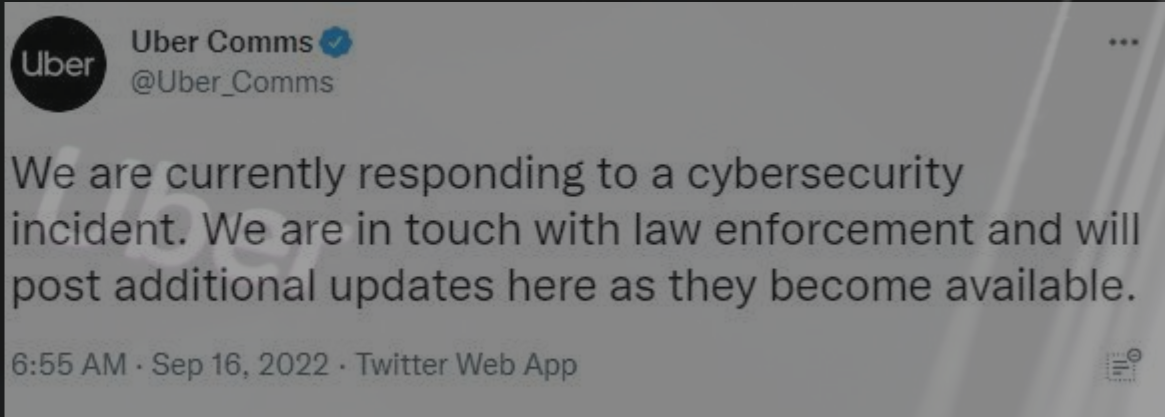
Key Takeaways for Enterprises

From Uber Security Incident

SHIRIS KUMAR

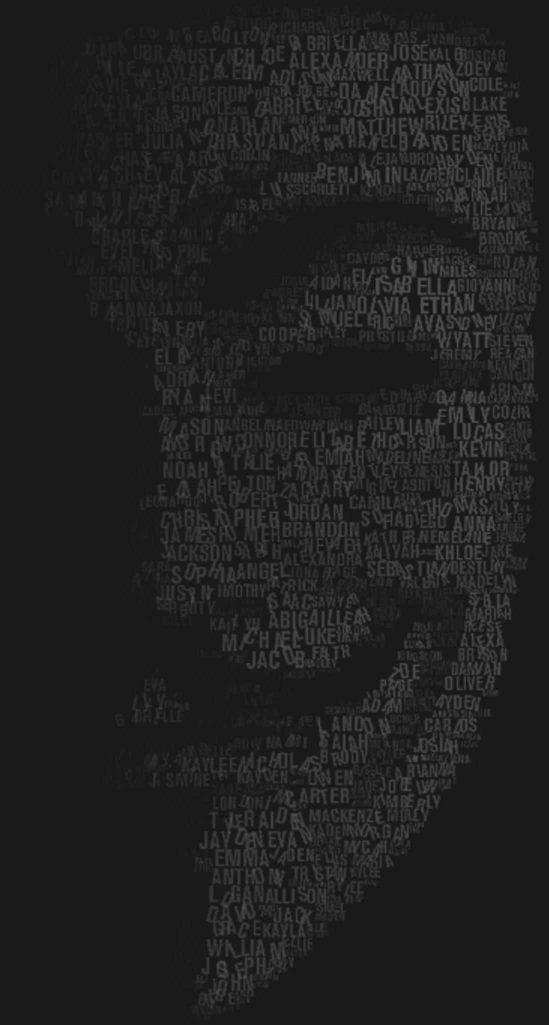
On September 16, 2022 at 6:55AM, Uber confirmed that it was responding to “a cybersecurity incident”



Uber Comms
@Uber_Comms

We are currently responding to a cybersecurity incident. We are in touch with law enforcement and will post additional updates here as they become available.

6:55 AM · Sep 16, 2022 · Twitter Web App



A 18-year-old hacker took responsibility for the attack. Uber believe LAPSU$ to be the culprit.

But what went wrong?

Could your company be the next victim?

What measures can we take to prevent it?

Key Takeaways

Train employees to prevent unconventional social engineering attacks.

SOC Teams can group alerts into incidents, so that they can see the bigger picture and prevent Alert Fatigue.

MFA Apps should implement rate limiting on Push Notification for Authentication to prevent MFA Bombing Attack

Disable 2FA via SMS by default as it is vulnerable to SIM Swapping

Use strong & unique passwords.

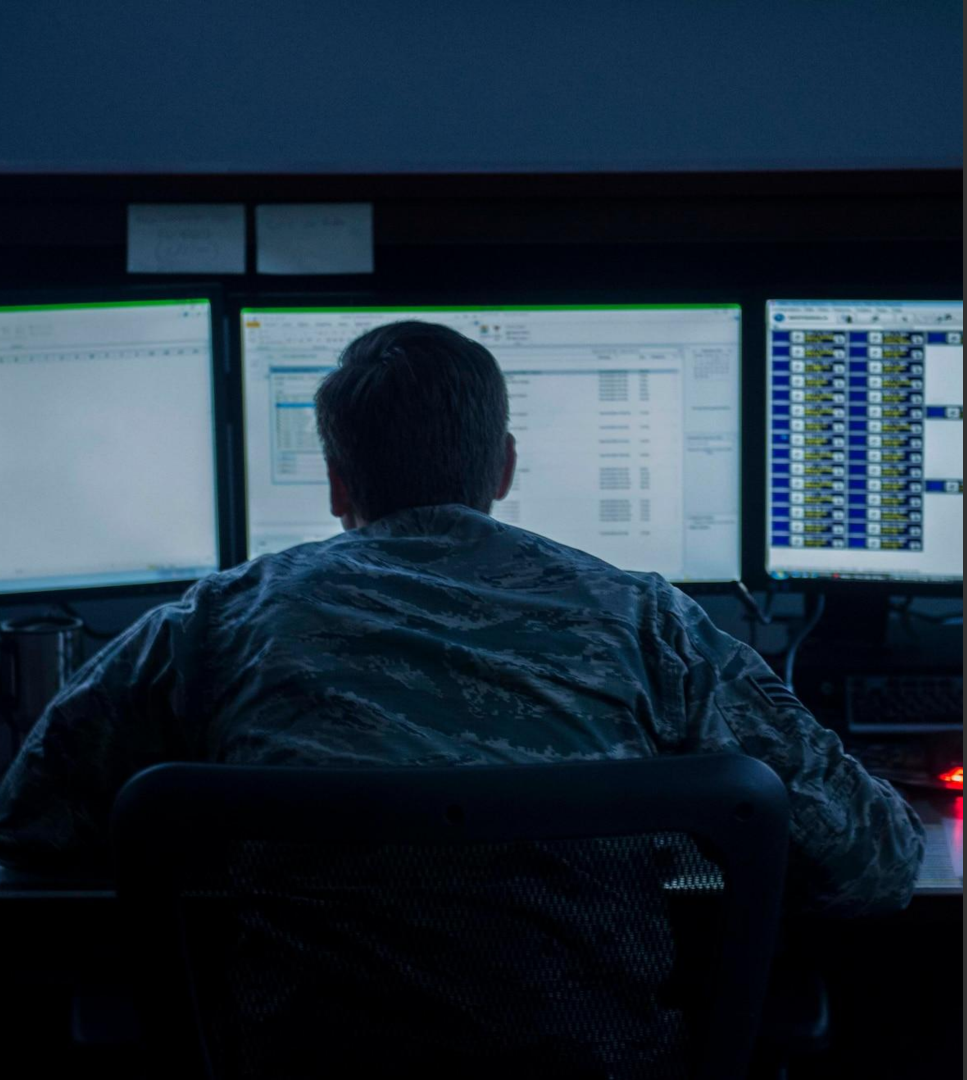
Never hardcode credentials in code. Instead use Password Vault.

```
tion(){cards();});
dow).on('resize', function(){cards();});
ion cards(){
var width = $(window).width();
if(width < 750){
    cardssmallscreen();
}else{
    cardsbigscreen();
}

}
nction cardssmallscreen(){
    var cards = $('.card').length;
    var height = 0;
    var card2 = 2;
    var i = 1;i<=cards;i++){
```

Always check-in code into a secure code repository & have ACL/RBAC Access Control.

Integrate Secrete Scanner into your code repository.



Recon is the initial step of an attack. SOC Team should look for signatures of vigorous internal port scanning from unintended sources.

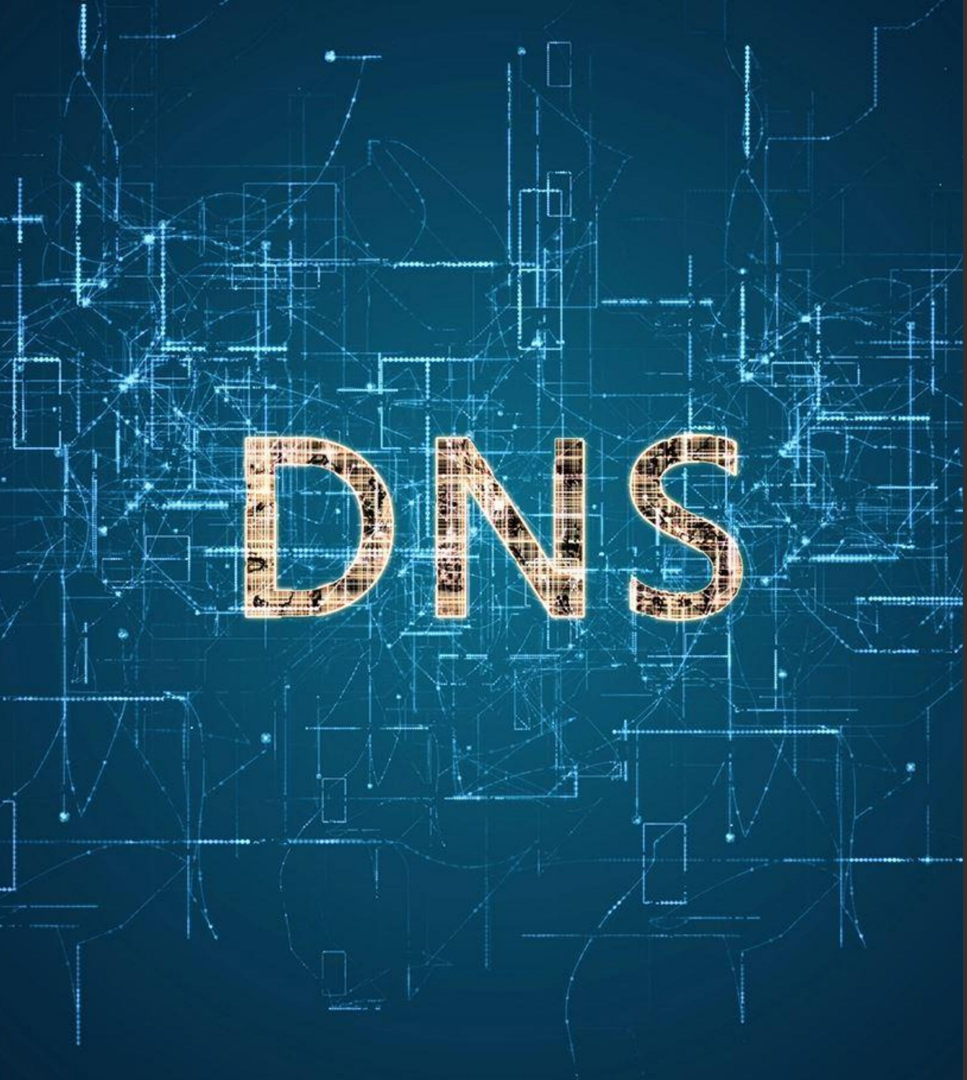
On Cloud premises, implement additional MFA & automate Attribute - Based Access Control.

Cyber Insurance - Its not an option, but a need.

Include quarantine or isolation plans with DFRA to take quick action soon after detecting any incident.

Always vet your DLP Solution with latest exfiltration techniques.

Prioritize Security over features and budget the teams accordingly.



Prevent Domain hijacking with Registry Lock.

Use DNSSEC (both signing zones & validating responses).

Disable Audit accounts created for security review after use.

Default settings are generally insecure. Always customize or tweak settings to maximize security.