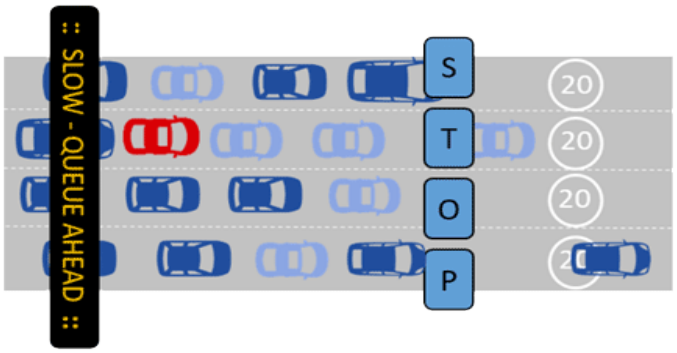
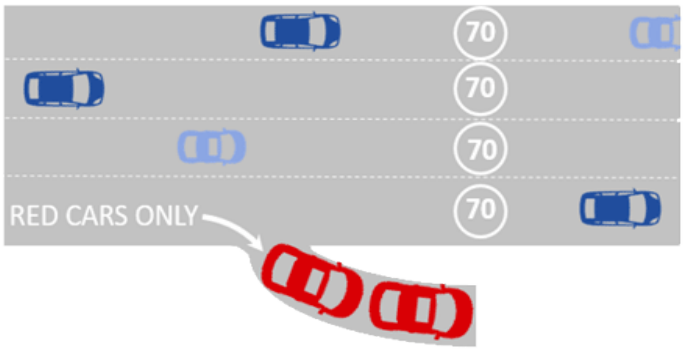
FIELD CAPTURE (FCAP)

You are looking for someone with brown hair, wearing a white T-shirt, last seen in a red car.

Do you stop all cars to look at every single passenger, or just the red cars?





Effective cyber threat detection involves locating the tiniest of signals indicating malicious behaviour. In a network, these signals become lost in Terabytes of background noise. So, companies invest $millions in machine learning to sift the signal from this noise. Botprobe takes a different approach. Rather than look inside every car, we only look inside the red cars.

Finding malicious threats involves analysing data for *Indicators of Compromise*. These IOCs (brown hair, white T-shirt) differ between attack type or variant. Yet core fields vary little across most threats. Take, for example, the 10,000s of rules in a modern Intrusion Detection System. The number of different data fields used by these rules is very few.

Botprobe has developed Field Capture (FCAP). Powerful AI-driven data capture algorithms that extract only IOCs needed for threat detection.

FCAP dynamically alters which IOC fields are captured, adapting as a threat profile evolves.

Adaptive FCAP has several advantages:

- Data volumes can be reduced by over 90%
- Less data needs transporting to a SOC
- Captured data is clean and structured
- SIEMs can ingest network traffic

Our adaptive field capture probes are suited to working in challenging environments. Such as high-speed Internet Provider backbones. Or capturing data on home networks that have low-speed internet connections.

Reducing the volumes of captured data means our probes can run on low power hardware. So scaling our technology over large estates is cost-effective. With fewer data points to analyse, our threat analysis tools are faster, more efficient and smarter.

To learn more about our technology, visit www.botprobe.co.uk/technology