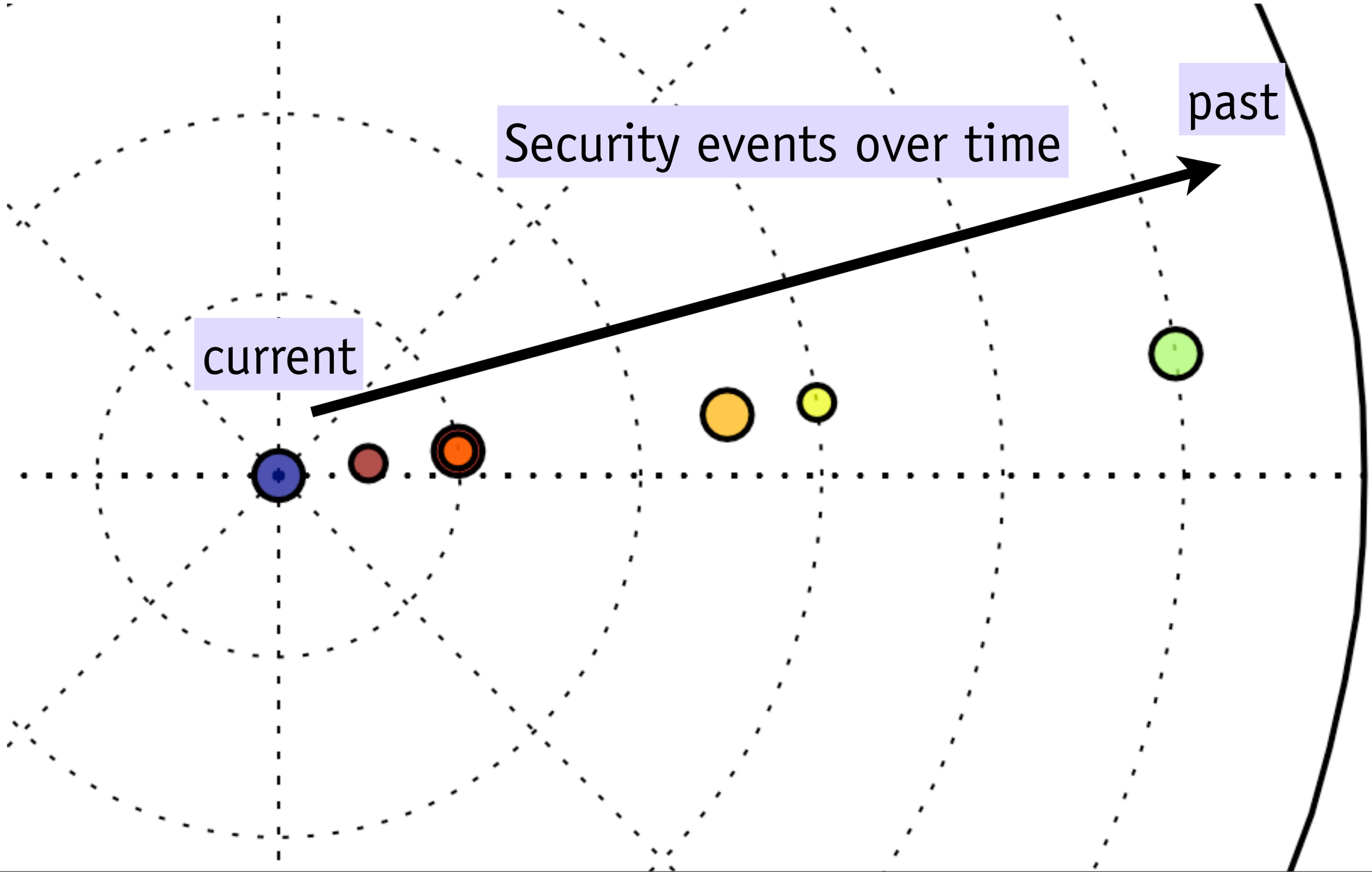
Monitoring

Security Visualization to The Rescue



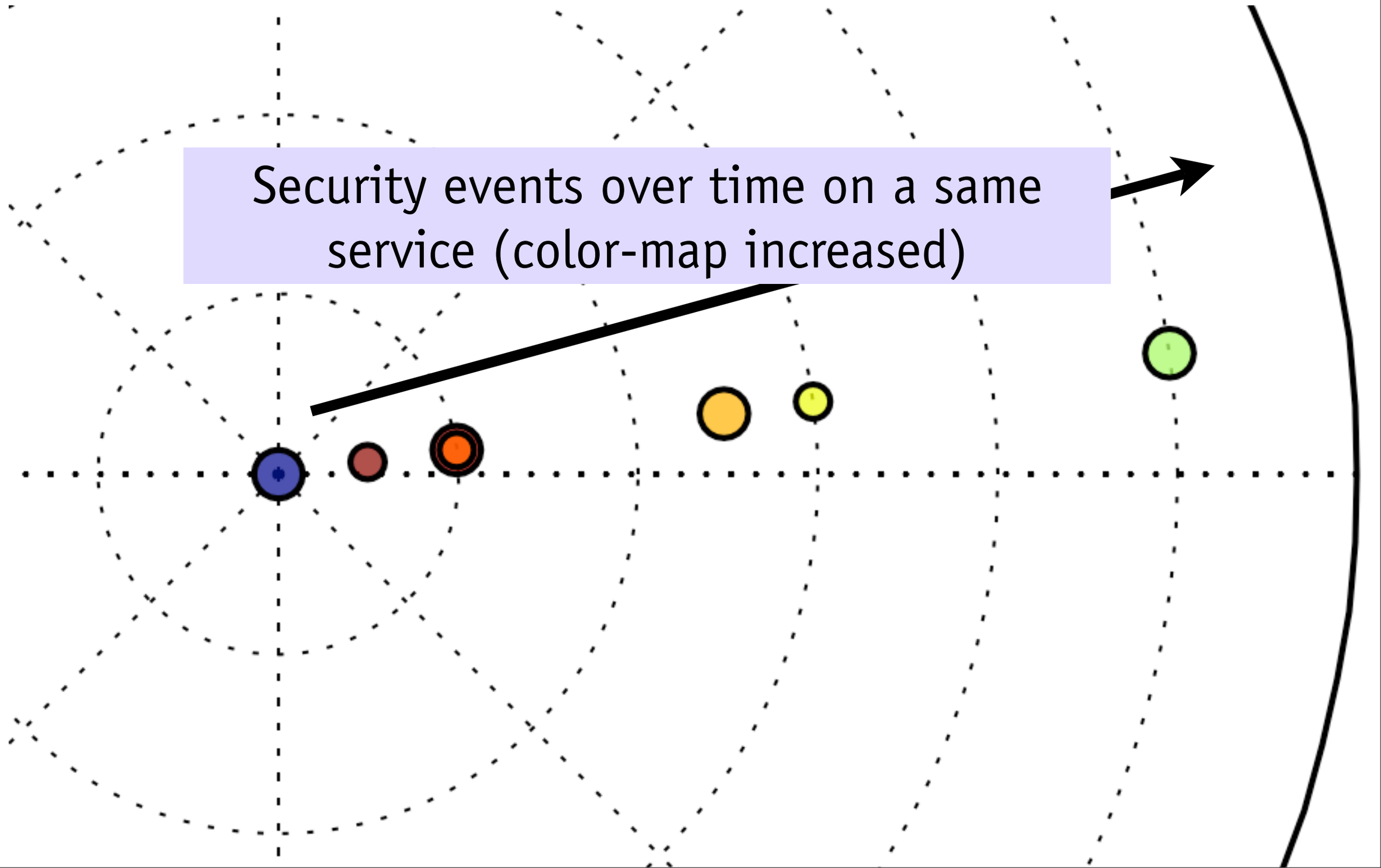
Monitoring

Security Visualization to The Rescue



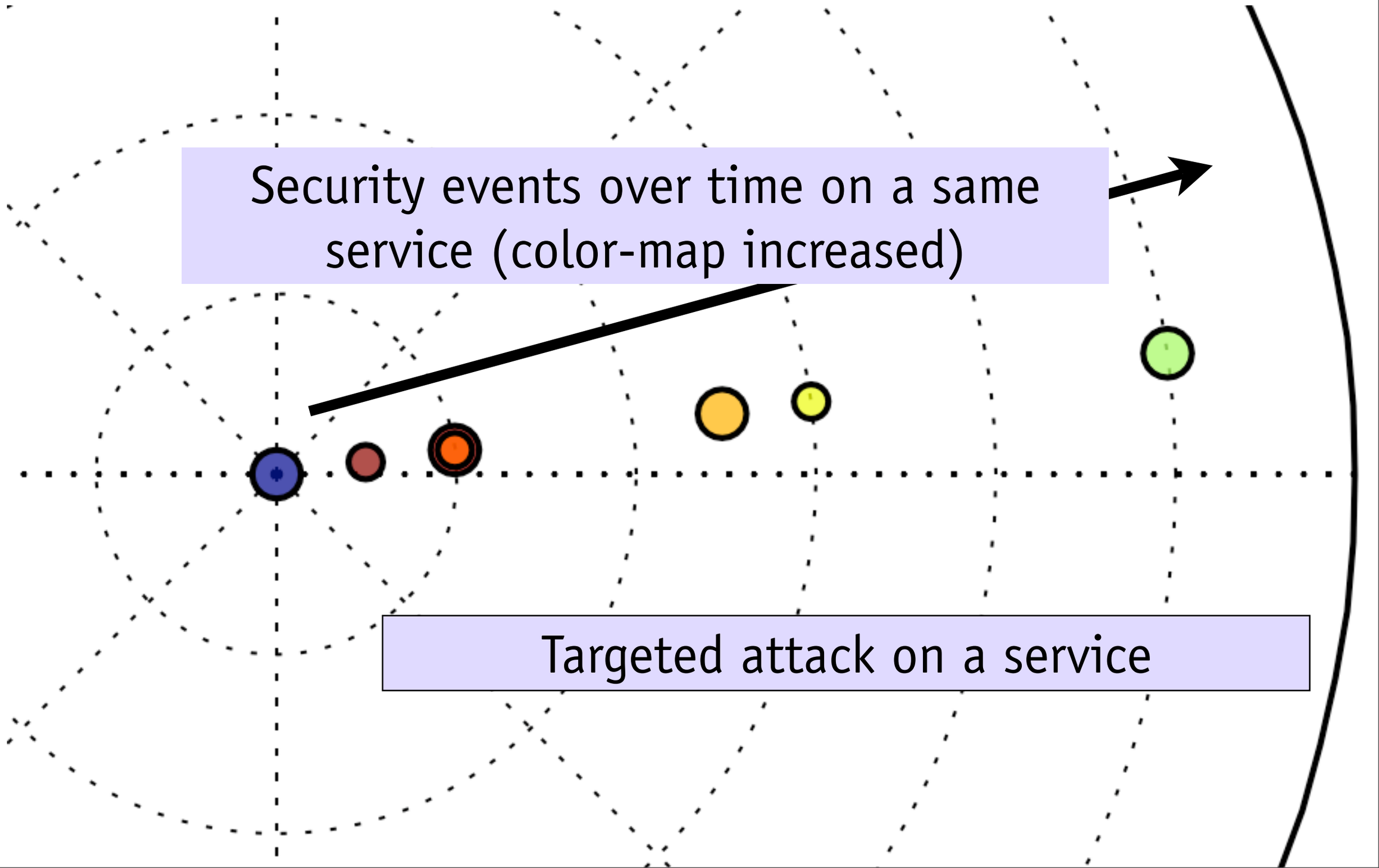
Monitoring

Security Visualization to The Rescue



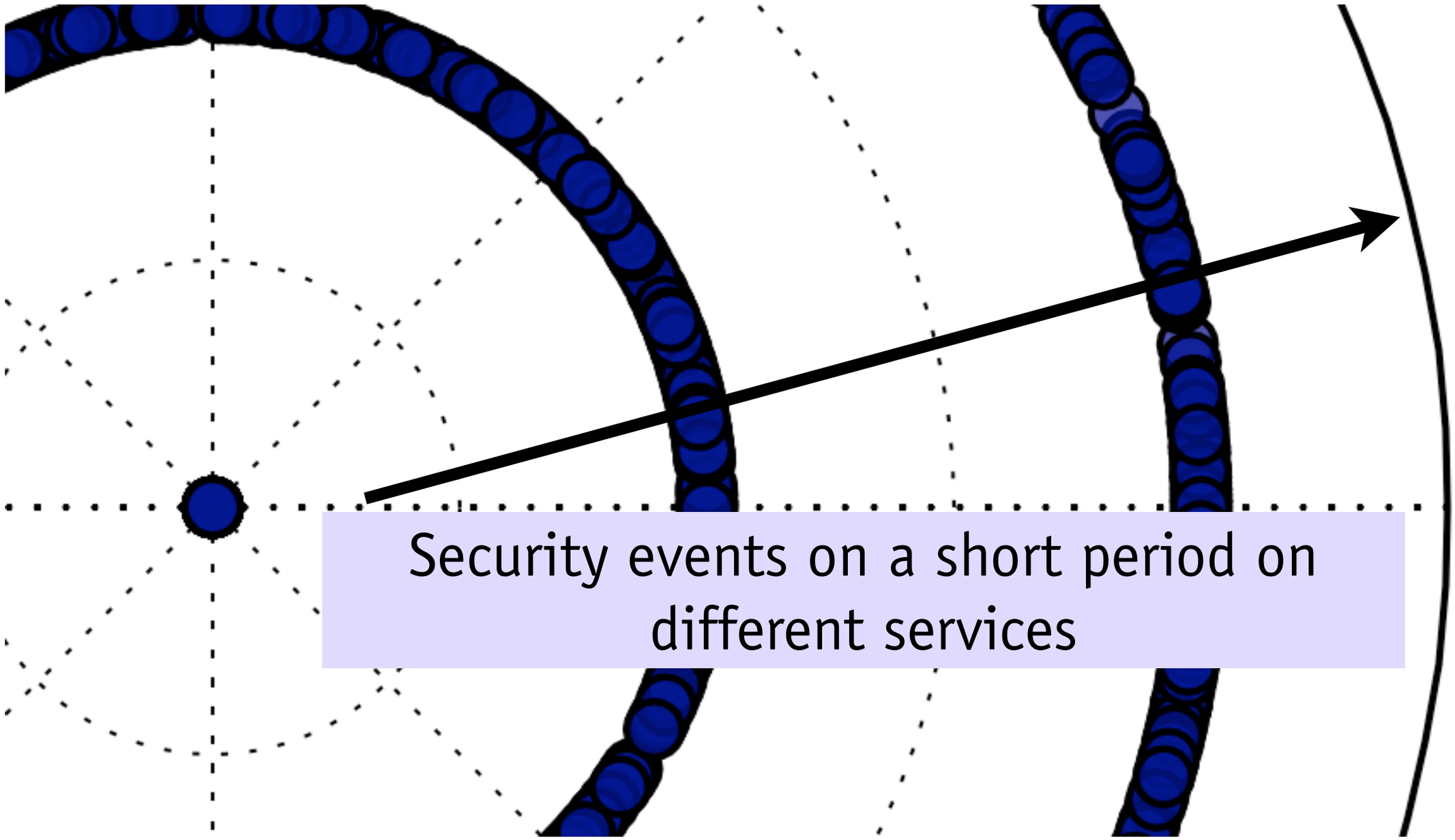
Monitoring

Security Visualization to The Rescue



Monitoring

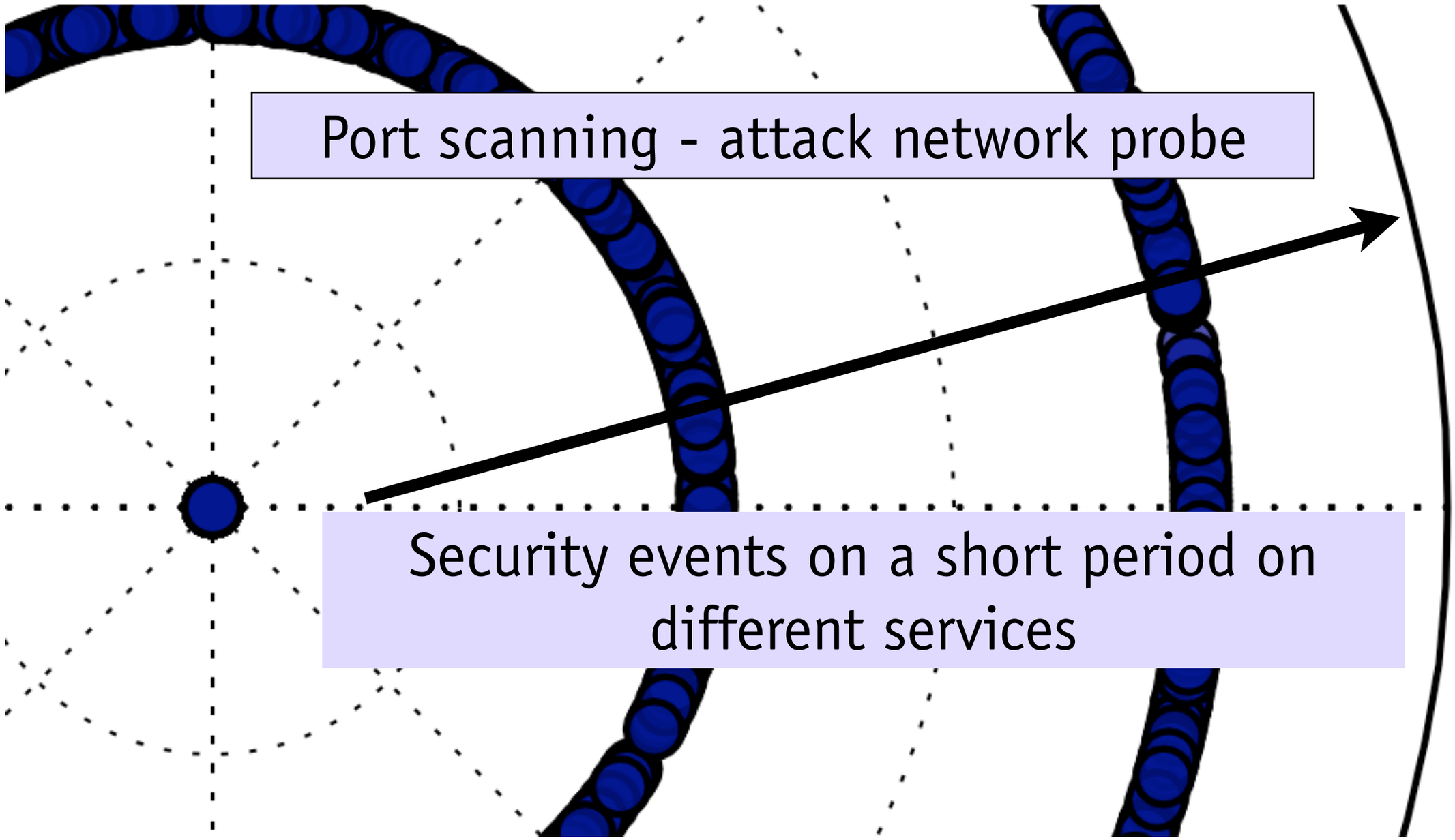
Security Visualization to The Rescue



Security events on a short period on different services

Monitoring

Security Visualization to The Rescue



HoneyBot

Combining Security Visualization and Honeypot Technologies

Increase accessibility of security monitoring

Ease interpretation of security events

Limiting the effect of information overload

Still a research area...

(quick) HoneyBot Dashboard Demo

HoneyBot Sensor Dashboard

Recent Network Security Activities in U-2010/CCPC demo

Overview [toggle]

sensorid	status	overview
2001		
2002		
2003		

HoneyBot Sensor Dashboard

Recent Network Security

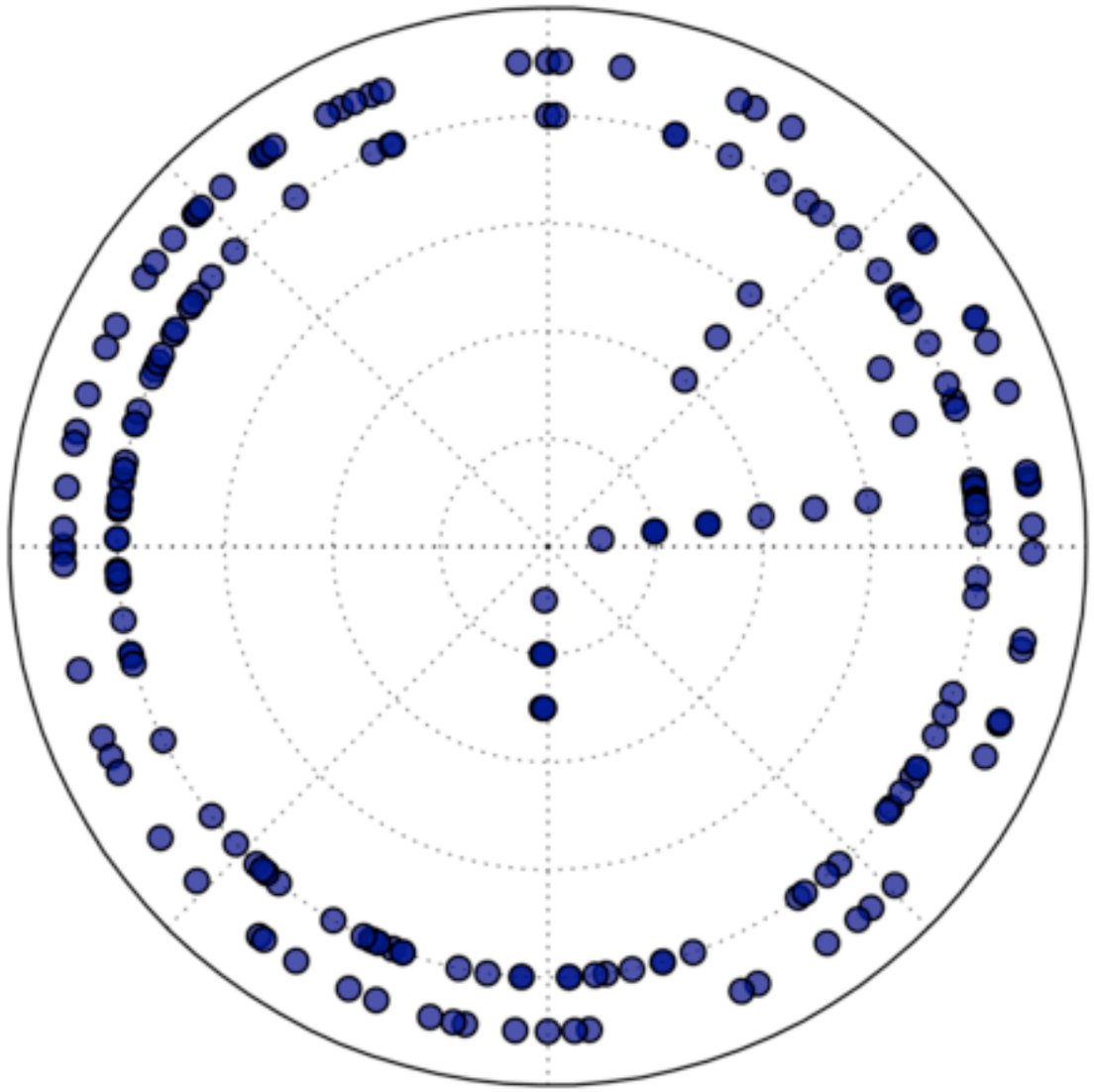
Overview [toggle]

Sensors [toggle]

Events [toggle]

id sensorid

sensor id 2001



CLOSE ✕

Q&A

Thanks for listening

Backup Slides

IPv6 security monitoring

Honeypot/net in IPv6 is challenging especially regarding the space of allocated addresses. In HoneyBot, we designed various “tricks” to overcome such limitation.

- Collecting Neighbor Discovery (RFC2461) messages to view current use of the network space
- Predicting manual IPv6 allocation (e.g. Hamming Distance in IPv6 addresses)

Security of the HoneyBot device

- Low-interaction honeypot (limiting risks of interaction with potential attackers)
- Each HoneyBot device uniquely identified with X.509 certificate
- Solid-state disk (read-only filesystem), privilege separation and non-executable stack