Article

[On the fourth day of Techmas Waterstons gave to me…](#)

Breadcrumb

1. [Home](#) /
2. Print /
3. Pdf /
4. Node /
5. [Entity Print](#)

Insight navigation

- [Latest insights](#)
- [Latest news](#)
- [Articles](#)
- [Case studies](#)

[Download PDF](#)

Dec 2022

On the fourth day of Techmas Waterstons gave to me…

Threat from human actors

Categories Cyber Resilience

Dec 2022

-
-
-
-

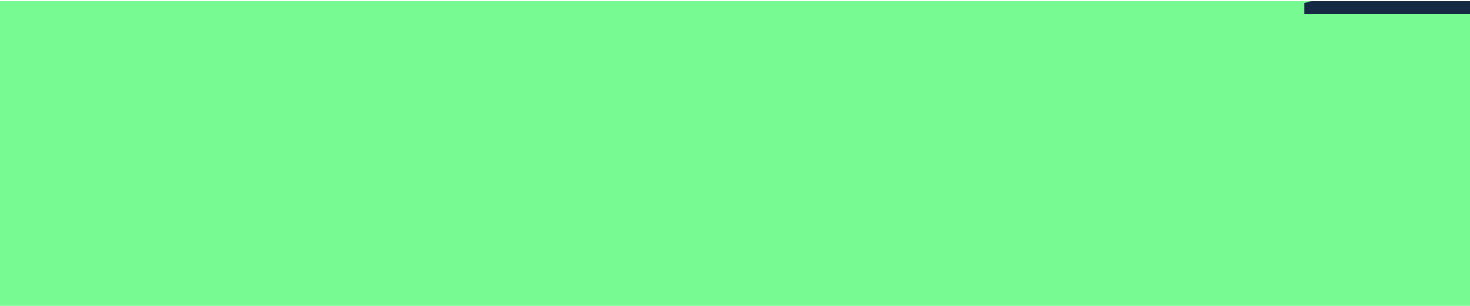### [Andrew Quinn](#)

Technical Strategy Lead

Email

andrew.quinn@waterstons.com

Once upon a time, we were afraid of viruses disrupting our systems.

Then, years* later, it was autonomous ransomware.

These days, it's increasingly common for human actors to pay an active part in security breaches.

Unfortunately, you won't have Jennifer Aniston, Tom Hanks or Leonardo DiCaprio hacking your systems (we hope), rather a *threat* actor is a person or a group of people that take part in an action that is intended to cause harm to the cyber realm including computers, devices, systems, or networks.

Instead of simply blind-firing malware at your network, they establish persistent access and perform detailed reconnaissance to understand your systems and data before launching a highly targeted attack.

Anti-virus doesn't cut it anymore, because it doesn't work on humans, instead we must look to EDR/XDR (E = Endpoint, X = eXtended Detection & Response) solutions that are tuned to detect suspicious activity and feed telemetry to your security team.

While it's tempting to say "EDR is the new anti-virus", EDR (and XDR in particular) requires more expertise to manage and interpret, so it is often paired with a security service from a trusted partner. Because security people love their acronyms this managed service may also be labelled MDR.

For support in protecting your systems and devices from these pesky ~~Oscar winners~~ threat actors, get in touch with our team of [cyber security experts](#) who can develop a bespoke solution just for you.

*maybe not years but go with the story telling theme