Keep Your Enemies Close and Your Secrets Closer

AUDREY LONG

SENIOR SECURITY SOFTWARE ENGINEER

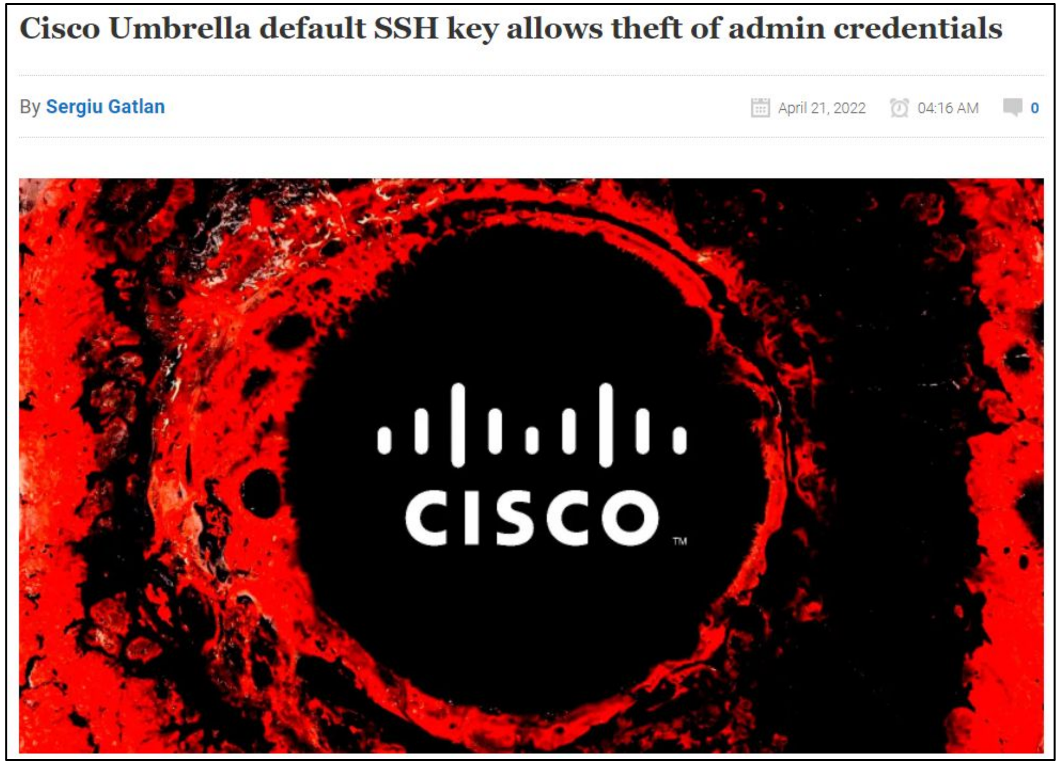
COMMERCIAL SOFTWARE ENGINEERING (CSE), MICROSOFT

About Me

- SR SECURITY SOFTWARE ENGINEER – MICROSOFT
- M.S. CYBERSECURITY – JOHNS HOPKINS UNIVERSITY
- B.S COMPUTER SCIENCE – UNIVERSITY OF CINCINNATI
- DIVERSITY AND INCLUSION AMBASSADOR
- PC GAMER

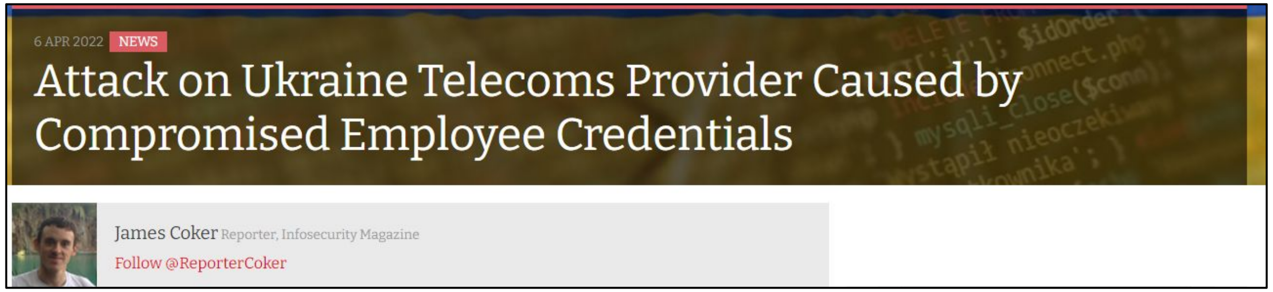
- FUN FACTS
  - MODERATOR FOR A KOREAN FOOD FORUM
  - I THINK A HOTDOG SHOULD BE CLASSIFIED AS A SANDWICH

Introduction



Cisco Umbrella default SSH key allows theft of admin credentials

By Sergiu Gatlan April 21, 2022 04:16 AM 0

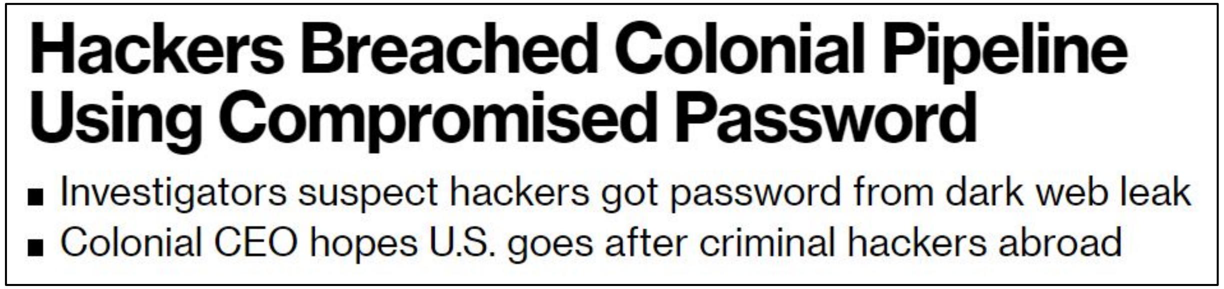


6 APR 2022 NEWS

Attack on Ukraine Telecoms Provider Caused by Compromised Employee Credentials

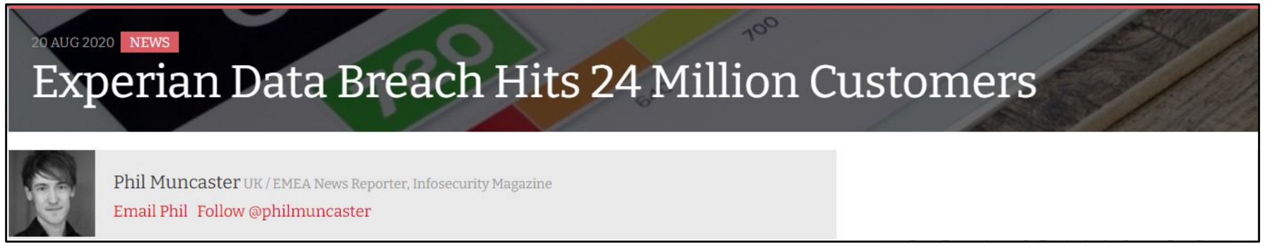
James Coker Reporter, Infosecurity Magazine

Follow @ReporterCoker



Hackers Breached Colonial Pipeline Using Compromised Password

- Investigators suspect hackers got password from dark web leak
- Colonial CEO hopes U.S. goes after criminal hackers abroad



20 AUG 2020 NEWS

Experian Data Breach Hits 24 Million Customers

Phil Muncaster UK / EMEA News Reporter, Infosecurity Magazine

Email Phil Follow @philmuncaster

Common Security Missteps

- Use of a stored test password
- Storing passwords in config files
- A lack of code scanning
- Storing sensitive information in open-source repositories
- Reuse of default passwords
- Not focusing on security during the full development cycle

Resiliency

Best approach:

Adopting an adversarial mindset

- Need to understand the attack landscape
- Build counter measures and mitigations
- Remove easily accessible secrets
- Shift security to the left

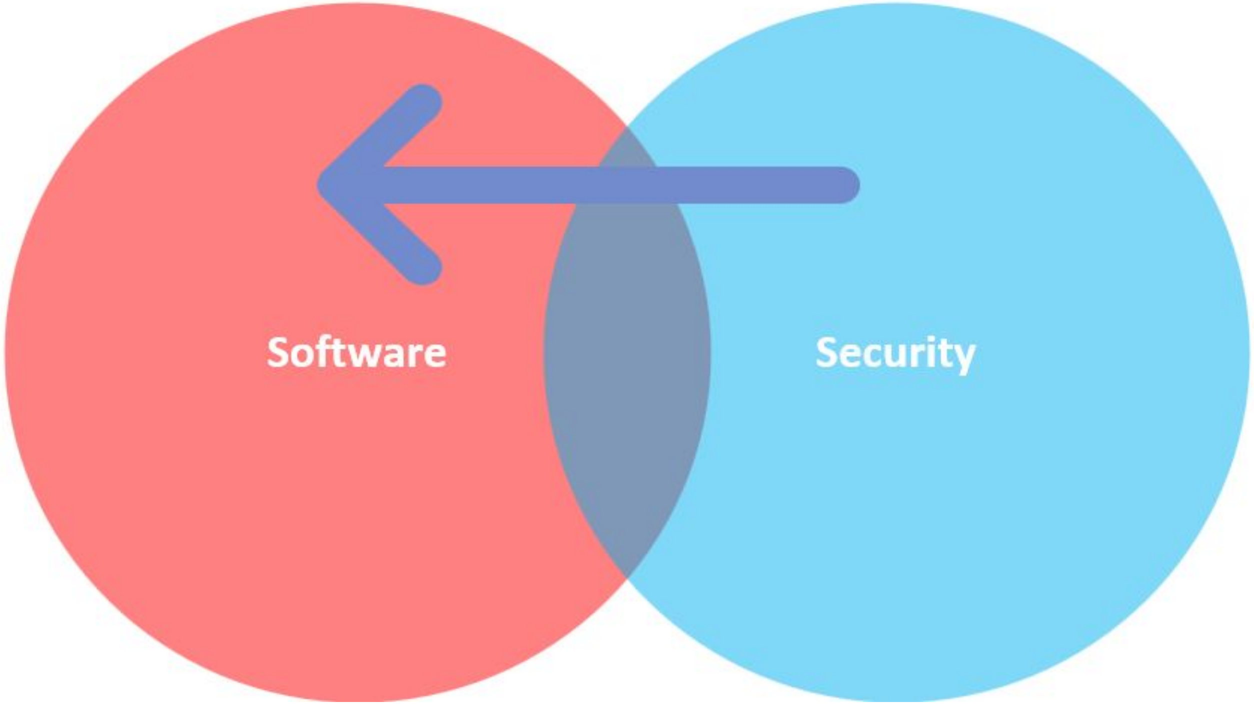
Why is this important to my team?

Only 1% of my organization is comprised of security engineers

- Both sides need to understand each other
- Need scalability across projects
- Modular security tools (plug and play)
- Dynamic in scanning nature
- Integration (backlog items)

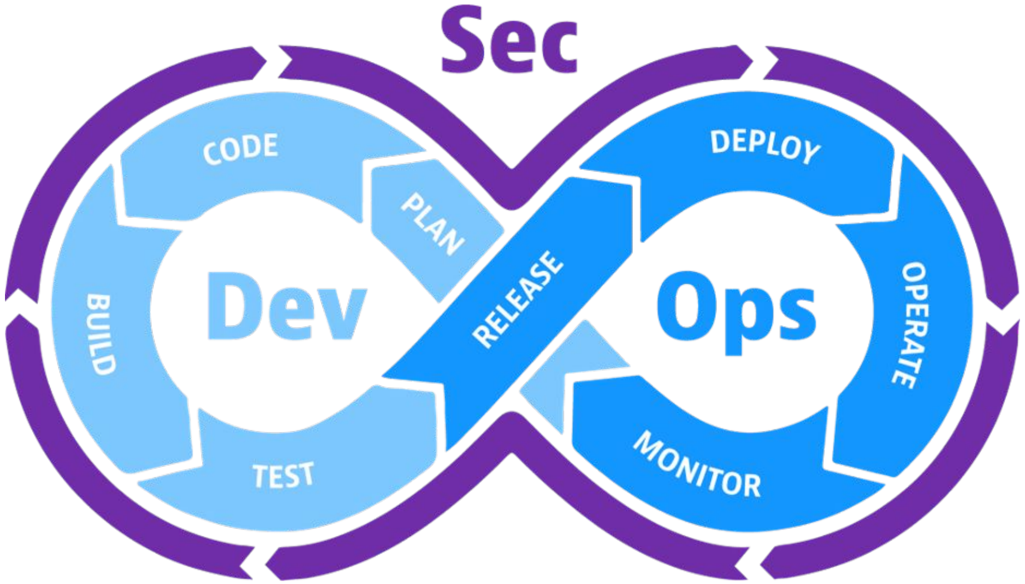
Intersection Between Software and Security

- Software Security Silo
- Shifting Left
- Development experience to understand attack vectors



DevSecOps Secure Pipelines

- Ensure developers don’t open doors in their pipelines
- Ability to monitor and fix pipelines
- Addressing risks without impeding development

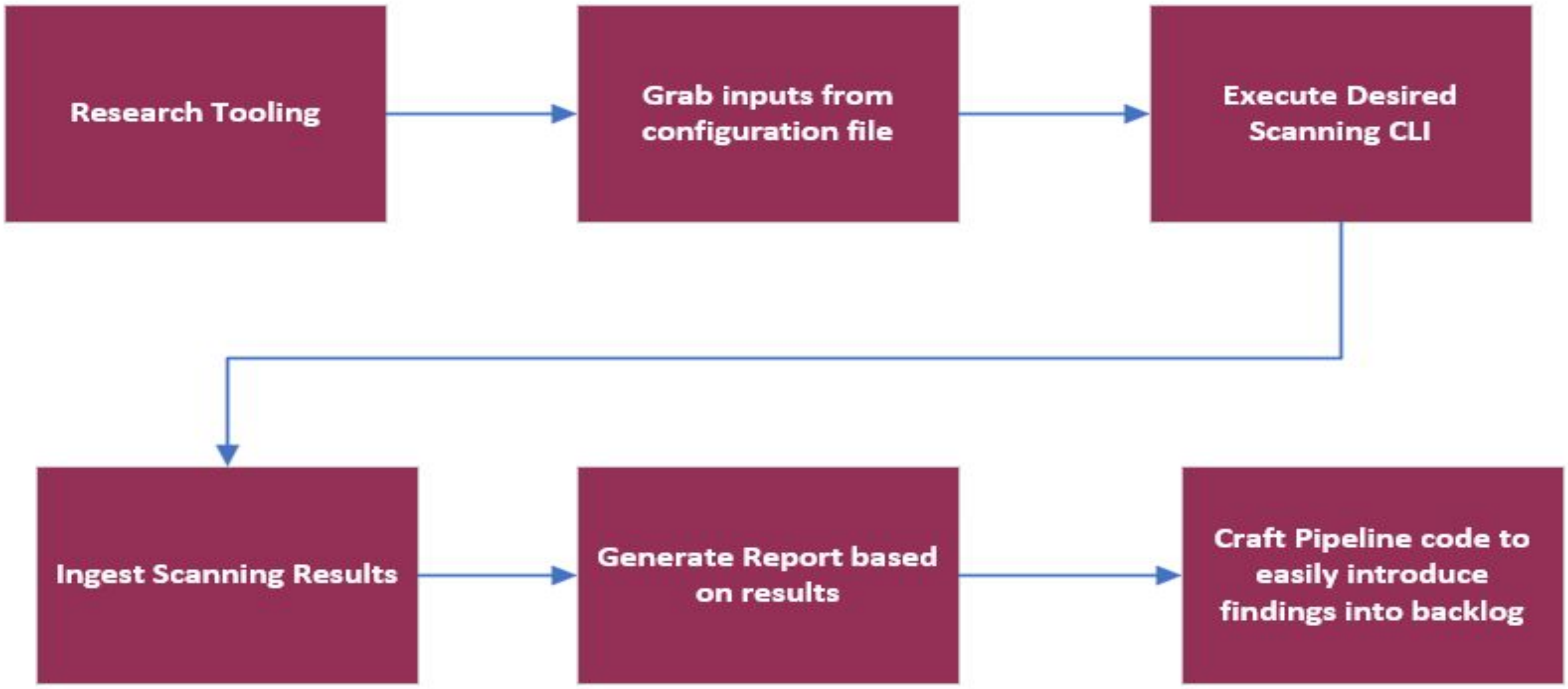


One tool to rule them all?

Answer: No there isn't… One tool doesn’t cover everything

- Multiple tools are needed
- Open-source reliability
- Security tooling default arguments
  - Custom rule sets

Reusable Architecture



Research Tooling

Grab inputs from configuration file

Execute Desired Scanning CLI

Ingest Scanning Results

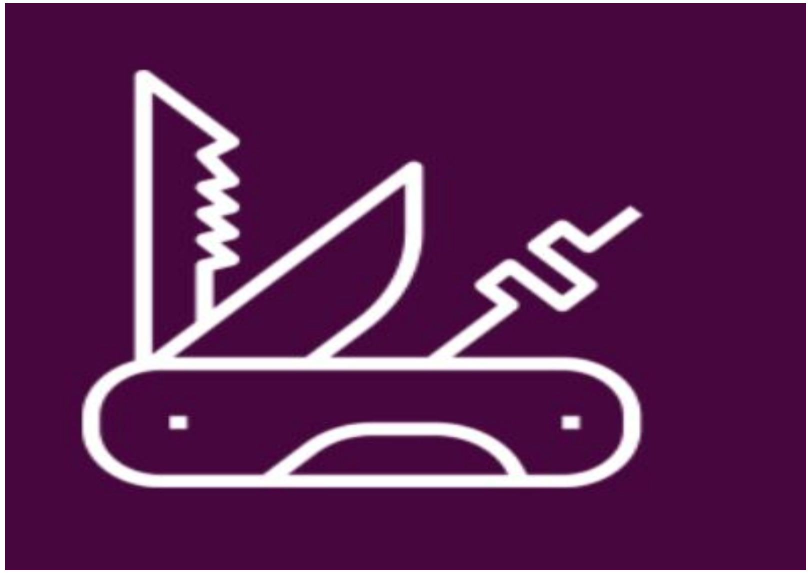
Generate Report based on results

Craft Pipeline code to easily introduce findings into backlog

Demo

Forward Thinking

- Smarter Secrets Detection
- Advanced Entropy Engines
- False Positive Reduction with ML
- Secure Code Pipelines by Default



Evolution

- Marriage between Software and Security
- Dynamic Security Practices
- Scalable Solutions to generate Security Impact

Let's Connect!

linkedin.com/in/**aulong**