

https://prezi.com/k_tnpyseherj/siem-summit-2017-actionable-detects/

//wiki.sans.blue

//cyber.gd/seth_prezis

Actionable Detects

Blue Team Tactics

Seth Misenaar GSE #28

Response-Based

Incident Response
AuthN/AuthZ
Censorship
Trust

