SolarWinds supply chain breach
What mainframers need to know

GSE UK Security Working Group – 4th February 2021

Al Saurette +1 (403) 818-8625 al@maintegrity.com

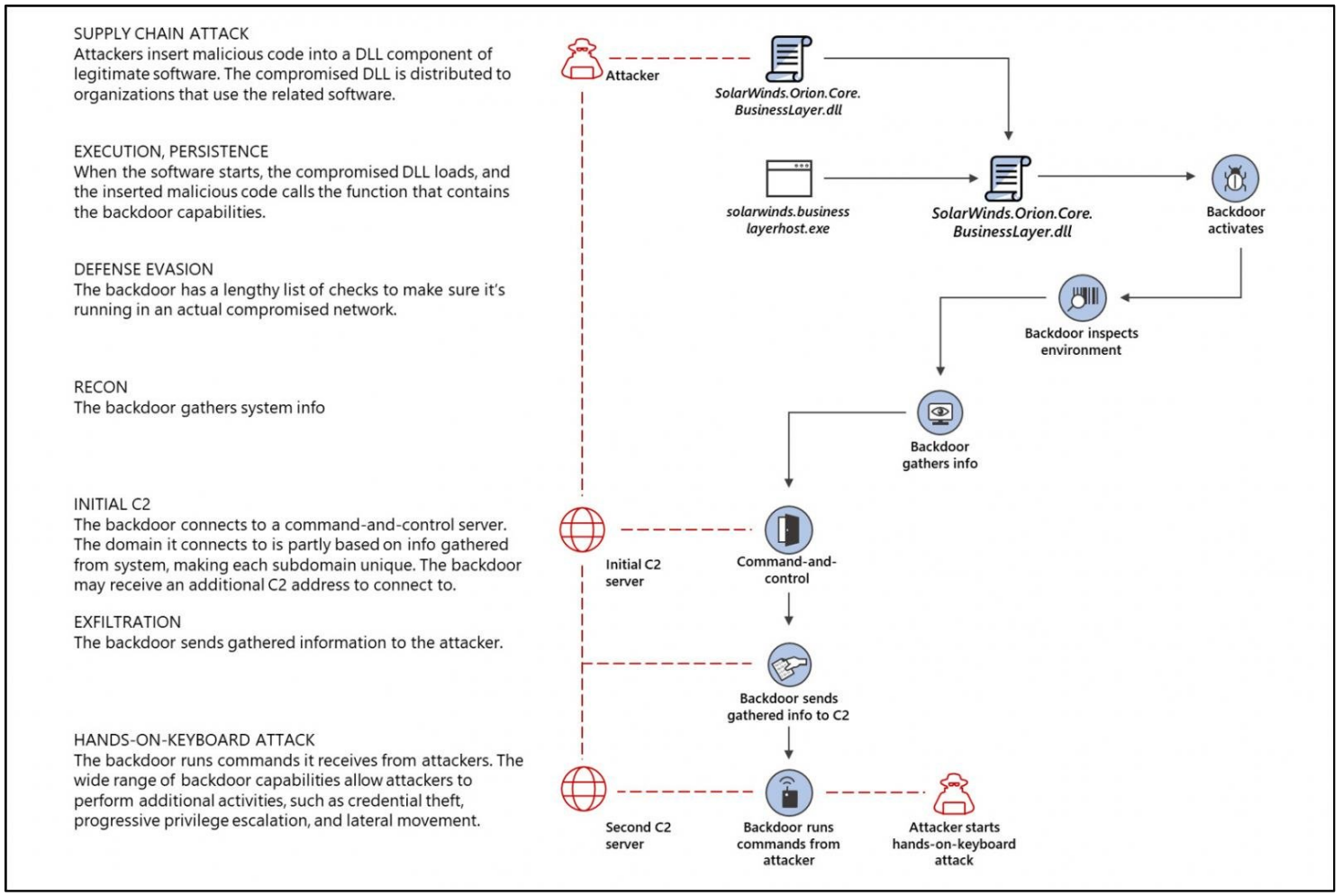
Customer consultant

SolarWinds supply chain breach
What mainframers need to know

Agenda

Intro	5
What happened in the SolarWinds attack	5
How does this apply to mainframes	5
First Questions	5
Counter-Measures - Avoidance	10
Questions /discussion	15

Sunburst Topology



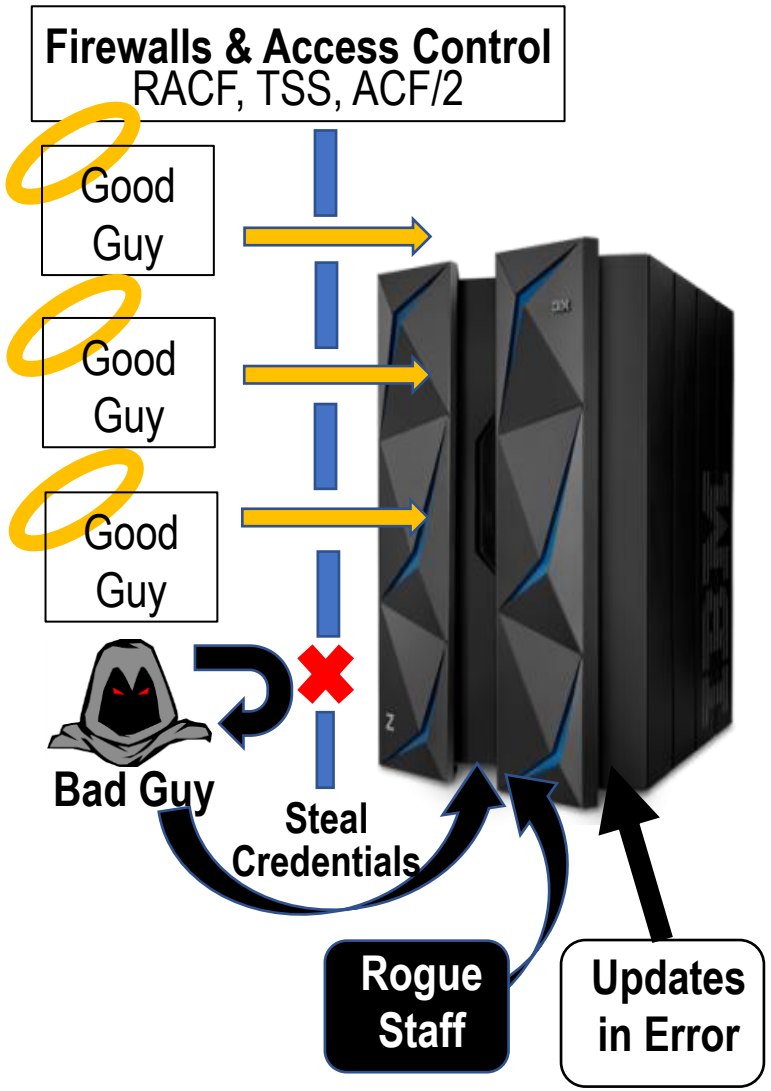
Courtesy of https://www.bleepingcomputer.com/news/security/the-solarwinds-cyberattack-the-hack-the-victims-and-what-we-know/

Related

https://www.toolbox.com/security/network-security/articles/what-tech-leaders-can-learn-from-the-solarwinds-trojan-horse-attack/

https://securityboulevard.com/2020/12/sunburst-how-it-happened-and-how-to-minimize-the-risk-of-future-nation-state-attacks/

Who are insiders?



Conventional Security – Guard the perimeter

- Insiders are past Firewall / Access Control
  1. Bad Guys Steal / Buy Credentials / USS
  2. Trusted employees go rogue (addiction, financial, health)

Well meaning staff make mistakes

- Were all changes approved and correct?
- Deployed successfully?
- Working remotely?

No matter how good your perimeter defences are motivated criminals will get in

Crux of Sunburst attack

GUIDE SHARE EUROPE UK REGION

SolarWinds Or Vendor portion

Gain Access
C2 (Command & Control) allows manual actions
Compromise Microsoft .dll
Hackers attack BUILD modules / parms
Inside for months, More credentials / authority
Cover their tracks – remove back door lateral
Replace problem code multiple times
Final build / test / posting

Client portion

Secure Download of code
Routine test and deploy
Hackers activate secondary back door
C2 (Command & Control) allows manual actions
Inside for months
More credentials, more authority
Exfiltrate data, intelligence, ransom

Mainframe attack

Gain Access
C2 (Command & Control) allows manual actions
Compromise IBM or client module / parms

SAME
SAME
SAME
SAME
SAME
SAME
SAME
SAME
SAME
SAME
SAME
SAME
Exfiltrate data, intelligence, ransom

Is your in-house build system more secure? Or less?

Exposures

This is a sophisticated attack – time, money, expertise, patience

- Few solutions to prevent or detect attack – before or after
- Build system attacked – Backdoors baked in
- A new version complicates verifying changes are correct
- Lack of penetrating tools for real time monitoring
- Hacks closer to the end are less likely to be detected – Deploy, Post Deploy
- Attack Package / Deploy steps - Modify JCL, Scripts, etc
- Compromise backups – prevent recovery

An ounce of protection… more like a gallon

Any questions yet?

Counter-Measures

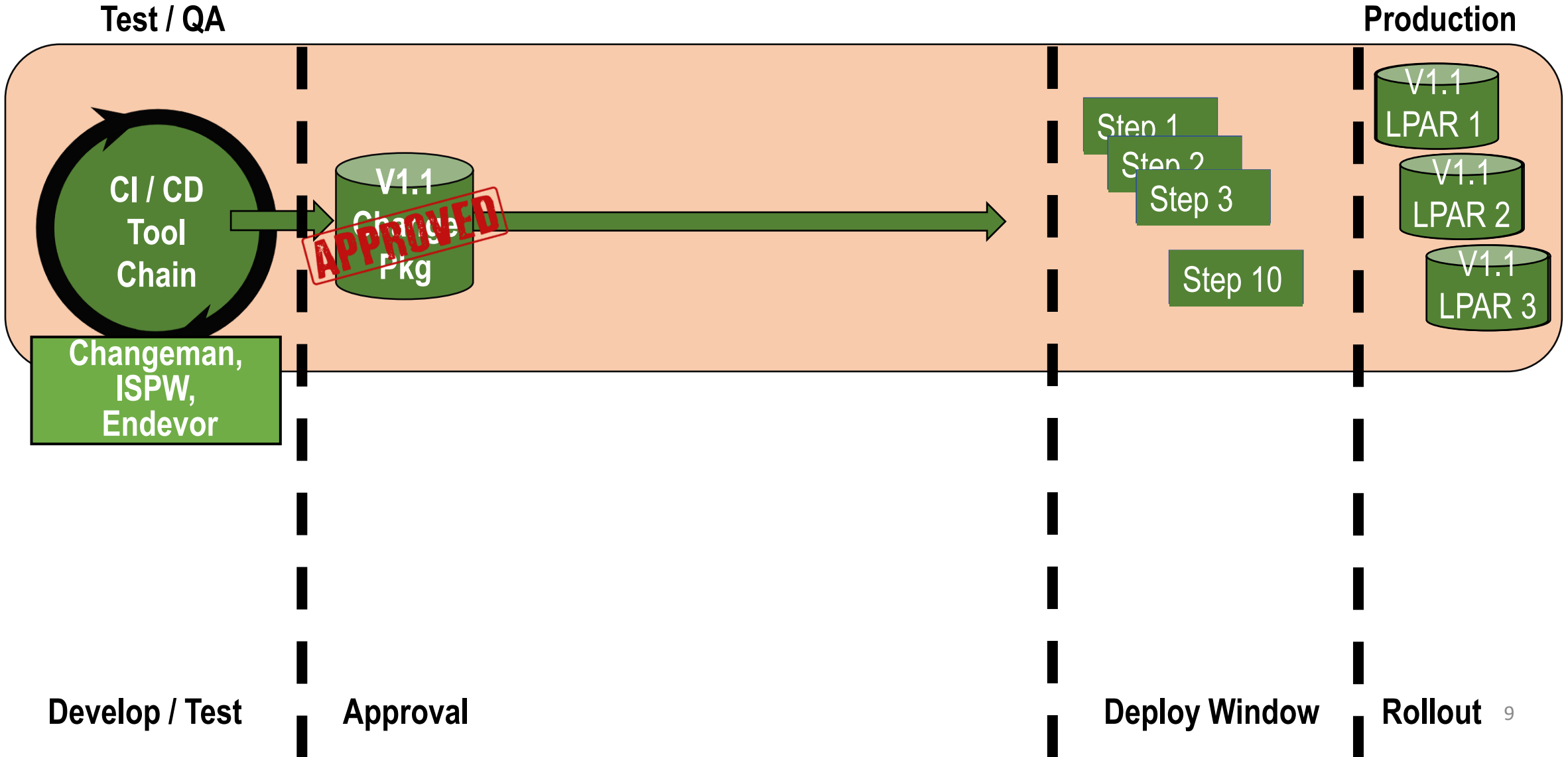
What can you do?

- Checksums (FIM) scans “look“ inside components – ask vendor to supply
- Scan your incoming maintenance / rescan before use
- Harden SCM / development process – monitor parms / modules / builds
- Peer / expert review - Verify contents & compare to prior releases
- Monitor subsequent actions – Component verify should be added
- Understand attack scope and interval – what affected, when correct
- Verify backups, Recover automation, then validate restore

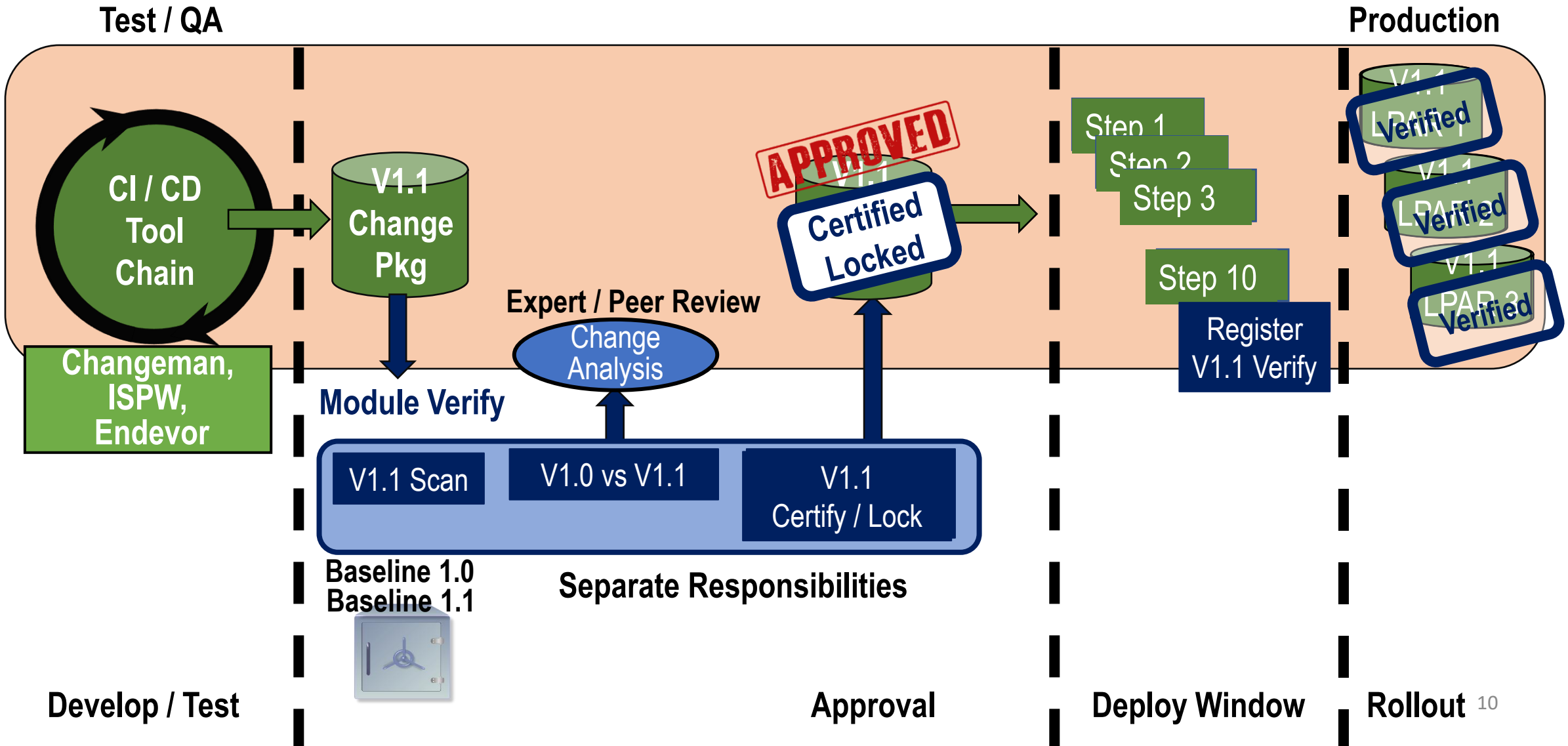
Compliance – PCI, NIST, Cyber Resiliency, GDPR, ISO

Brute Force - Audits, fines

Typical Change Process



Change Assurance



Change Assurance

GUIDE SHARE EUROPE UK REGION

Improve Release control / approval:

- Enable separation of duties – review, issue resolution
- See every component changed (look “inside” via compare)
- Visibility, cross-impact of parallel changes
- Certify / Lock release before approval & implementation
- Correct Deploy (verify added deleted, modified or missed components)
- Malicious vs changed (change control check, SCM only updates)
- Make SolarWinds type attack much harder

Automate - Less effort, more correct changes

So what should I do?

There are a lot more dumb hackers looking for an open door
than well funded hackers with lots of time and expertise

Just because you can't be perfect …
    Protect against less sophisticated attacks

Look like a compliance hero
    PCI, NIST, Resiliency, GDPR all call for checksum (FIM) processes

Sunburst should keep cyber security experts awake at night,
    but perhaps no one cares about mainframes

As a result of this session what are you going to do?

Al Saurette +1 (403) 818-8625 al@maintegrity.com