red canary

How do you define the severity of an incident?

LET'S TAKE A CLOSER LOOK →

SEV-4

Initiate response within two hours

Issues requiring triage
(not immediate attention)

SEV-3

Initiate response within five minutes

Issues preventing one or more customers from utilizing services **or** security misconfiguration without evidence of exploitation **or** commodity malware isolated to a single host/endpoint

SEV-2

Initiate response immediately

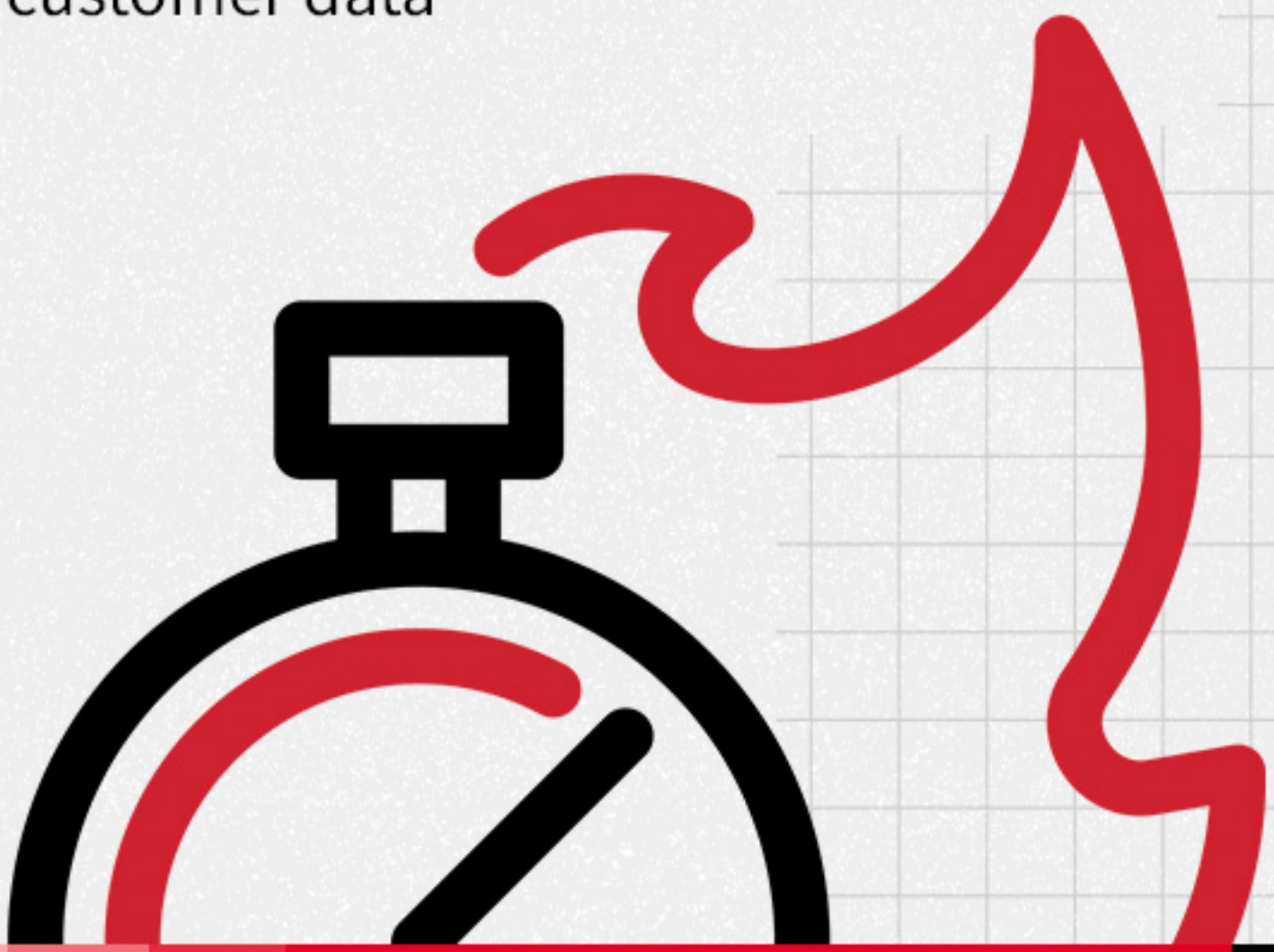
Suspected exploitation of security misconfiguration/vulnerability **or** exposure of sensitive customer data **or** sweeping malware infection involving multiple hosts

4 3 SEV-2 1

SEV-1

Initiate response immediately

Critical system failure preventing multiple customers from accessing services beyond acceptable downtime **or** widespread exposure of sensitive customer data



4 3 2 **SEV-1**