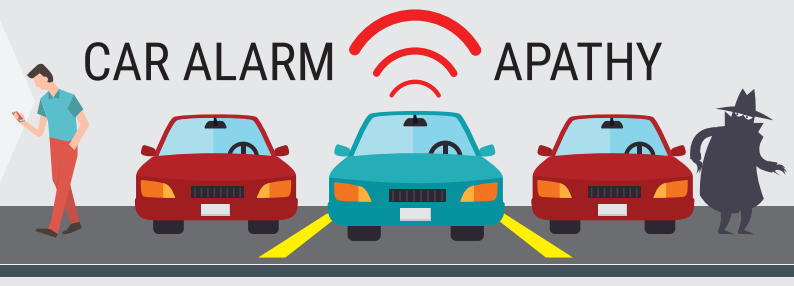
WHY POOR SIGNAL VS. NOISE HAS THWARTED ATTACK DETECTION

Delve into nearly every account about a data breach and you are likely to discover that data existed that could have warned about an in-progress attack. In many cases, alerts may have been issued but they were probably buried in a flood of other alerts.

CONDITION	PROBLEMS
Large volume of alerts.	NEEDLE IN THE HAYSTACK 
Alerts generated for each action, rather than a single alert representative of an activity.	CAR ALARM APATHY 
Activities seen as singular and isolated rather than connected and a part of an organized effort.	TREES VS FOREST 

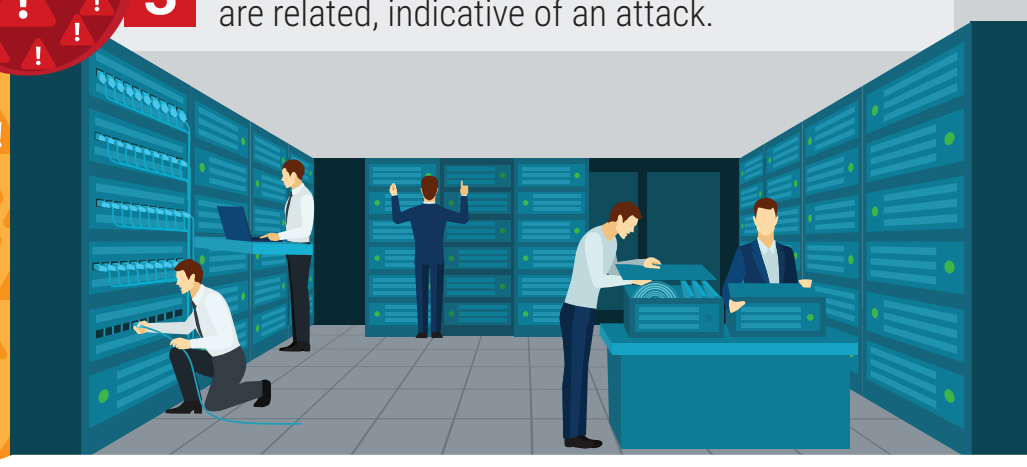
	WHAT HAPPENED	EVENT-CENTRIC	BEHAVIOR-CENTRIC
Failed Logins 	Attacker had 5,000 failed password attempts	Alerts on each failed log-in, in this case causing 4,995 alerts SIGNAL VS. NOISE 4,995:4,995	Issues a single alert showing there were 5,000 failed password attempts SIGNAL VS. NOISE 1:5,000
Port Scans 	Attacker sets off a port scan initially covering ports 21-3389	Alerts on each port scanned on each device in the network being accessed. In a network of 1,000 IP-devices, this might be some 10,000 ports scanned with possibly 10,000 alerts issue SIGNAL VS. NOISE 10,000:10,000	Issues a single alert that port scanning is being used, covering 50,000 ports SIGNAL VS. NOISE 1:50,000
Use of PS Exec Admin	Attacker executed 37 commands Remotely	Alerts on each command executed, in this case causing 37 alerts SIGNAL VS. NOISE 37:37	Issues a single alert about use of PS Exec but showing the 37 commands SIGNAL VS. NOISE 1:37
Total Alerts	**55,037**	**15,032**	**3 Alerts**

High Noise, Low Signal
Low Liklihood of Detecting Attack

Low Noise, Low Signal
High Liklihood of Detecting Attack

The Flood

1. Creates apathy and carelessness on the part of security operators. In this example, only 3 out of 55,037 alerts were relevant.
2. Degrades efficiency of security operator – too many wild goose chases rather than being focused on important events.
3. Lack of context – no ability to see events are related, indicative of an attack.



SOURCE: LIGHTCYBER

LIGHTCYBER

LIGHTCYBER.COM • (844) 560-7976