Locked Down, Not Locked Out:

How I Escaped Your Secure Operator Workstation

WHO AM I?

Aaron Boyd

OT Cybersecurity Generalist

- SYSTEM ENGINEER @ LIBERTY ENERGY
- PENETRATION TESTING SINCE AROUND 2003 (HOBBYIST)
- PRIOR EXPERIENCE AS LEAD ICS SECURITY ARCHITECT IN OIL & GAS, MANUFACTURING & AEROSPACE.
- PRESENTED AT ICS VILLAGE, HOU SEC CON, SANS ICS SUMMIT, DRAGOS INDUSTRIAL SECURITY CONFERENCE, ICSJWG, & MORE…

WELCOME & GROUND RULES

- This won’t be a super deep technical exploitation talk.
- I won’t be naming vendors or integrators.
- If you want names, tools, or war stories, come find me!

WHAT DOES ‘LOCKED DOWN’ EVEN MEAN?

EXPECTATIONS VS. REALITY

😎

EXPECTATIONS

- Operator has minimal access to system functions
- Strict GPO and allowlisting control
- No local administrative privileges
- AppLocker or Solid core in full enforcement mode
- Login scripts are “harmless” config helpers
- Alerts if anything bad happens
- Everything is well-documented and reviewed

😭

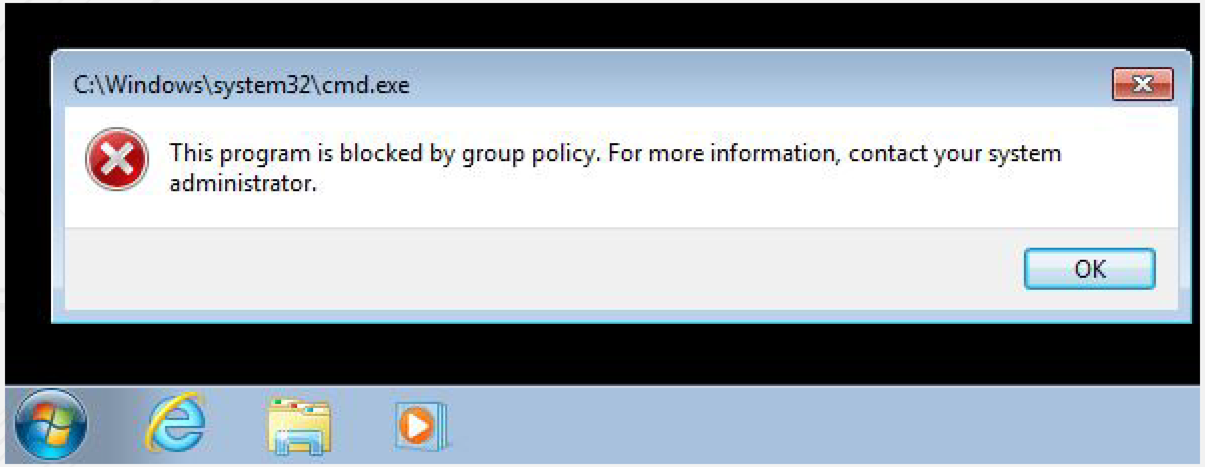
REALITY

- Operator can run renamed binaries or launch LOLBins
- Misconfigured or pathless GPO rules: allowlisting gaps
- Shared or default local admin creds still work
- Still in audit/learning mode or too permissive
- Login scripts expose drive paths, secrets, or tool access
- Misuse of signed tools rarely triggers alerts
- Integrator left it as-is: no one revisits post-deployment

HERE ARE SOME SPECIFIC EXAMPLES..

Example #1 - Group Policy Objects

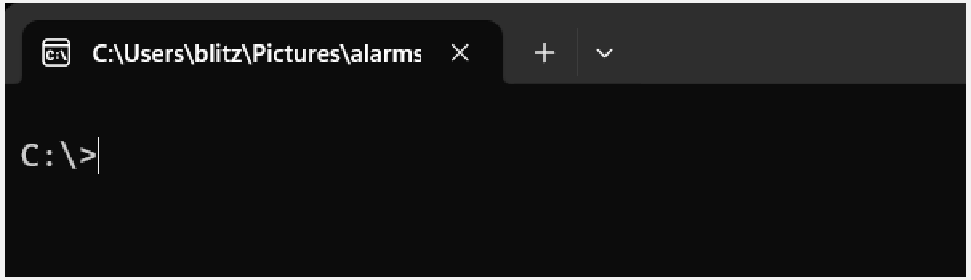
When trying to launch a "non-allowed" binary and having it be blocked by Group Policy Object…



C:\Windows\system32\cmd.exe

This program is blocked by group policy. For more information, contact your system administrator.

I bet the alarms manager binary called 'alarms.exe' is allowed and will let me launch command prompt if I rename cmd.exe to it…



```
C:\Users\blitz\Pictures\alarms

C:\>
```

Example #2 – Allowlisting Autopilot

😎

EXPECTATIONS

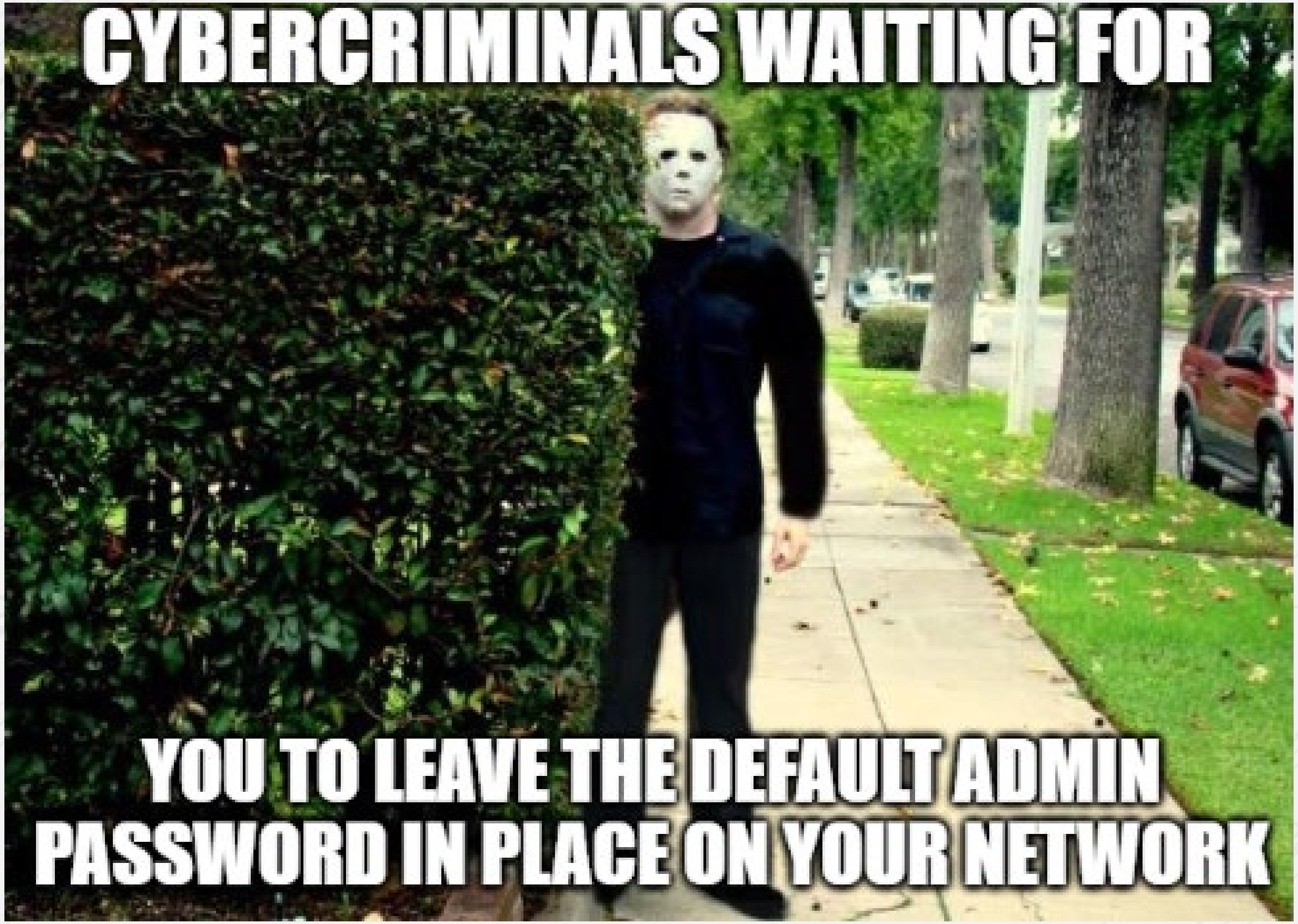
- “It’s deployed, so we’re protected”
- Only approved applications can run
- Policies block script abuse and LOLBins
- Alerting and logging are in place
- Integrator configured it per best practices
- Changes are managed and reviewed
- It prevents malware execution
- We’re safe – “It passed compliance!”

😭

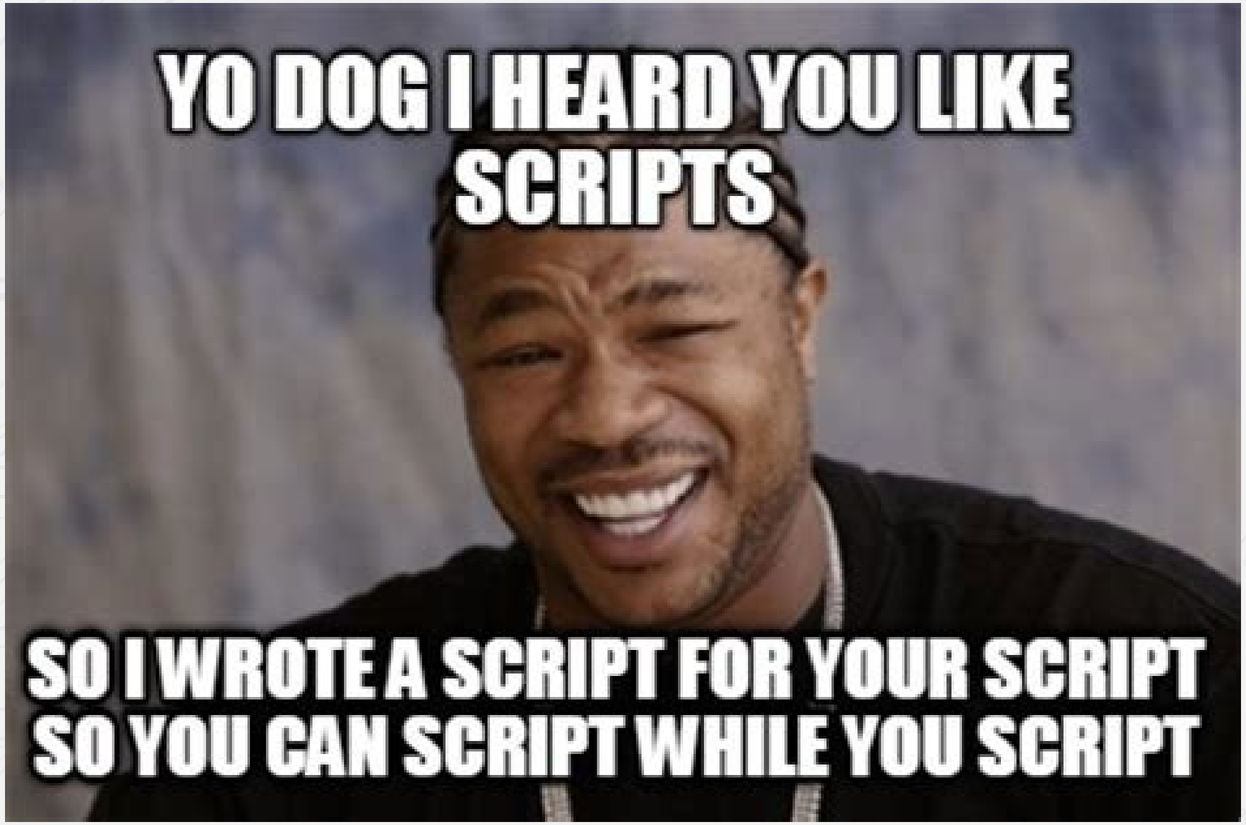
REALITY

- It was deployed in learning mode, never enforced
- Trusts too many things
- Regsvr32, msbuild, Bitsadmin, all happily bypass
- Logs are too noisy, ignored, or not forwarded to a SIEM
- Integrator copied the last working config – never validated
- Updates are ad hoc, allowlist exceptions not audited
- It breaks tools, it got neutered to reduce false positives

Example #3 – Default Creds (Yes, Really)


CYBERCRIMINALS WAITING FOR
YOU TO LEAVE THE DEFAULT ADMIN PASSWORD IN PLACE ON YOUR NETWORK

Example #4 – Login Scripts That Work For Me, Too


YO DOG I HEARD YOU LIKE SCRIPTS
SO I WROTE A SCRIPT FOR YOUR SCRIPT SO YOU CAN SCRIPT WHILE YOU SCRIPT

WHY DO THESE PATTERNS PERSIST?

JUST MY TWO CENTS…

Vendors

- Vendors want to ship stable systems fast
- Default images with basic hardening that “works everywhere”
- Not securely tailored to you or your org

Integrators

- Under pressure to deploy fast
- Configurations reused because it’s “what worked last time”
- The same oversights get copy-pasted from project to project.

Allowlisting

- Gets treated like antivirus.
- Install it, trust it, never look back.

Compliance

- Doesn’t ask “can an attacker break out?”
- Instead, asks “Did you enable allowlisting?”
- Organizations are trained/encouraged to follow checklists instead of chasing actual adversarial behaviors.

“We’re following the rules – just not the ones attackers play by.”

CHANGE THE CULTURE! NOT JUST CONFIGS

SECURITY ISN'T JUST TECHNICAL

- **Stop Outsourcing Accountability – Security isn't the vendors job, it's yours. Validate everything.**

- **Treat Security Tools Like Living Systems – They're not "set and forget." Tune, test, challenge them regularly.**

- **Shift From "Checkbox" to "Challenge". Go beyond what standards and frameworks suggest.**

- **Involve Operations In Security Decisions – If they're not part of the process, the controls will get worked around.**

- **Create Space for Failure – and Learning. Let people learn before attackers do.**

TLDR?

TAKEAWAYS

- ✓ Locked Down Doesn’t Mean Secure – Especially If You’ve Never Tried To Break It
- ✓ These Aren’t Zero-Day Techniques (Those Exist, Too) – They’re Day One Misconfigurations
- ✓ Ask Better Questions Of Your Vendors And Integrators! Trust But Verify!
- ✓ Don’t Just Deploy It – Test It. Don’t Wait For Attackers To Test It For You

“The cost of complacency is way higher than the cost of validation”

THANK YOU!
QUESTIONS?
COME FIND ME ☺

Aaron Boyd • ics-blitz@protonmail.com • @ics_blitz