How to securely recover business after a security incident

X-Force IR- Thanassis Diogos
2022-11-03

IBM Security

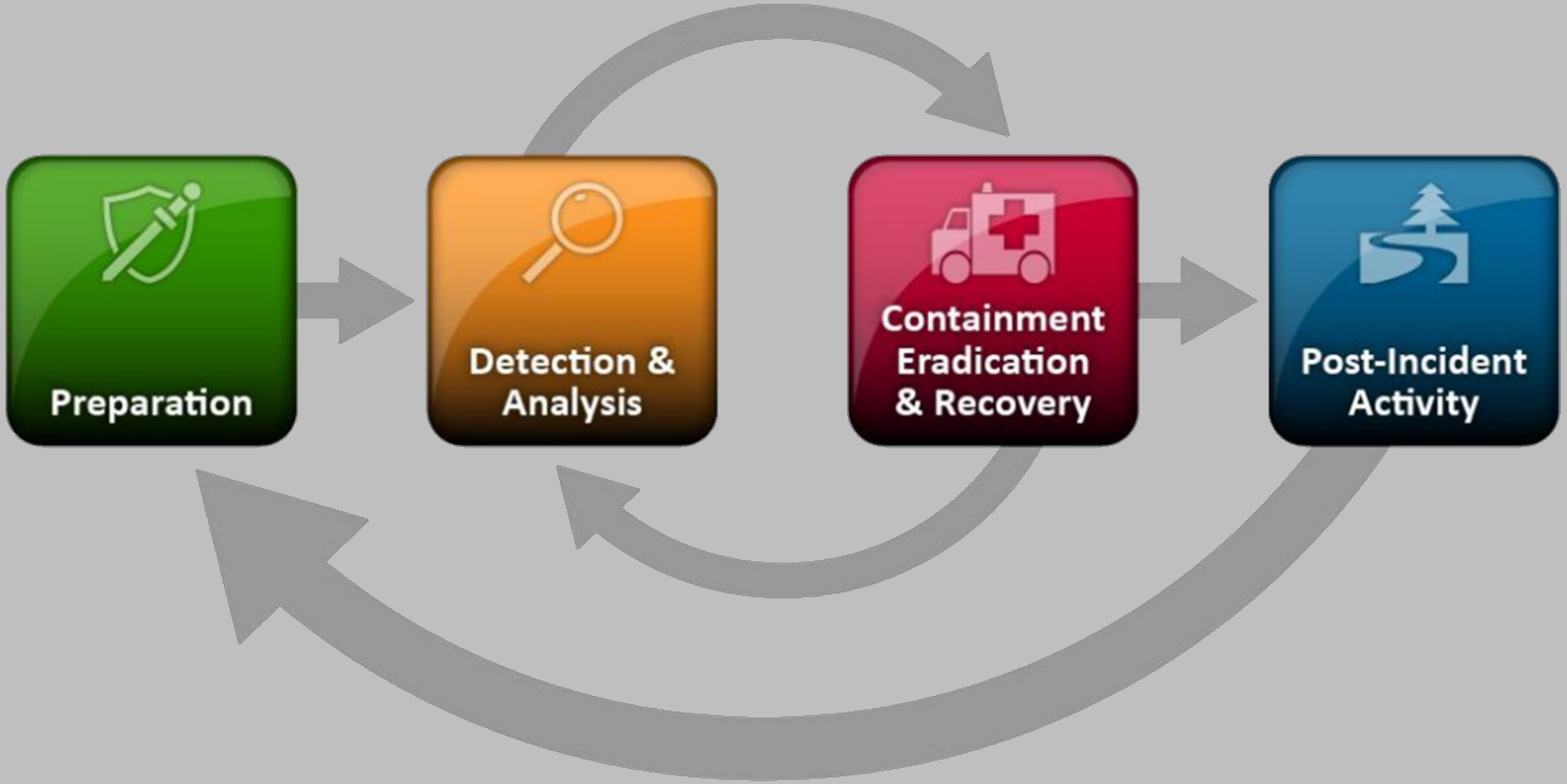
Key learnings

Security breaches and tactical recovery vs business operations.

- Remediation best practices
- Things to avoid
- Post incident reflection

Intro

- ~10 years in IR
- State sponsored cyber attacks
- Wiping incidents (shamoon)
- PCI DSS investigations
- Ransomware cases

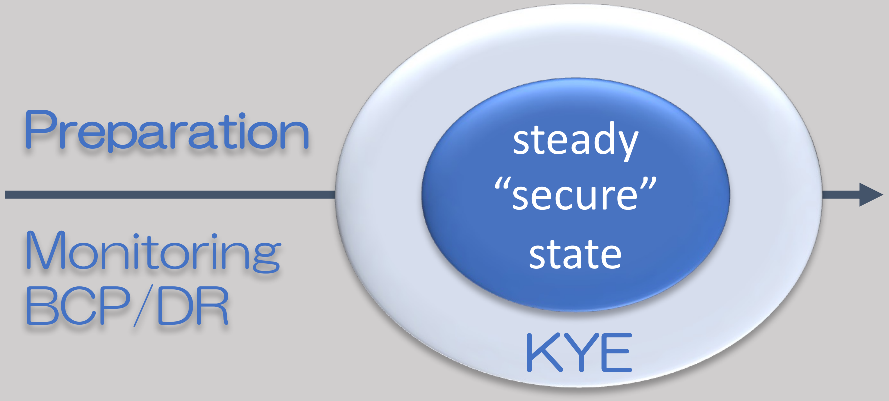


Incident Response

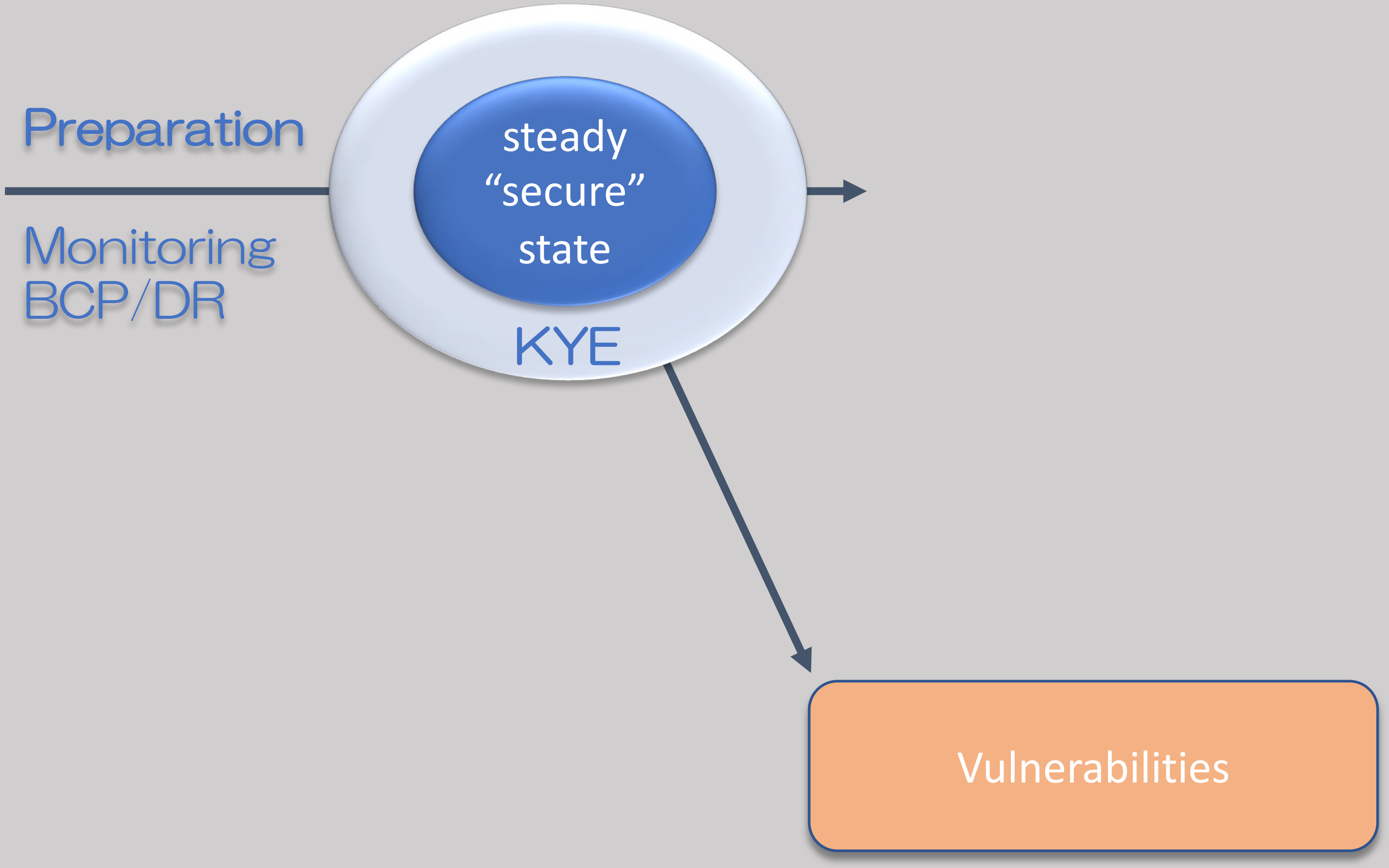
Ongoing state

steady “secure” state

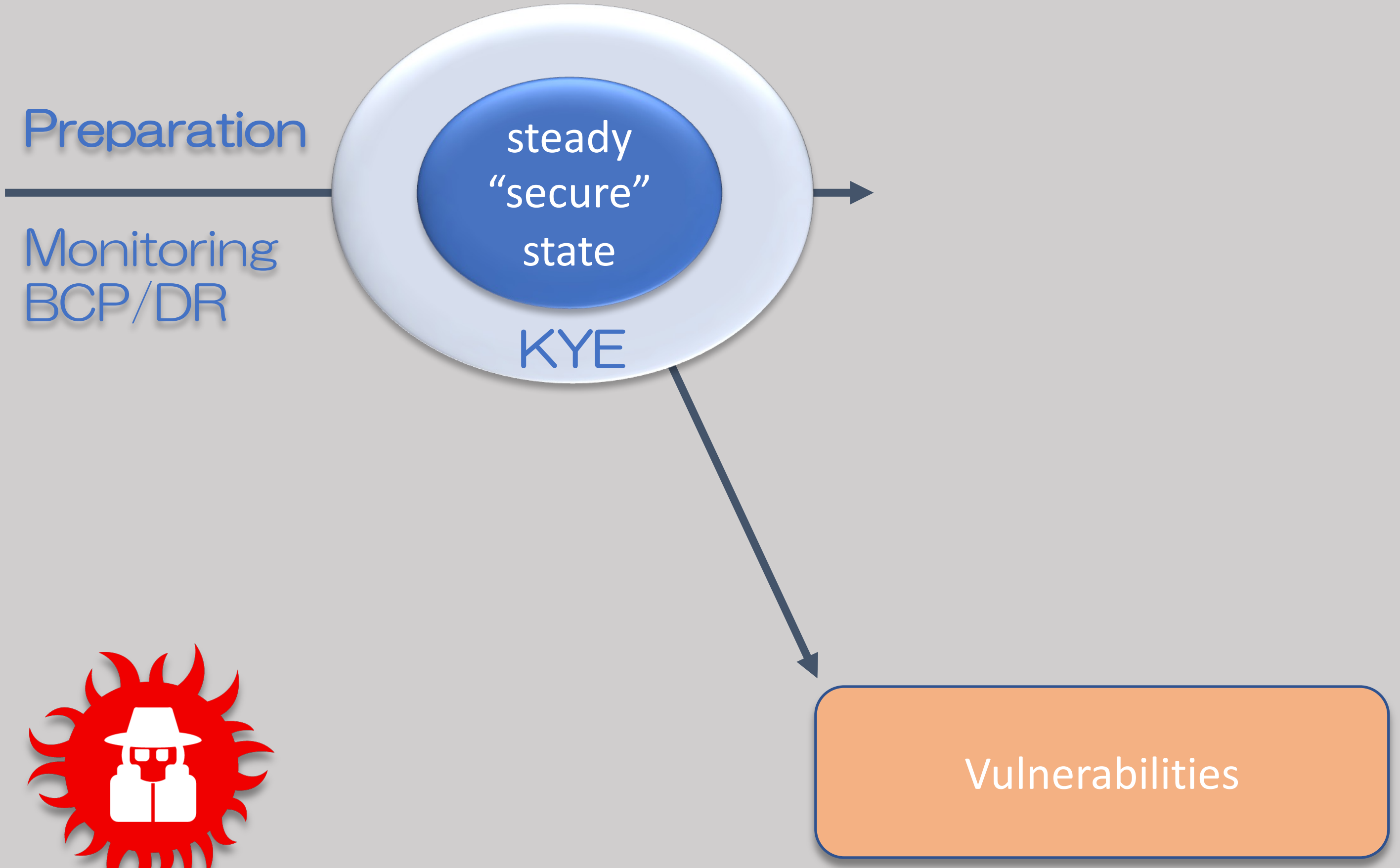
KYE = Know Your Environment



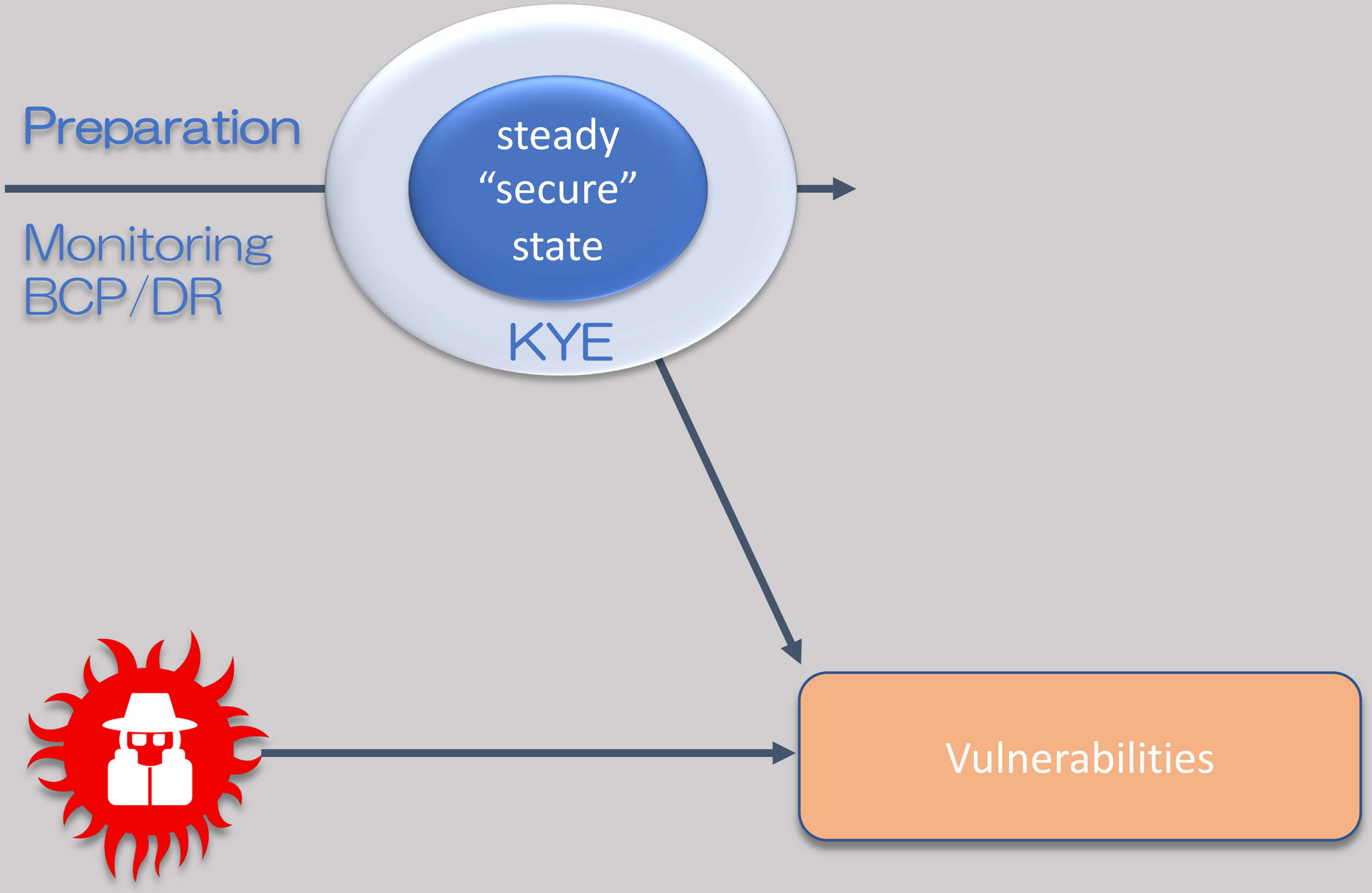
KYE = Know Your Environment



KYE = Know Your Environment
vs
KYE = Know Your Enemy



KYE = Know Your Environment
vs
KYE = Know Your Enemy



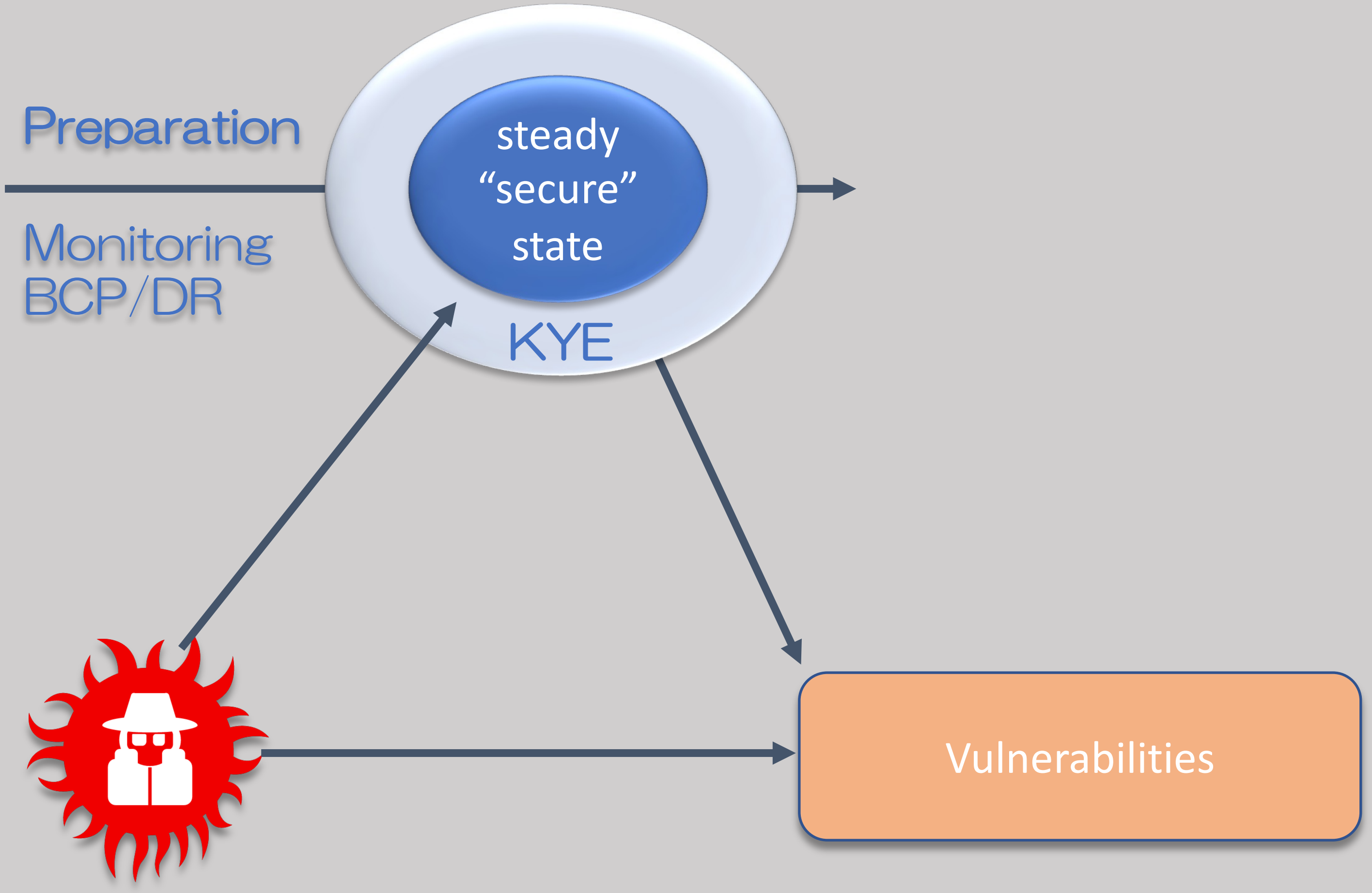
Preparation

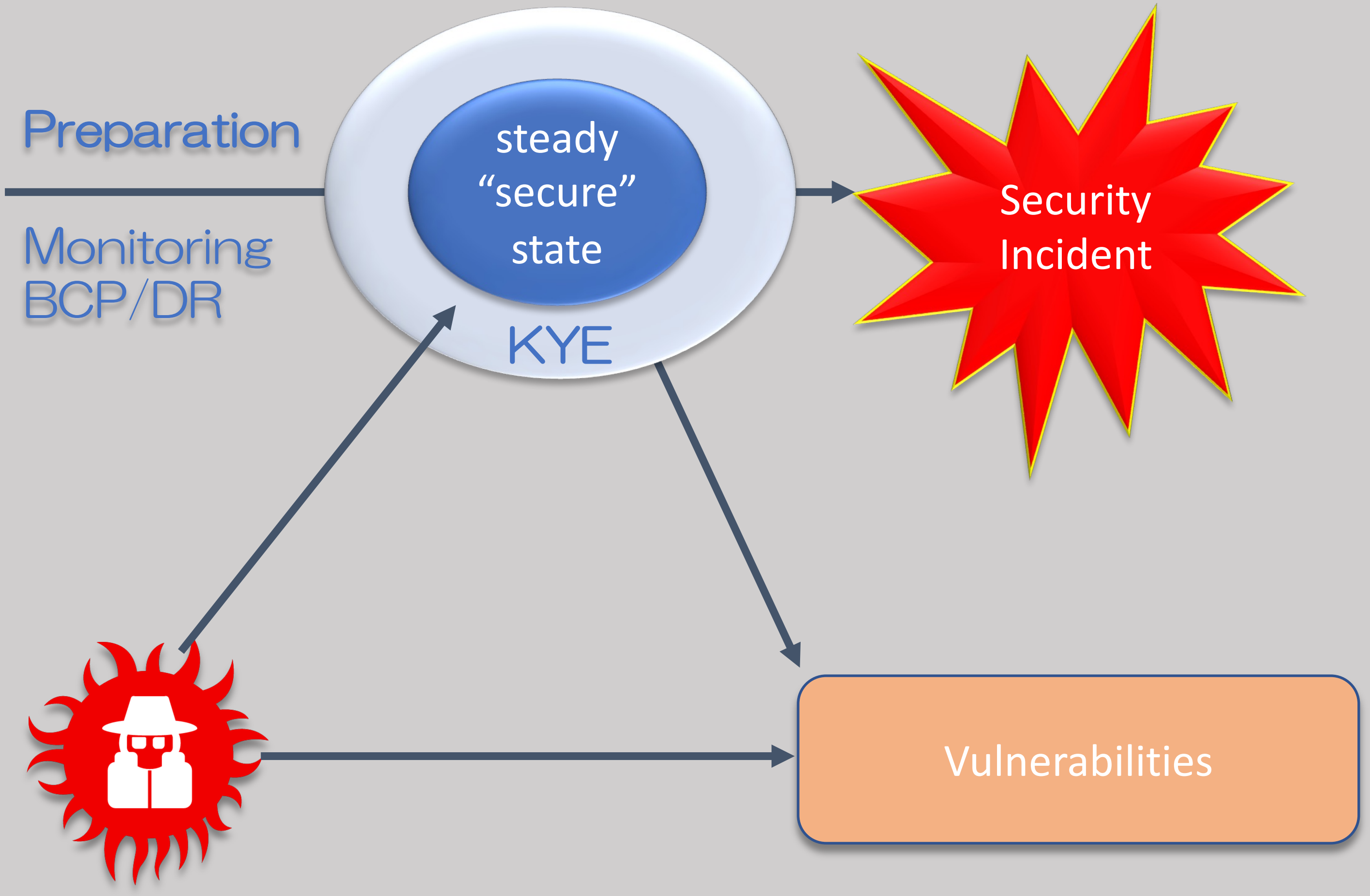
Monitoring
BCP/DR

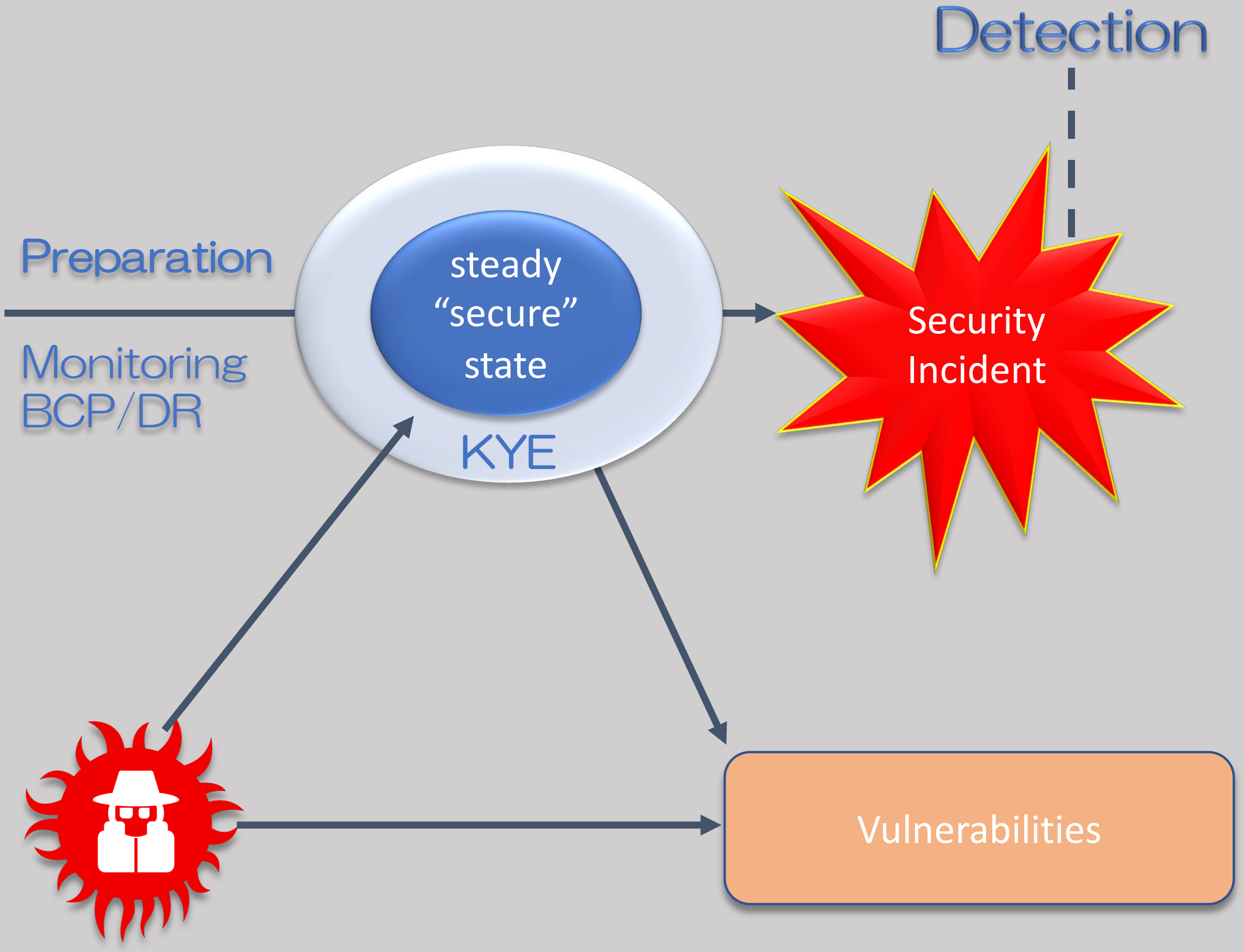
steady
“secure”
state

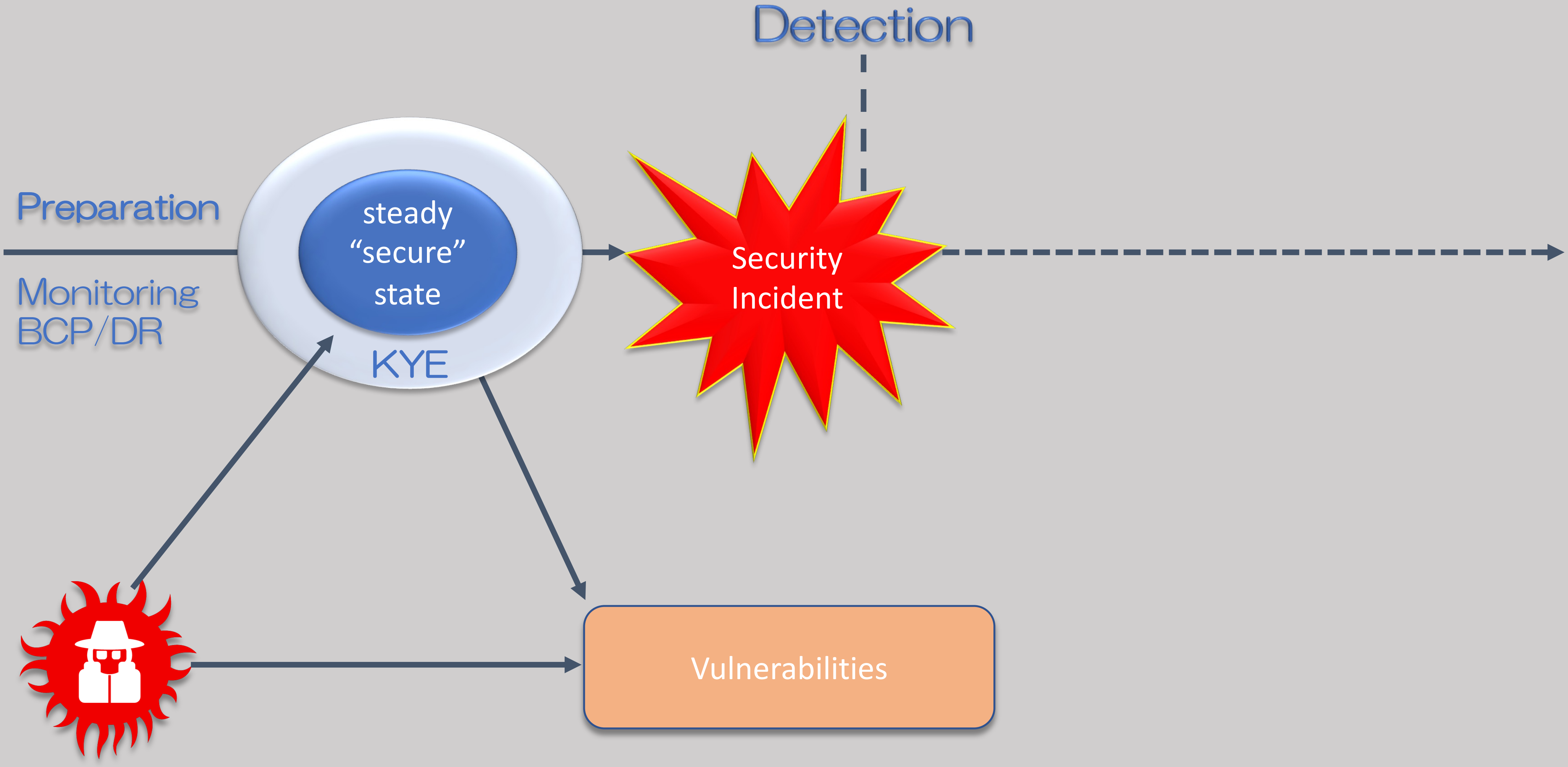
KYE

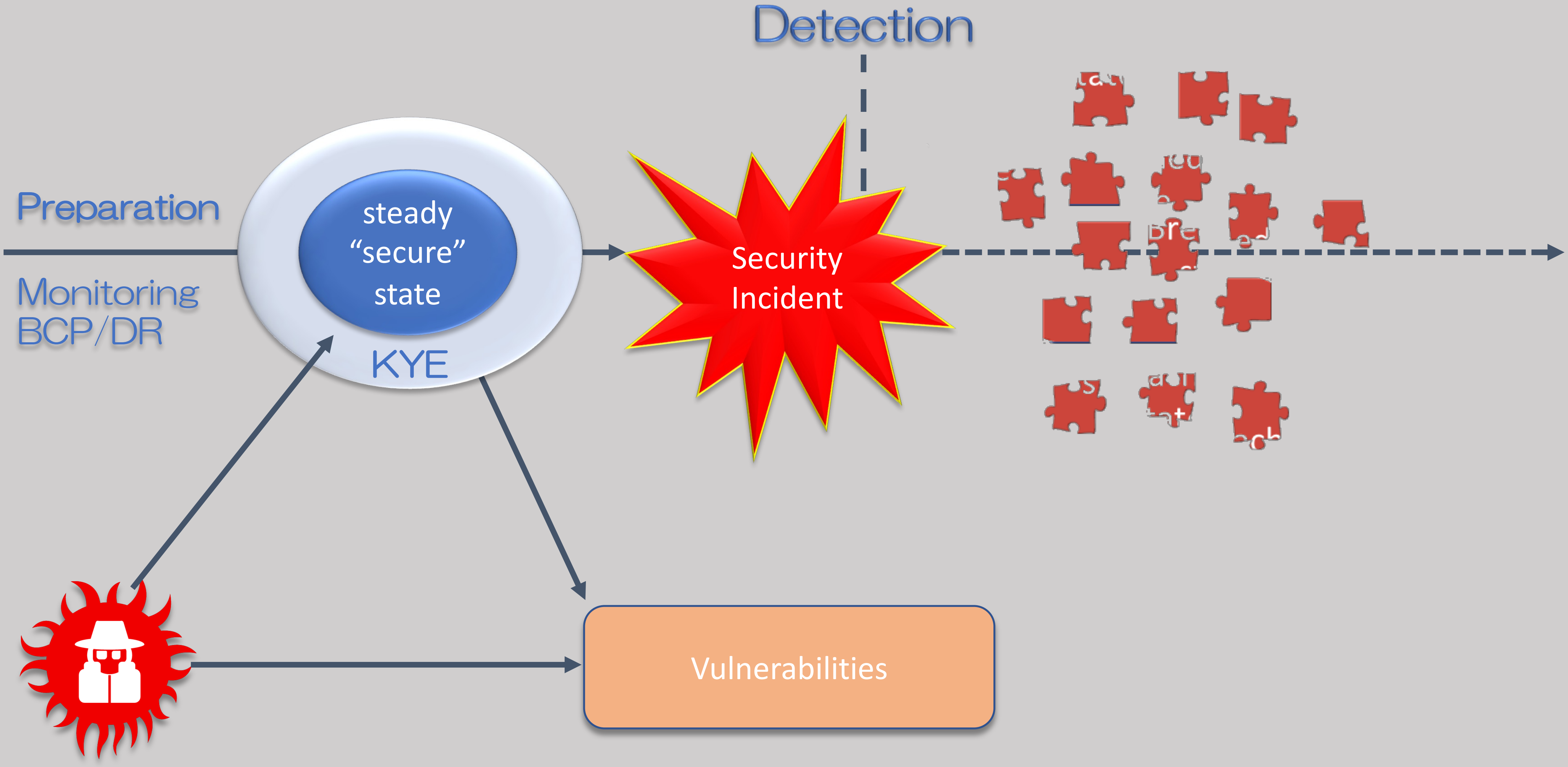
Vulnerabilities


Preparation
Monitoring
BCP/DR
steady
“secure”
state
KYE
Vulnerabilities


Preparation
Monitoring
BCP/DR
steady
“secure”
state
KYE
Security
Incident
Vulnerabilities


Detection
Preparation
steady
“secure”
state
KYE
Security
Incident
Monitoring
BCP/DR
Vulnerabilities


Detection
Preparation
steady
“secure”
state
KYE
Monitoring
BCP/DR
Security
Incident
Vulnerabilities



Detection

Preparation

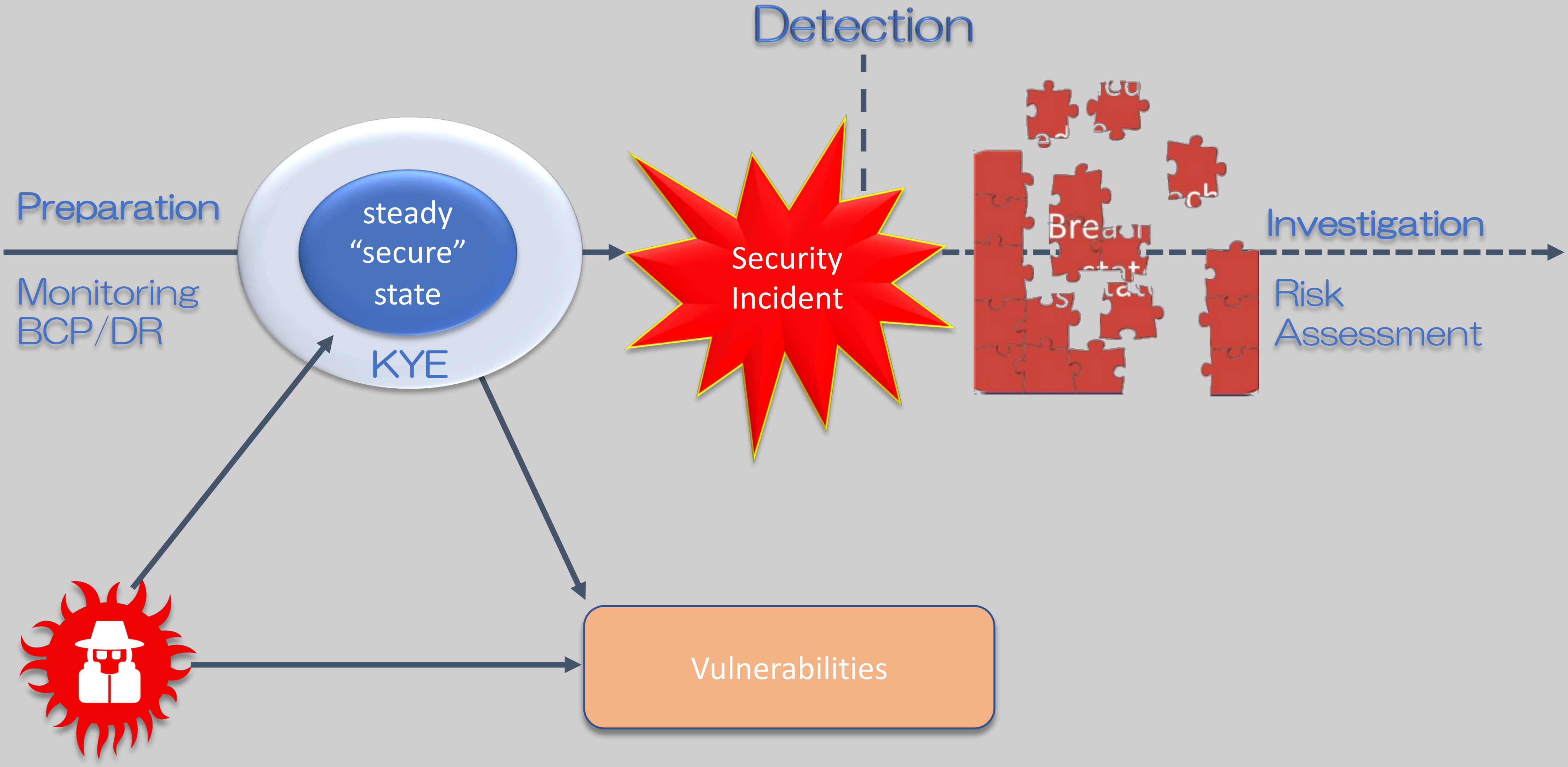
Monitoring
BCP/DR

steady
“secure”
state

KYE

Security
Incident

Vulnerabilities



Detection

Preparation

Monitoring
BCP/DR

steady
“secure”
state

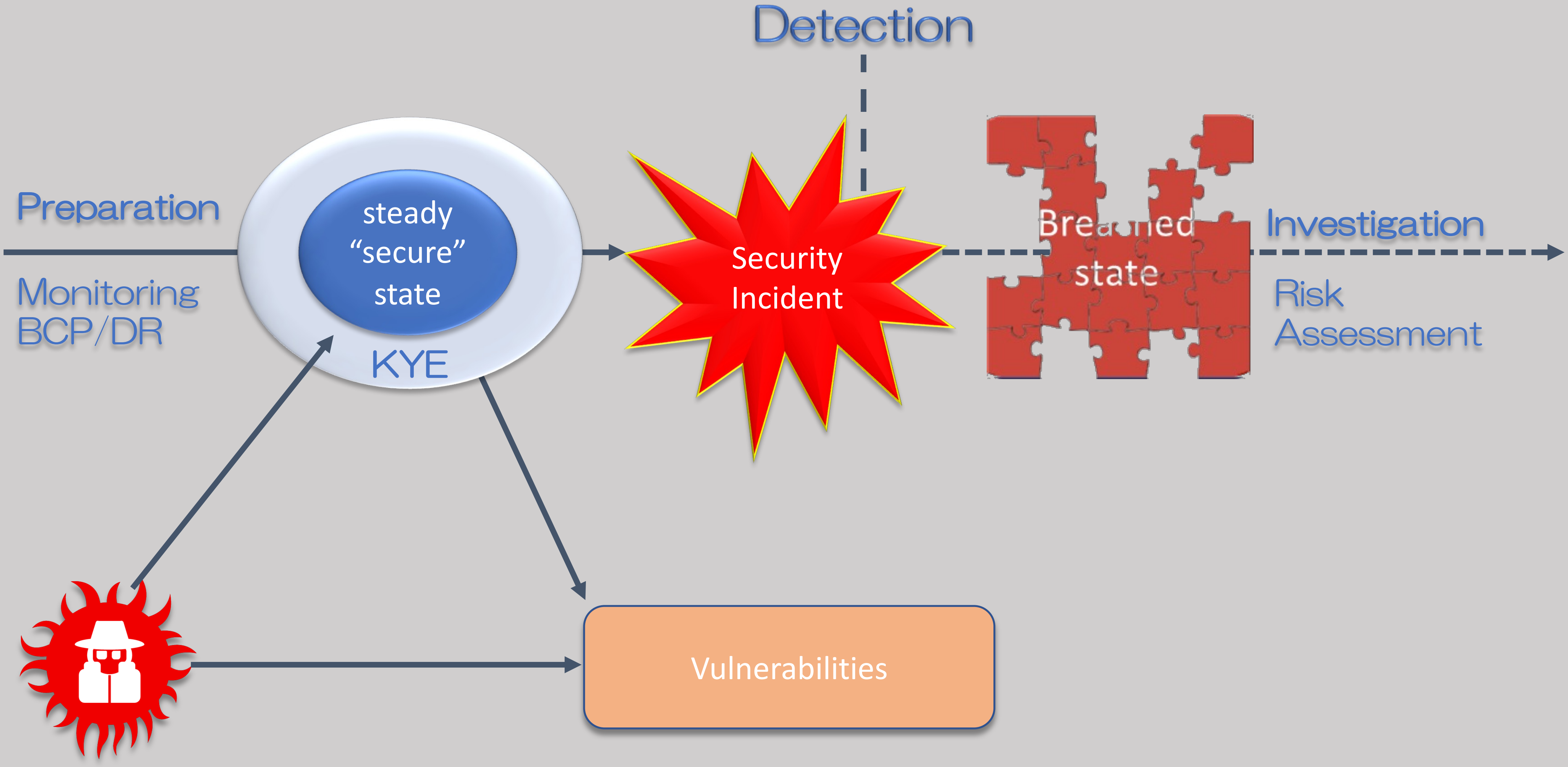
KYE

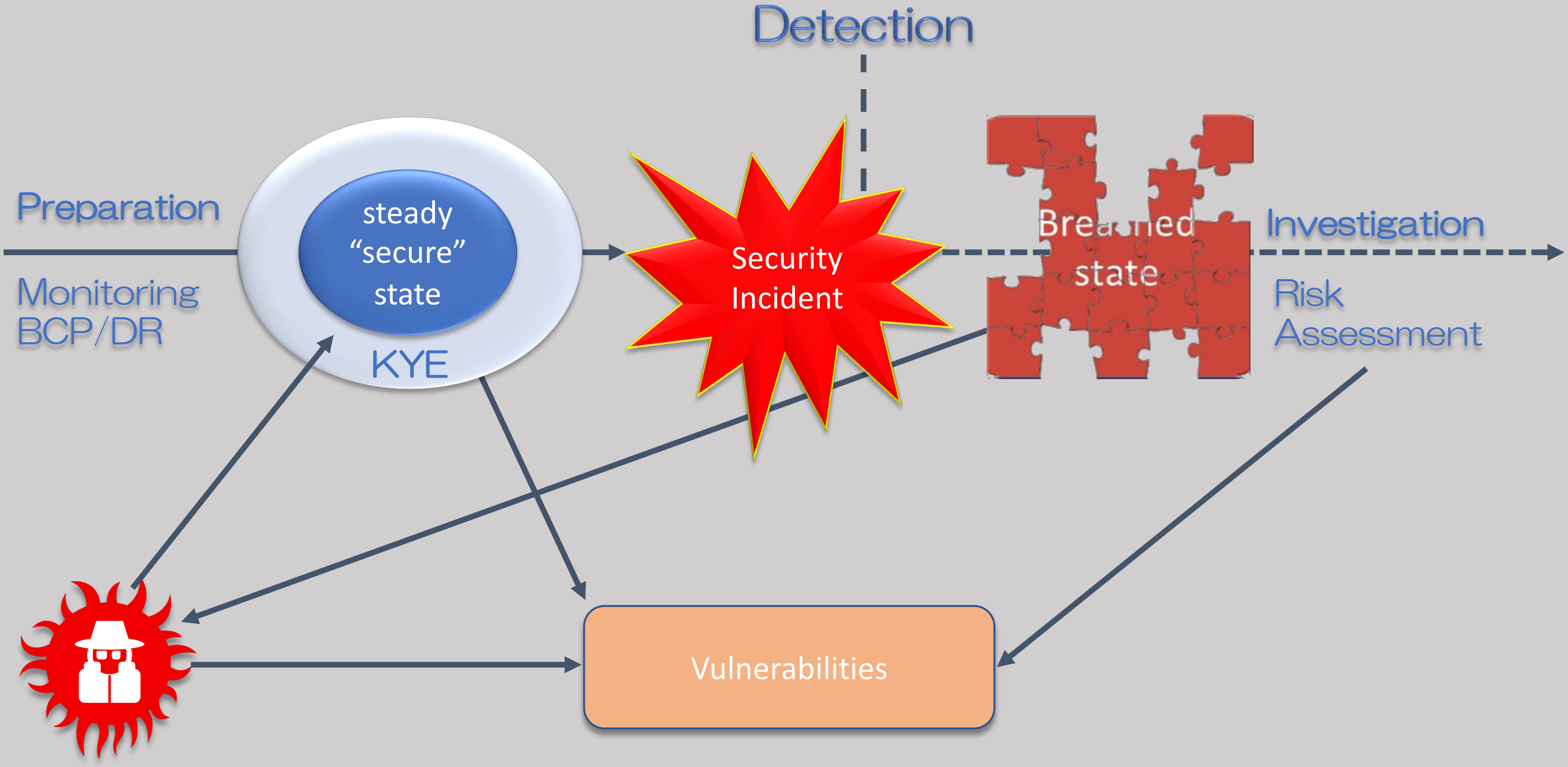
Security
Incident

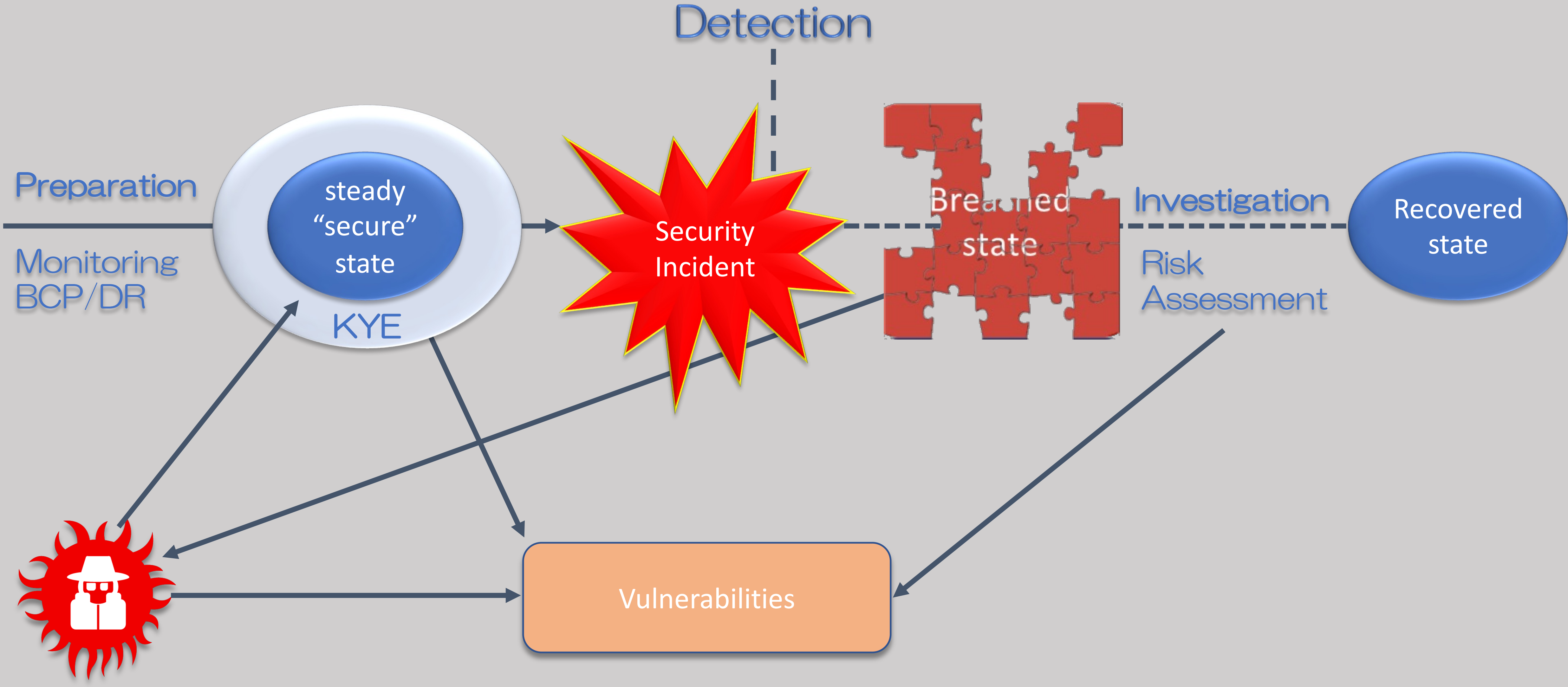
Investigation

Risk
Assessment

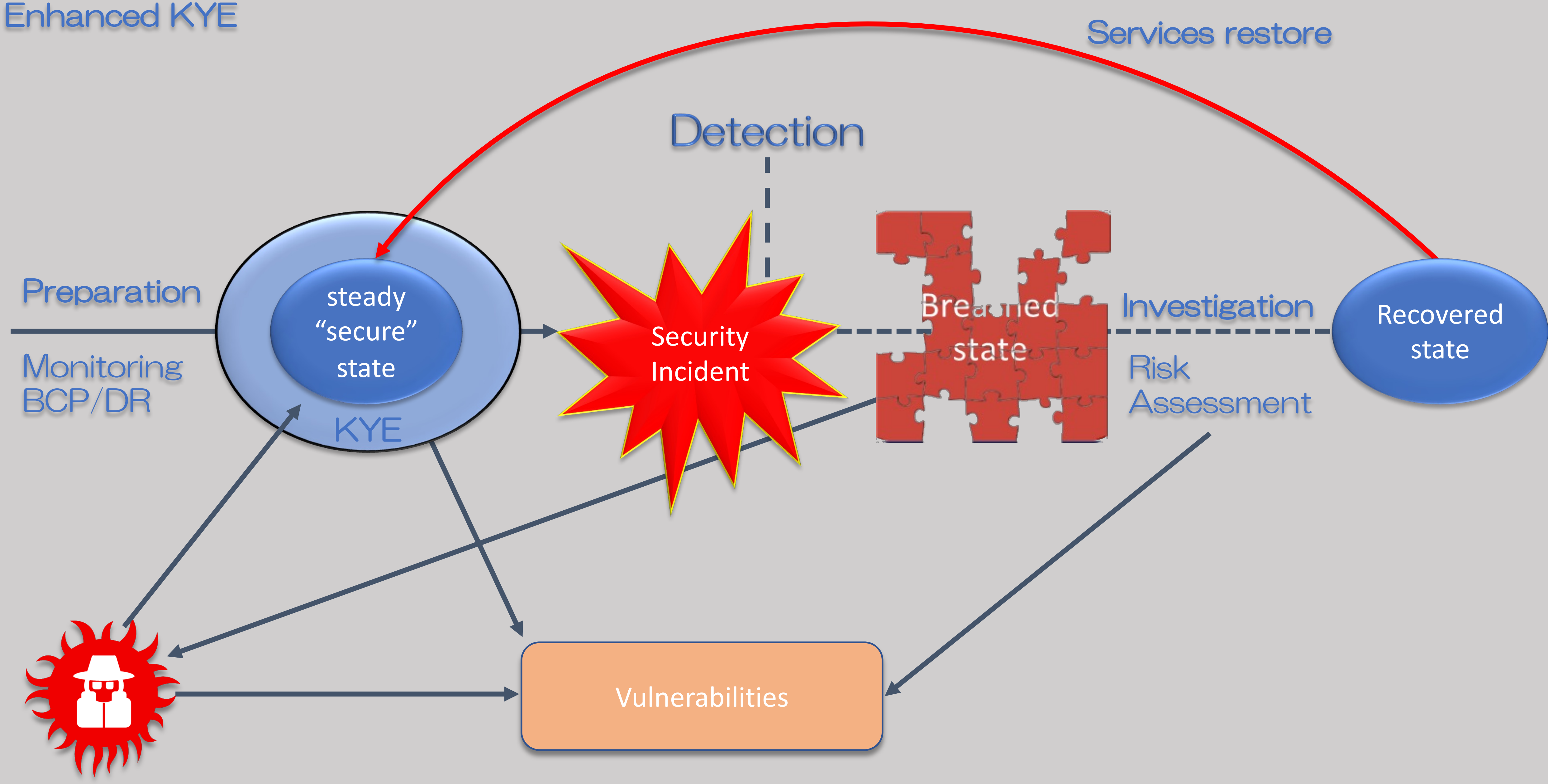
Vulnerabilities


Detection
Preparation
steady
“secure”
state
KYE
Monitoring
BCP/DR
Security
Incident
Breached
state
Investigation
Risk
Assessment
Vulnerabilities


Detection
Preparation
Monitoring
BCP/DR
steady
“secure”
state
KYE
Security
Incident
Breached
state
Investigation
Risk
Assessment
Vulnerabilities


Detection
Preparation
Monitoring
BCP/DR
steady
“secure”
state
KYE
Security
Incident
Breached
state
Investigation
Risk
Assessment
Recovered
state
Vulnerabilities

Enhanced KYE



Services restore

Detection

Preparation

Monitoring
BCP/DR

steady
“secure”
state

KYE

Security
Incident

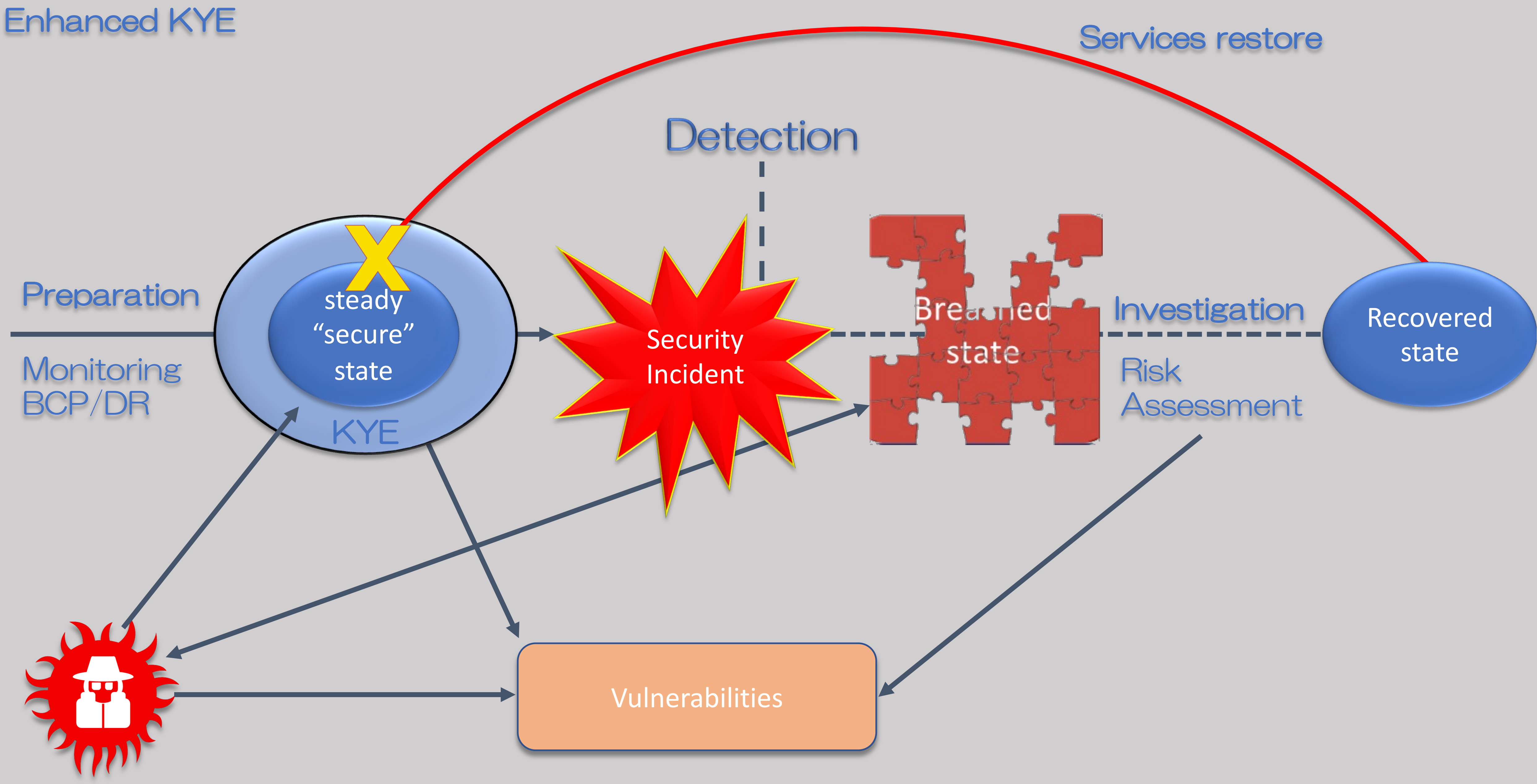
Breached
state

Investigation

Risk
Assessment

Recovered
state

Vulnerabilities


Enhanced KYE
Services restore
Detection
Preparation
steady
“secure”
state
KYE
Monitoring
BCP/DR
Security
Incident
Breached
state
Investigation
Risk
Assessment
Recovered
state
Vulnerabilities

Remediation best practices

- Prepare culture, teams and process
- Keep things simple
- Choose partners early
- Monitor infrastructure with EDR/XDR
- Understand your environment (SIEM)
- Minimize privileged accounts exposure

Things to avoid

- Don’t panic
- React without a plan
- Not blocking/isolating
- Alter evidence
- Unrestricted communication
- Unsecure recovery

Post incident reflection

- Leverage report internally
- Identify gaps in processes, people, tools, partners
- Information sharing
- Learn and apply

Thank you

Follow us on:

ibm.com/security

securityintelligence.com

ibm.com/security/community

xforce.ibmcloud.com

@ibmsecurity

youtube.com/ibmsecurity

www.linkedin.com/in/thanassis-diogos/

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

IBM Security