Backdoors & Breaches

Inject Cards

BLACK HILLS
Information Security

Choose a number between 1 and 10

BLACK HILLS
Information Security

Card 1

Bobby the Intern Kills the System You are Reviewing

This. Happens. Far. Too. Often.

NOTES

No. Murder is never okay. Don't even think that.

Backdoors & Breaches

BLACK HILLS Information Security

Card 2

Data Uploaded to Pastebin

Bummer, the attackers have posted internal sensitive data on Pastebin. Your customers are now informed of the attack by the media.

NOTES

It happens... a lot, but it's just pure evil. Time to bring in Upper Management and the Legal Team.

Backdoors & Breaches

BLACK HILLS Information Security

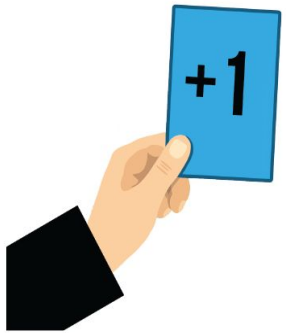
Card 3

Give the Defenders a Random Procedure Card

For whatever reason, everyone forgot they had this procedure. It must be Monday.

NOTES

Look, it happens all the time. We forget what we have. Different teams, different tools, different offices. It's nice when we all pull together as a team.



Backdoors & Breaches

BLACK HILLS Information Security

Card 4

HONEYPOTS DEPLOYED

The defenders had honeypots on their network. The "Incident Master" has to show their Pivot and Escalate Card to the defenders.

NOTES

Check out the Active Defense Harbinger Distribution (ADHD), it has lots and lots of cool tools. Also, take a look at canarytokens.org.

https://www.activecountermeasures.com/free-tools/adhd

https://canarytokens.org/generate

Backdoors & Breaches

BLACK HILLS Information Security

Card 5

IT WAS A PENTEST

Ha! Ha! Just kidding, you were never attacked! The CEO hired an external firm (BHIS?) to run an unannounced Red Team.

NOTES

This is almost always a bittersweet moment for companies. On the one hand they are glad it wasn't the real thing. On the other... well, they were compromised. It's time to start working through how to prevent this from happening again.

https://www.blackhillsinfosec.com

Card 6

Legal Takes Your Only Skilled Handler into a Meeting to Explain the Incident

Who brought a lawyer to the party? There's always one person who pretty much runs the whole IR process. That one essential person. Well, the legal team took that person away for "Very Important Reasons."

NOTES

They may never come back... all of the quiet people who were just passively listening and hoping to not get called on now need to step up. Now is your time. Shine!

Backdoors & Breaches

BLACK HILLS Information Security

Card 7

Management has Just Approved the Release of a New Procedure

Internal Network Capture and Analysis (+5 Modifier for Network Capture Analysis Tasks)

How many times has management come to the rescue? Knights in shining business suits. Every once in a great while the benevolent C-suite smiles on you.

NOTES

Get taps and monitoring in ASAP!!

Backdoors & Breaches

BLACK HILLS Information Security

Card 8

SIEM Analyst Returns from Splunk Training

+2 Modifier for Log-Related Actions

NOTES

Training is awesome. You need to get some.

Backdoors & Breaches

BLACK HILLS Information Security

Card 9

Lead Handler has a Baby, Takes FMLA Leave

Yeah, there's always one person who pretty much runs the whole IR process. That one essential person. Well, now it's time for the "Incident Master" to silence that person.

NOTES

We have to continue to be able to work effectively without the one or two most advanced people on the team. All of the quiet people who were just passively listening and hoping to not get called on now need to step up. Now is your time. Shine!

Backdoors & Breaches

BLACK HILLS Information Security

Card 10

Take One Procedure Card Away

What it says on the tin. Take a Procedure Card away from the defenders.

NOTES

Sometimes procedures fail. Sometimes they're not followed correctly. Sometimes you can't find a procedure when you need it the most. Nobody's perfect. Sorry.