The state of vulnerability response in utilities/energy organizations: Patch work demands attention

The severity and volume of cyberattacks continue to increase

- 53% of utilities/energy organizations experienced one or more data breaches in the last two years
- 25% increase in cyberattack severity over the last 12 months
- 40% of utilities/energy breach victims knew they were vulnerable before they were breached
- 52% of utilities/energy breach victims said they were breached due to a vulnerability for which a patch was available

Hackers are outpacing security teams

- 65% say attackers are outpacing enterprises with technology, i.e., machine learning and AI
- 59% say they find it difficult to prioritize what needs to be patched first
- 1.8 million global shortage of cybersecurity professionals by 2022*
- 26% headcount increase in the next 12 months

Security’s patching paradox:

No common view of assets and applications across security and IT

No easy way to track whether vulnerabilities are being patched

Things slip through the cracks because emails and spreadsheets are used to manage the patching process

- 69% time lost coordinating patching across teams
- 59% manual processes and siloed tools delay patching
- 48% 10 days

Learn how utilities/energy organizations avoid breaches. Get the report: www.servicenow.com/energy-ponemon