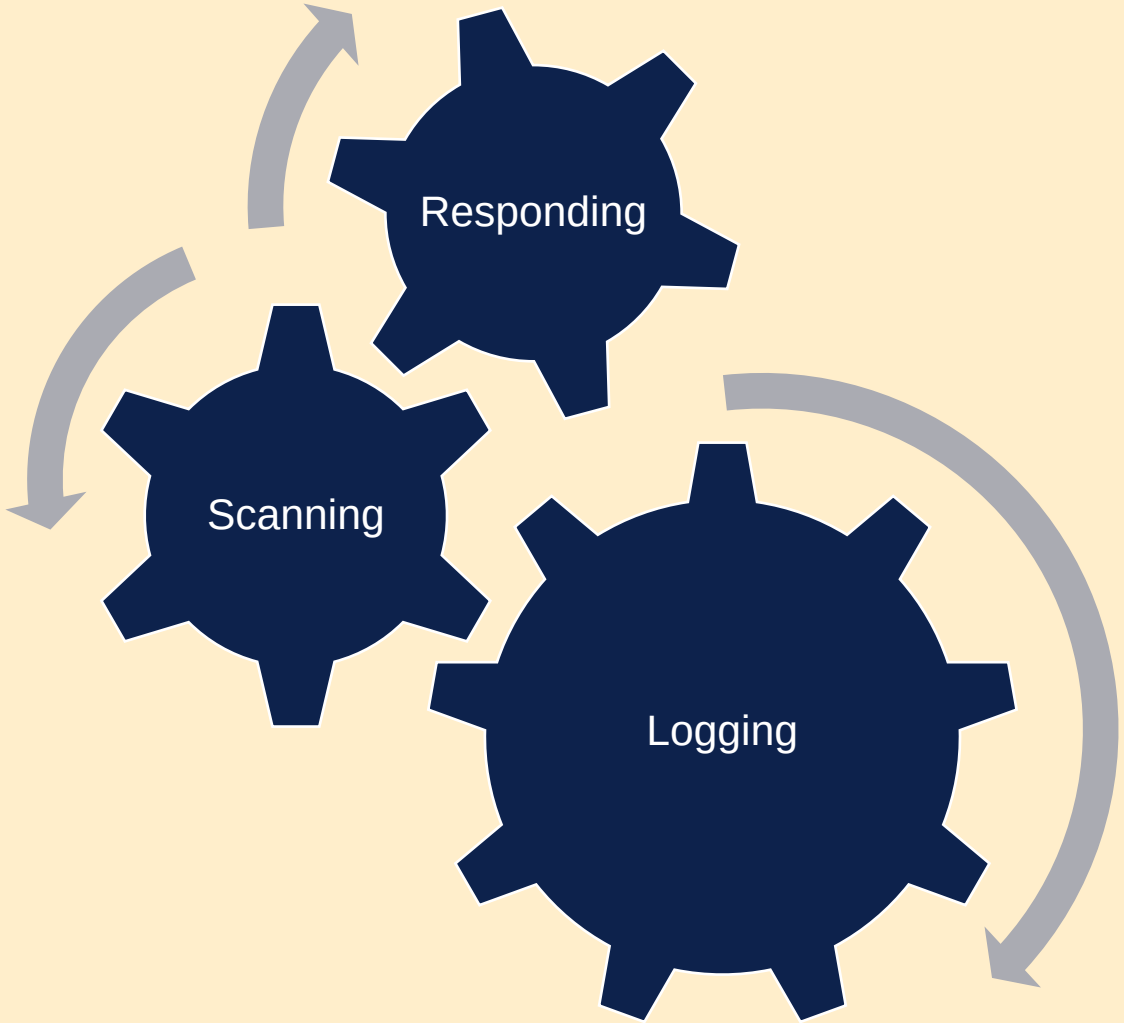
October 2020

Incident Response and the Law

Andrew Cormack, Chief Regulatory Adviser (@Janet_LegReg)


Responding
Scanning
Logging

Logging

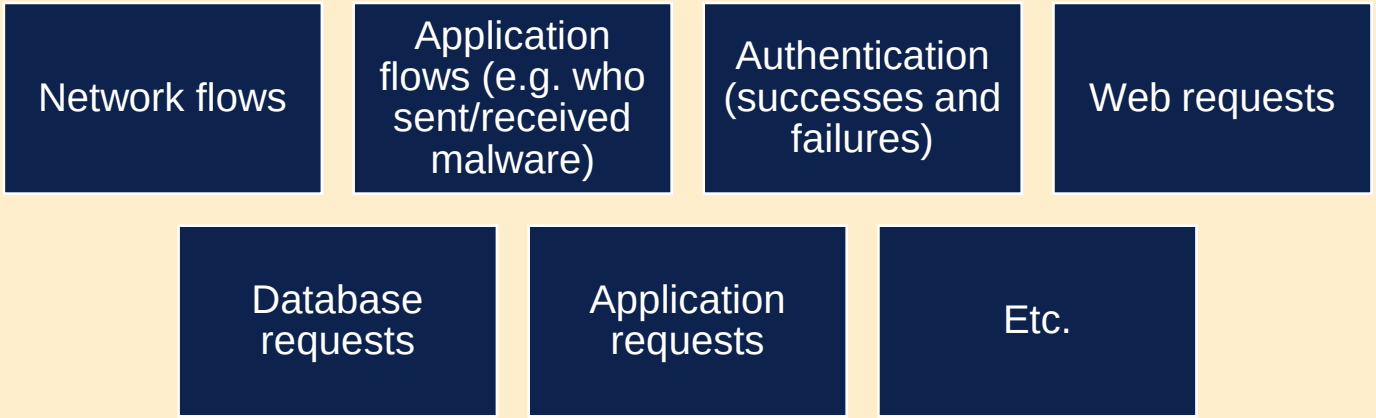
Essential for…

Detection	• Did anything happen?
Investigation	• What happened?
Mitigation	• How to repair it?
Learning	• How to stop it happening again?

Jisc

Logging

Most logs contain (GDPR) personal data



Jisc

Logging

OK (under GDPR Rec.49) to keep these so long as…

They help us detect/respond

and

No less intrusive way to do that

and

Risk of keeping < risk of not keeping

So…

Start from detection/response processes

and

Keep (securely) the logs those may use

and

Delete logs when no longer useful (e.g)

- External changes make investigation impossible
- Lapse of time makes investigation pointless

Jisc

Scanning: Proactive test for vulnerable machines

Scanning

Is this (criminal) “unauthorised access?”

Is it…	
Access?	
Unauthorised?	
With good intention?	

Scanning

Is this (criminal) “unauthorised access?”

Is it…	UK Computer Misuse Act 1990
Access?	Yes: Anything that prompts a response is “access”
Unauthorised?	Not defined, but UK law recognises both explicit (e.g. by contract/policy) and implicit (e.g. by action) authorisation.
With good intention?	Irrelevant

- Limited case law suggests
  - “in-protocol” scans (e.g. SYN/ACK or banner grabbing): should be OK
  - Active exploits: probably not OK
  - Scans that may crash target: probably not OK

Jisc

Incident Response

Investigation

Again: “least intrusive that will achieve purpose”

Focus on malicious/unknown activity

Automate that selection where possible

Avoid linking to humans if you can

- Machine identifiers are preferable

Identify *victims* when you know they need help

Keep identification of *attackers* (“attribution”) separate

- Legal provisions are very different

Jisc

Notification/Sharing

Again: “risk of sharing < risk of not sharing”

Informing victims (internal and external – to mitigate/remediate)

- Send only the information they need to help themselves
- Keep distribution small/effective (victim, org…)

Informing peers (mostly external – to prevent/detect)

- Send only the information they need to help themselves
- Use trusted communities if possible

Would this help attacker more than defender?

Jisc