category	sub-category	evidence	author	pages
communities	attackers	"... increasingly sophisticated technical and social attacks from organized criminal operations"	D'Amico	19
data	external	"information published on hacker websites"	D'Amico	29
data	processed	"incident report, intrusion set, problem set from other organizations, information about the source and or sponsor of attack" & "incident reports are [often] textual documents"	D'Amico	35
data	raw	"network packet traffic, netflow data or host-based log data"	D'Amico	25
design guidelines	tutorial	"tutorial on how to get started; not just the user's manual .... certification process so people can become certified"	Erbacher	212
design guidelines	uncertainty visualization	"visualization should have a weight based on the accuracy of info" & "force-directed graphs where trust is the primary spring force"	Erbacher	210,212
other	metaphor	"Cyber security is essentially a human-on-human adversarial game played out by automated avatars. "	Fink	46
phases	situational awareness	"During the first stage, a CND analyst acquires data about the monitored environment, which is typical of the perceptual stage of situation awareness."	D'Amico	32
responsibilities	communication	"importance of analyst communication in the data transformation"	D'Amico	30
roles	managers	"most were active analysts; a few were managers"	D'Amico	23
roles	network analyst	"computer network defense (CND) analysts"	D'Amico	19
workflows	investigate	"If a vulnerability scan returned a suspect IP address, he would then have to go through several different tools in different windows to get information about the IP, such as the host name, its location in the network or building, its OS version and update status, its owner, and the owner's phone number."	Fink	49