

Wednesday, February 13, 2019

3:10 p.m. – 3:30 p.m.

Determining Evil from Benign in the Normally Abnormal World of InfoSec

Rick McElroy

Head of Security Strategy

Carbon Black

Abstract: Have you ever been positive you had found evil only to realize it was normal after hours of triage and work? We have all heard and love “KNOW NORMAL FIND EVIL” but how hard is it to actually know normal? The MITRE ATT&CK Framework gives defenders a better map to “find evil” but how can this Framework be used to “know normal”? Join Carbon Black’s Head of Security Strategy, Rick McElroy, as we discuss how knowing normal in a world of abnormal is harder than one thinks and how addressing the actual root cause of evil can improve the technology industry as a whole.