

More Information

Capabilities not covered

Elastic Fleets and Agents

<https://www.elastic.co/guide/en/fleet/current/fleet-overview.html> Capability 2 covered

Winlogbeat

https://www.elastic.co/guide/en/beats/winlogbeat/current/_winlogbeat_overview.html

Related Information

Written Information on Packetbeat

<https://www.pluralsight.com/guides/setup-dns-traffic-event-monitoring-elasticsearch-siem>

List of subjects in the area

- Windows & Linux Setup
- Detailed Config Review
- More Technical References



Thank you!

LinkedIn: <https://www.linkedin.com/in/owendubiel66/>

Twitter: @Protect_Data66

