**Name: Jovanie C. Felamin Yr & sec: 4B laravel**

**Research and Case Evaluation on Auditing**

1. What is a key strategy for maintaining cybersecurity compliance in large organizations?

**Answer**: Automating security controls for compliance2

2. What is a key benefit of using security configuration management tools in organizations?

**Answer**: They identify misconfigurations and monitor critical changes

3. What action is essential for organizations to achieve security compliance?

**Answer**: Implementing controls and processes

4. How can organizations ensure effective security compliance?

**Answer**: Automate security controls and continuous monitoring

**I. Case Study – Role of Audit**

**Case 1: Okta Customer Support System Breach (2023)**

Nature of incident:

* Threat actor accessed Okta’s customer support case management system; some stolen files (HAR) contained session tokens.

How auditing/logs helped:

* Partner telemetry and log monitoring flagged suspicious admin activity early, enabling rapid response.

Audit policies/procedures that could have prevented/mitigated:

* Continuous monitoring of admin sessions; short‑lived, device‑bound tokens; sanitization/scrubbing of uploaded artifacts; centralized logs with ≥90‑day retention.

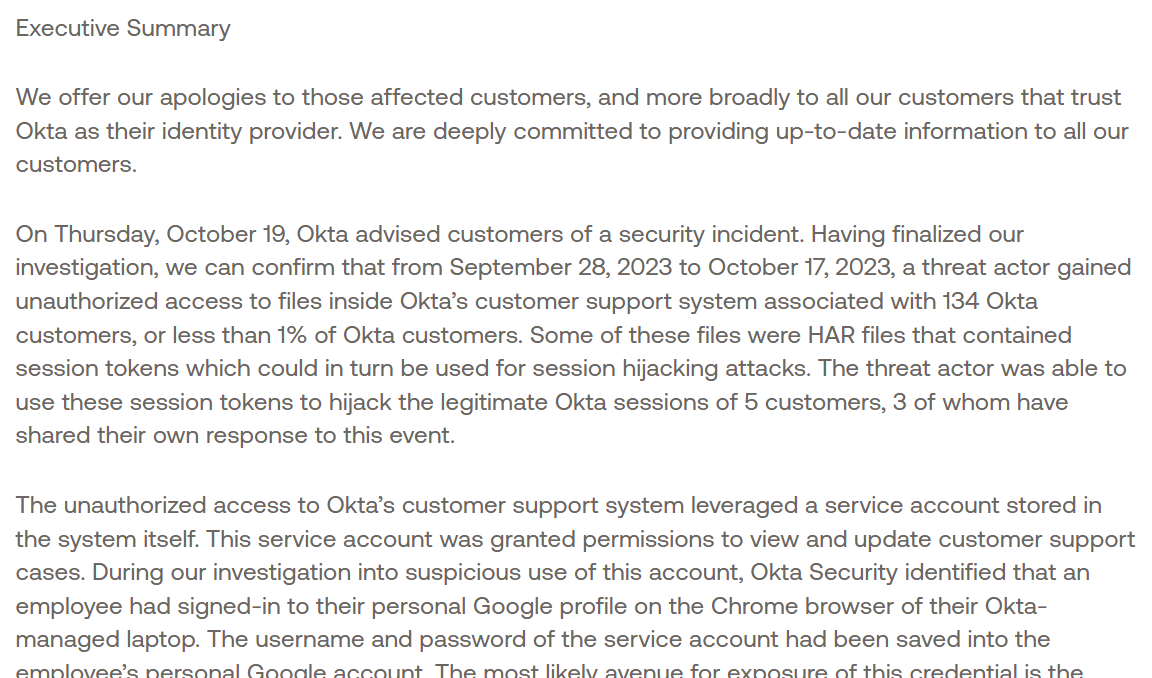
Lessons learned:

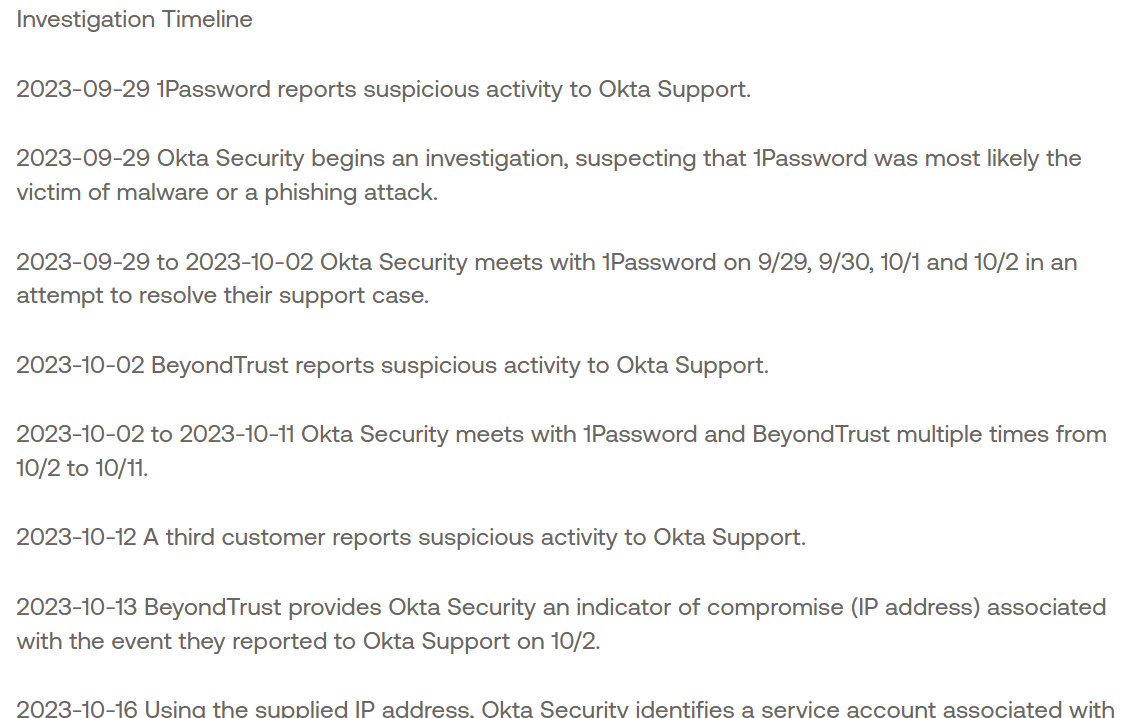
* Treat support workflows as high‑risk; detect token theft indicators quickly; monitor IdP/admin actions closely.

**Brief Report**

In September 2023, Okta experienced a security incident where a hacker got into their customer support case management system. The attacker was able to access files that some customers uploaded for troubleshooting, and a few of those files had session tokens that could be used to take over accounts. Out of all Okta customers, only a small number were affected, but a few well-known companies confirmed they were impacted.

The investigation showed that the problem started from a compromised service account. An employee had logged into their personal Google account on a work laptop, and the service account credentials were accidentally saved there. Once that personal account was breached, the attacker got hold of the credentials. What made things worse was that Okta’s system didn’t immediately catch the unusual file downloads because of a blind spot in how those actions were logged.

To fix this, Okta disabled the compromised account and made several changes to improve security. They blocked personal Google sign-ins on company devices, added stronger monitoring inside the support system, and introduced new protections like session token binding. These steps were done to make sure the same type of issue doesn’t happen again in the future.



Source:

Okta – Unauthorized Access to the Support Case Management System (Root Cause, Nov 3, 2023): <https://sec.okta.com/articles/2023/11/unauthorized-access-oktas-support-case-management-system-root-cause/>

**Case 2: SolarWinds Orion Supply Chain Attack (2020–2021)**

Nature of incident:

* Attackers inserted malicious code (“SUNBURST”) into SolarWinds Orion software updates, which were downloaded by ~18,000 organizations worldwide. This gave the attackers backdoor access to sensitive networks, including U.S. government agencies.

How auditing/logs helped:

* Security firm FireEye discovered the compromise after noticing suspicious use of their own authentication tools. Log analysis revealed unusual traffic from Orion servers to attacker-controlled domains, which exposed the larger campaign.

Audit policies/procedures that could have prevented/mitigated:

* Stronger code-signing validation and integrity checks during software builds; continuous monitoring of outbound connections from critical servers; anomaly detection in update processes.
* Broader log retention and centralized analysis would have helped organizations spot unusual Orion behavior earlier.

Lessons learned:

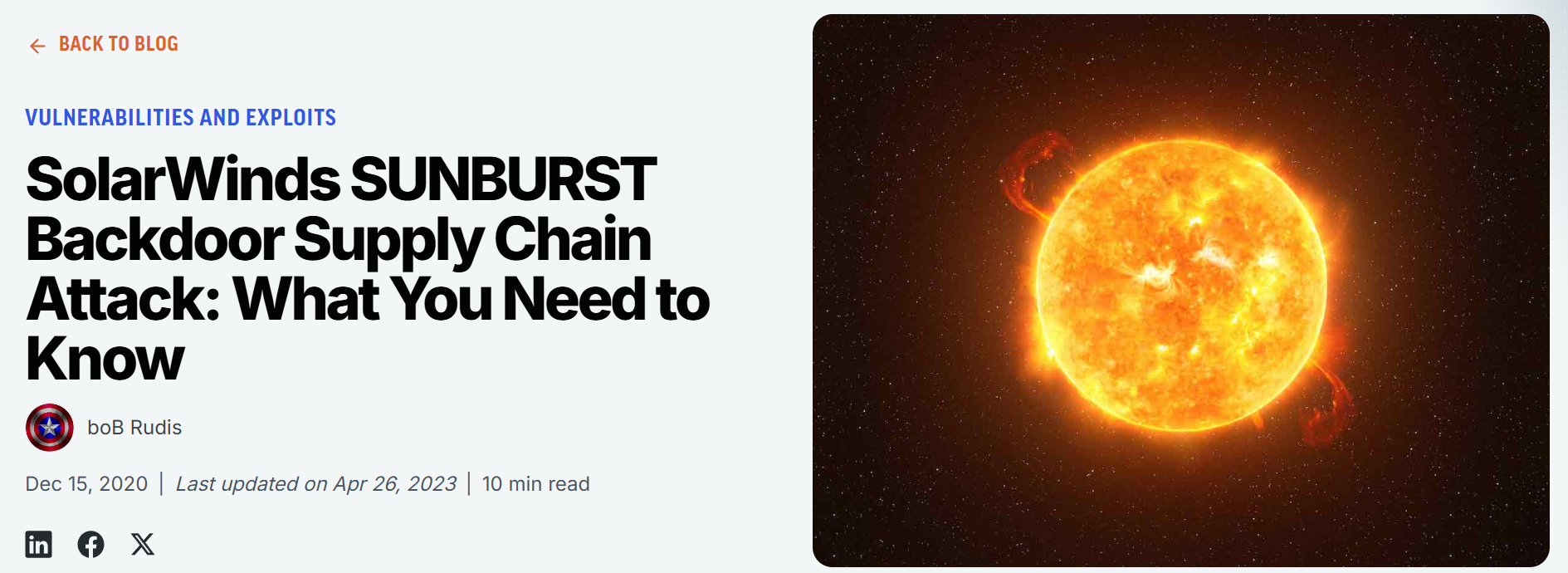
* Supply chain systems must be treated as critical audit targets; logs of software build processes and outbound network activity are vital. Organizations should combine endpoint, network, and application auditing to detect stealthy persistence.

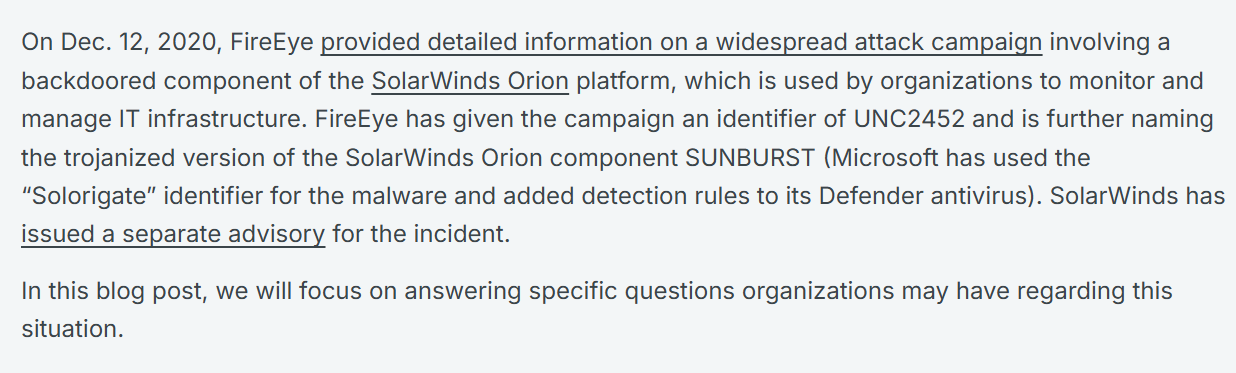
**Brief Report**

In late 2020, the **SolarWinds Orion supply chain attack** became one of the most significant cybersecurity breaches, affecting thousands of organizations.Hackers managed to insert malicious code into official software updates, which were then sent out to thousands of SolarWinds customers. This meant organizations—including U.S. government agencies—unknowingly installed backdoors that gave attackers access to their networks.

The breach came to light when FireEye noticed strange activity in its logs, showing unauthorized access attempts through Orion servers. Their investigation revealed that the compromised updates were communicating with attacker-controlled servers. Without those audit trails, it would have been much harder to detect such a stealthy attack.

To respond, SolarWinds and security agencies recommended stronger supply chain protections, stricter code integrity checks, and extended logging for critical systems. The lesson here is clear: organizations need deeper visibility into both their build environments and network traffic so that anomalies can be spotted before attackers gain long-term access.





Source:

SolarWinds – SUNBURST Backdoor Supply Chain Attack (Dec 14, 2020): <https://www.rapid7.com/blog/post/2020/12/14/solarwinds-sunburst-backdoor-supply-chain-attack-what-you-need-to-know/?utm_source=chatgpt.com>

**II. Audit Case Analysis – Simulated Audit Log**

**Suspicious Activities & Why They're Suspicious**

**Event ID 1001 & 1002 – App Crash or System Error** The system or an app crashed unexpectedly. This could mean something is wrong or someone tried to force it to crash.

**Event ID 6062 – Power Problem (Kernel-Power)** Shows the computer may have shut down or restarted in an unsafe way. This might be a power issue or someone forced it to shut down.

**Event ID 10016 – Permission Issue (DistributedCOM)** A program tried to do something it didn’t have permission for. This can be a sign of bad settings or someone trying to bypass limits.

**Event ID 16384 & 1003 – Software Protection Warnings** Many quick logs from Security-SPP might mean someone is trying to mess with software licenses or system files.

**Event ID 7001 – Service Failed to Start** A needed service didn’t start properly. This could stop important features or be caused by someone changing settings.

Recommended actions / policies:

* Enforce MFA and conditional access for all privileged accounts; restrict remote admin logons to PAM/JIT pathways.
* SIEM rules for: repeated 4625 followed by 4624, 4720 + 4728 within 10 minutes, any 1102 events, and encoded PowerShell.
* Use immutable (write-once) log storage and retain for ≥180 days; forward critical logs to SIEM in near real time.
* Apply least privilege; require approvals for group membership changes; enable Just‑In‑Time (JIT) admin with time‑bound roles.
* Restrict outbound traffic from servers; alert on large or unusual transfers to unknown IPs/domains.

**Suggested Corrective Measures (Aligned with Audit Policies)**

**Audit Process Tracking (4688, 4689):** Monitor unexpected program crashes and ensure all critical application failures are investigated.

**Audit System Events (6005, 6006, 6008, 41):** Configure alerts for unsafe shutdowns or Kernel-Power errors to detect possible tampering.

**Audit Privilege Use (4672, 4673):** Track attempts to escalate privileges and enforce least-privilege access to reduce DistributedCOM permission errors.

**Audit Object Access (4656, 4663):** Apply monitoring on software protection files and licensing components to catch tampering attempts.

**Audit Service Control Manager Events (7034, 7036):** Monitor when services fail to start or stop unexpectedly and implement service-hardening policies.

**III. Self‑Reflection**

I realized that security auditing is really important because it helps find out what happened in a system and who did it. Logs can show small details that explain a bigger problem, like failed logins or sudden system changes. In the future, if I manage systems, I would make sure logging is always turned on and safe from tampering.

I would also keep important logs for months so they can be checked later if something goes wrong. Setting alerts for unusual things, like too many failed logins or a new admin account being created, would help spot problems quickly. For sensitive actions, I think using multi-factor authentication is necessary so only the right people can do them.

From the cases I studied, my main lesson is that good auditing makes it easier to catch attacks and limit the damage. Without logs, it’s almost impossible to know what really happened. But with clear and complete logs, problems can be detected faster, and the system can be protected better.