

GRR

GRR (GRR Rapid Response) är ett agent-baserat IRT-verktyg, för live forensic på klienterna som kör GRR-agenten.

SUNET använder det själva på en delmängd av framförallt servrar som har tjänster på sig med upptidskrav, samt mycket disk och minne, vilket gör det svårt att överföra data för analys på sidan av.

SUNET CERT har en instans för interna system samt för att kunna bistå andra med att hitta "artifacter" utan att behöva vara på plats.