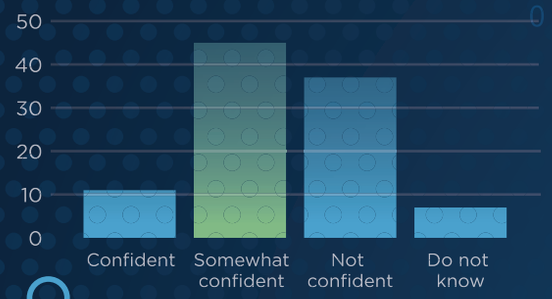
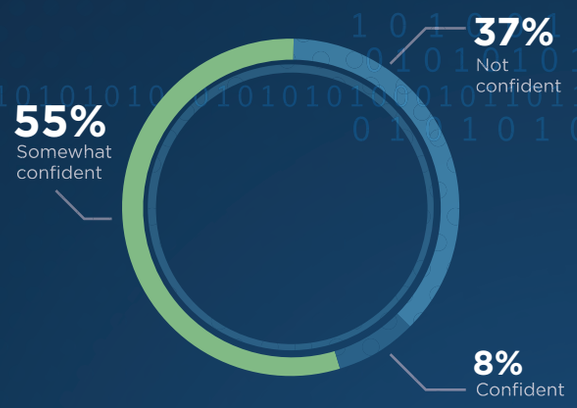
IS YOUR COMPANY'S CYBER SECURITY ACTUALLY GOOD ENOUGH?

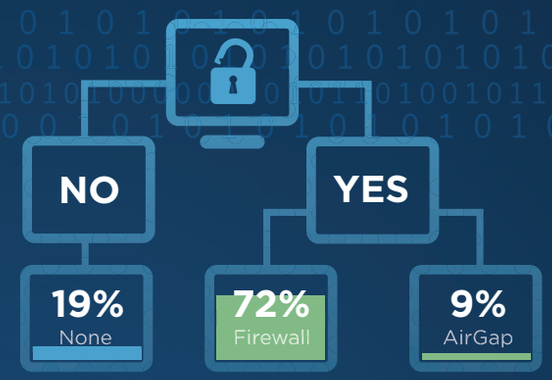
1. In a recent Oil & Gas IQ survey it showed that most concerns are aimed on Hackivism (61%) and State actors (Espionage 20% & Cyber Warfare 8%). How confident are you that your current defense mechanisms can handle/detect Hackivism?



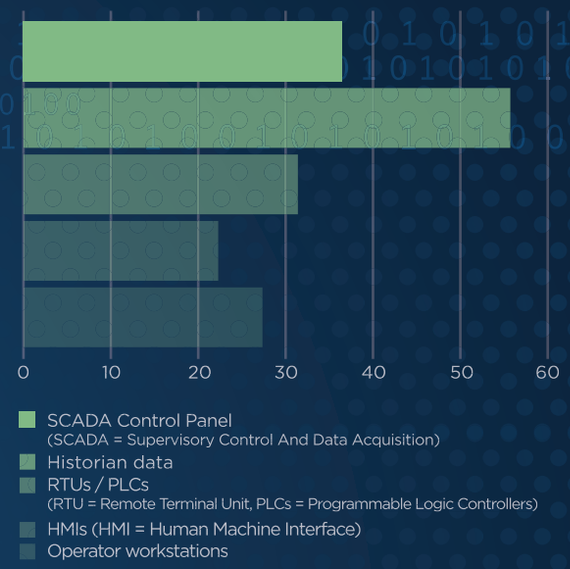
2. And how confident are you that your defense mechanisms can handle/detect State Actors/APTs? (APT=Advanced Persistent Threat)



3. Have you segregated your IT (Information Technology) network from your OT (Operational Technology) network?



4. From within your IT network, to what kind of data and/or devices do you need to have access to in your OT network?



5. Are you monitoring your network?

23% No

23% Yes, we have host IDS

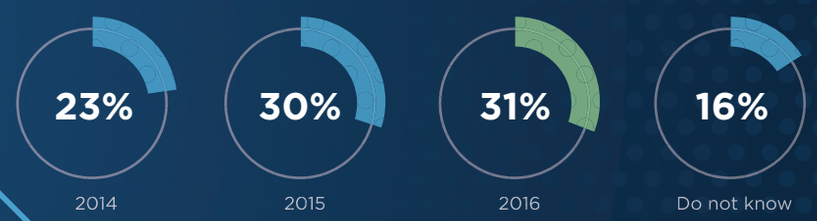
54% Yes we have network IDS (IDS = Intrusion Detection System)

38% Yes, we use a SIEM (SIEM = Security Information and Event Management)

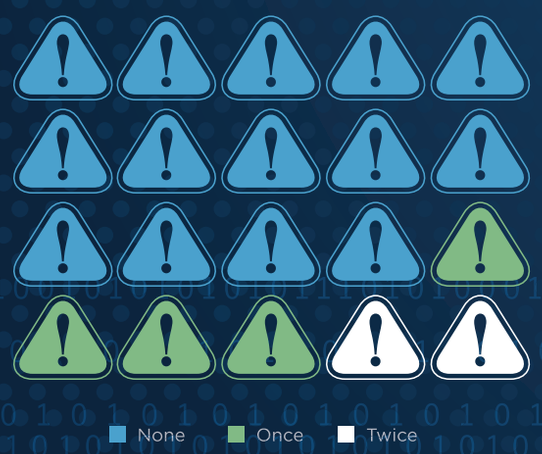
8% Yes, we use Honeypots

7% Don't know

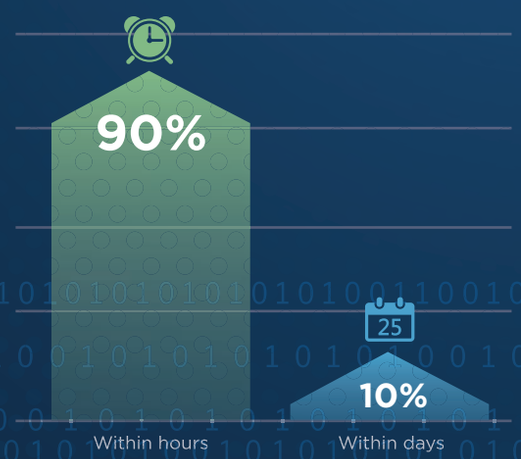
6. In what timeframe do you need to make (additional) investments in (cyber) security solutions as a result of regulatory compliance?



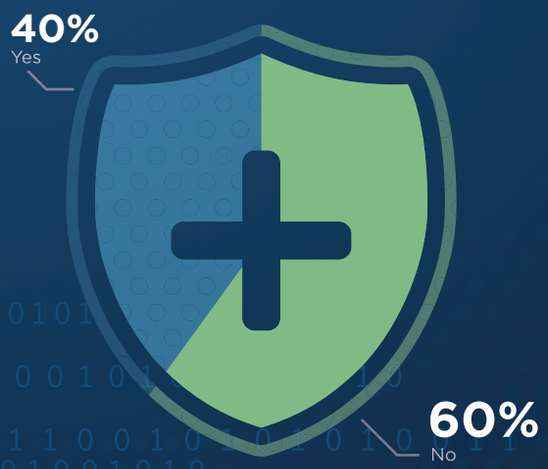
7. In the last three years, how often have you been confronted with a serious ICT (Information and Communication Technology) cyber incident?



8. How fast do you think it is necessary to be able to respond on a (cyber) security incident?



9. Does your organization have an Incident Response Plan in place?



40% Yes

60% No

10. If you had to make an estimate of the costs involved to recover from a cyber attack, what estimate would that be?

Oil & Gas iQ

FOX IT
FOR A MORE SECURE SOCIETY