	Immediate Alert Investigation	Breach Investigation	Skills Required	Time to Resolution	Risk Reduction
Network Detection Tools (i.e Darktrace)	• Limited packet information • Filtered/alert-based packet capture • Manual investigation	• Packet information is very limited • No content visibility	• Suitable only for experienced security users • Requires deep network skills	• Time to resolve is long due to limited information available	• Not enough visibility to reduce risk
Full Packet Capture Tools (i.e RSA Netwitness)	• Captures all traffic - but only for a few days • Missing correlations • Manual investigation	• Short term visibility • Huge storage requirements • Slow performance	• Very experienced users • Requires extensive network and security knowledge	Long: • Large amount of data to go through • Expertise required	• Only for investigating few days • Not quick enough • No context visibility into breaches
SIEM (i.e Splunk)	• Missing network visibility • Only Metadata information	• Limited view – used mainly to prioritize what to investigate • Not an investigation tool	• Requires Level 3 analysts • Limited visibility because of missing network payloads	• Long: • limited data available • Expertise required	• Required as compliance • Not enough visibility to reduce risk
WireX Systems	• Contextual analytics • automating investigation process • Fast retrieval	• Contextual analytics visualization • In-depth content visibility available for months	• Eliminates skillset barriers • Can be used by entry level personnel	Fast: • Automated contextual analytics • Built-in investigation process	• Reduces risk and impact of security breaches

wirex

EXTRALINK