Crazy like a Fox

#Infosec Ideas that Just Might Work™
Think differently.

Use an adverb to describe our mental process correct.
Get pwned. Hard.

@jschauma
Get pwned. Hard.
(Then blame APT.)
Pay outside consultants to tell you what you already know.
Pay outside consultants to tell you what you already know.

If they come up with other ideas, one of you is likely wrong. Figure out who.
mount -o ro /

mount -o noexec,nosuid,nodev /home

mount -o noexec,nosuid,nodev /tmp

...
Just because Microsoft does it, doesn’t necessarily mean it’s terrible.

I <3 Kerberos.

@jschauma
Forget Network ACLs.
Forget Network ACLs.

You’ve been pwned already.
root ssh for everybody!

@jschauma
root ssh for everybody!

Most frequently executed sudo(8) commands?
Survey says: bash(1), su(1)
No login for you!
Come back... never!

Sorry, not a fox.

@jschauma
Reboot, refresh, repeat.

What could possibly happen?
Don’t have a security team.

Security is everybody’s responsibility.

@jschauma
Embrace “cyber”.

It’s YUGE.
Focus

@jschauma
Focus

Srsly.


@jschauma
Think differently.

- Get pwned. Hard. (Then blame APT.)
- Pay consultants to tell you what you already know.
- Learn from Microsoft. (Don’t reimplement Kerberos.)
- mount –o ro /; mount –o nosuid,noexec,nodev /home
- Forget ACLs. (You’re already pwned.)
- root ssh for everybody!
- No logins whatsoever. (User login => reimage.)
- Auto-reboot and auto-update regularly.
- Make security everybody’s job.
- Embrace “cyber”.

@jschauma

Focus.
Think differently.

• Get pwned. Hard. (Then blame APT.)
• Pay consultants to tell you what you already know.
• Learn from Microsoft. (Don’t reimplement Kerberos.)
• `mount –o ro /; mount –o nosuid,noexec,nodev /home`
• Forget ACLs. (You’re already pwned.)
• root ssh for everybody!
• No logins whatsoever. (User login => reimage.)
• Auto-reboot and auto-update regularly.
• Make security everybody’s job.
• Embrace “cyber”.

Focus.

@jschauma