



Using Prowler with Security Hub for AWS Assessments

Using Prowler with Security Hub for AWS Assessments

Christophe Limpalair
Founder & Trainer
at Cybr



Victoria Shutenko
Security Engineer &
Web App Pentester at
TechMagic



Today's Session

- Introductions
- What are cloud security assessments and CSPMs?
- Comparing CloudSploit with Prowler
- Demo of integrating Prowler with CodeBuild and Security Hub
- Wrapping up: About Cybr & about TechMagic
- Open to Q&A

TechMagic

CYBR

About Us





Using Prowler with Security Hub for AWS Assessments

Christophe Limpalair
Founder & Trainer
at Cybr



Victoria Shutenko
Security Engineer &
Web App Pentester at
TechMagic





About Victoria Shutenko

- Security Engineer at TechMagic
- ☁️ AWS Cloud Practitioner
- 🛡️ Background in web, infrastructure and crypto security
- 🎸musician, CTF player, love box, tourism and travelling, coffee addicted
- 🌊 I live in Odesa, Ukraine

Victoria Shutenko
linkedin.com/in/victoria-s-a44050b8/

@bjknbrrr
https://github.com/bjknbrrr

TechMagic

CYBR

Using Prowler with Security Hub for AWS Assessments

Christophe Limpalair
Founder & Trainer
at Cybr



Victoria Shutenko
Security Engineer &
Web App Pentester at
TechMagic





About Christophe Limpalair

- 📽️ Founder and Trainer at Cybr
- 👨‍💻 8+ years of AWS experience
- ⏮️ Background primarily in web dev and AWS cloud
- 🥾 I live in Colorado and love hiking & skiing

Cybr.com/discord

Christophe Limpalair
https://linkedin.com/in/christophelimpalair

@ChristopheLimp
https://twitter.com/christophelimp

TechMagic

CYBR

Christophe Limpalair
Founder & Trainer at Cybr



Victoria Shutenko
Security Engineer & Web App Pentester at TechMagic



Importance of Security in Cloud Environments

- Cloud environments offer scalability and accessibility but also present unique security challenges.
- With the rise of cyber threats, protecting sensitive data stored in the cloud is paramount.

Key Points:

- Growing Threat Landscape
- Protecting Sensitive Data
- Compliance Requirements



TechMagic

CYBR

Christophe Limpalair
Founder & Trainer at Cybr



Victoria Shutenko
Security Engineer & Web App Pentester at TechMagic



Prowler

Prowler is a robust security and compliance auditing tool designed specifically for cloud environments.

Key Features:

- Automated auditing: Conducts comprehensive security audits to identify vulnerabilities and compliance issues.
- Extensive coverage: Supports auditing of a wide range of AWS services and configurations.
- Customization: Offers flexible configuration options to tailor audits based on specific requirements.
- Compliance: CIS, PCI, HIPAA, NIST etc.

Using Prowler with Security Hub for AWS Assessments

Christophe Limpalair
Founder & Trainer at Cybr



Victoria Shutenko
Security Engineer & Web App Pentester at TechMagic



prowler

Run Prowler From:

Workstation computer

Kubernetes

docker

AWS Cloud

AWS CloudShell | AWS Cloud9 | Amazon EC2 | AWS CodeBuild | AWS ECS Fargate | Amazon EKS

Azure

VM Images | Azure Cloud Shell

Google Cloud Platform

Compute Engine | Kubernetes Engine | Container Optimized OS | Cloud Shell

Kubernetes Cluster

job

AWS Credentials or Role

Azure Credentials

GCP or Google Account

Kubernetes KubeConfig

Scan:

Query CSP Public APIs all regions, accounts, subscriptions, projects and namespaces available:

aws

Enrich:

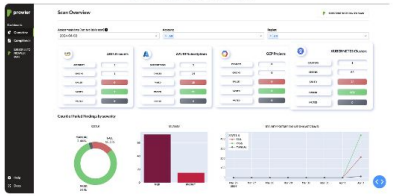
SHODAN

External Attack Surface:
Query for publicly exposed resources
[aws.ec2_elastic_ip_shodan]
[azure.network_public_ip_shodan]
[gcp.compute_public_address_shodan]

Formats and Visualization:

CSV | JSON

Local Dashboard



Integrations:

Native or via S3

Amazon S3 | AWS Security Hub | Amazon QuickSight | Amazon RDS | splunk> | elasticsearch | wazuh.

TechMagic

CYBR

Using Prowler with Security Hub for AWS Assessments

Christophe Limpalair
Founder & Trainer
at Cybr



Victoria Shutenko
Security Engineer &
Web App Pentester at
TechMagic



```
                                 _
 _ __  _ __ _____      _| | ___ _ __
| '_ \| '__/ _ \ \ /\ / / |/ _ \ '__|
| |_) | | | (_) \ V  V /| |  __/ |
| .__/|_|  \___/ \_/\_/ |_|\___|_|v3.0
|_| the handy cloud security tool
```

Date: 2022-12-02 12:53:30

This report is being generated using credentials below:

AWS-CLI Profile: [dev] AWS Filter Region: [all]
AWS Account: [1 6] UserId: [A
Caller Identity ARN: [arn:aws:sts::106 verica.io]

Executing 84 checks, please wait...

-> Scan is completed! |██| 84/84 [100%] in 1:07.2

Overview Results:

32.96% (442) Failed	67.04% (899) Passed

Account 106908755756 Scan Results (severity columns are for fails only):

Provider	Service	Status	Critical	High	Medium	Low
aws	ec2	FAIL (107)	0	67	23	17
aws	iam	FAIL (3)	2	0	1	0
aws	kms	PASS (3)	0	0	0	0
aws	s3	FAIL (322)	1	1	320	0
aws	ssm	PASS (2)	0	0	0	0
aws	vpc	FAIL (10)	0	0	10	0

*** You only see here those services that contains resources.**

Detailed results are in:
 - CSV: /Users/user/Documents/prowler-repos/prowler/output/prowler-output-1 6-20221202125330.csv
 - JSON: /Users/user/Documents/prowler-repos/prowler/output/prowler-output-1 6-20221202125330.json

TechMagic

CYBR

Christophe Limpalair
Founder & Trainer at Cybr



Victoria Shutenko
Security Engineer & Web App Pentester at TechMagic



CloudSploit

CloudSploit is a comprehensive security monitoring and compliance tool specifically designed for AWS environments.

Features and Functionalities:

- Automated scanning: Conducts automated scans of AWS infrastructure to identify security vulnerabilities and compliance issues.
- Real-time monitoring: Provides real-time alerts and notifications for potential security threats and misconfigurations.
- Remediation guidance: Offers actionable recommendations to remediate identified vulnerabilities and strengthen AWS security posture.

Using Prowler with Security Hub for AWS Assessments

Christophe Limpalair
Founder & Trainer
at Cybr



Victoria Shutenko
Security Engineer &
Web App Pentester at
TechMagic



bash

```
  _____ _                 _  _____      _     _ _
 / ____| |               | |/ ____|    | |   (_) |
| |    | | ___  _   _  __| | (___  _ __ | | ___ _| |_
| |    | |/ _ \| | | |/ _` |\___ \| '_ \| |/ _ \ | __|
| |____| | (_) | |_| | (_| |____) | |_) | |  __/ | |_
 \_____|_|\___/ \__,_|\__,_|_____/| .__/|_|\___/|_|\__|
                                  | |
                                  |_|

  CloudSploit by Aqua Security, Ltd.
  Cloud security auditing for AWS, Azure, GCP, Oracle, and GitHub

INFO: Ignoring passing results
INFO: Skipping AWS pagination mode
INFO: Testing plugin: ACM Certificate Validation
INFO: Determining API calls to make...
INFO: Found 2 API calls to make for aws plugins
INFO: Collecting metadata. This may take several minutes...
INFO: Metadata collection complete. Analyzing...
INFO: Analysis complete. Scan report to follow...
```

Category	Plugin	Description	Resource	Region	Status	Message
ACM	ACM Certificate Validation	ACM certificates should be configured to use DNS validation.	arn:aws:acm:us-east-1:131213121312:certificate/02b8e442-daec-49e1-9a93-131213121312	us-east-1	WARN	test.example.com is using EMAIL validation.
ACM	ACM Certificate Validation	ACM certificates should be configured to use DNS validation.	arn:aws:acm:us-east-1:131213121312:certificate/eb92c724-2643-4b46-8b71-131213121312	us-east-1	WARN	clouexample.com is using EMAIL validation.
ACM	ACM Certificate Validation	ACM certificates should be configured to use DNS validation.	arn:aws:acm:us-east-1:131213121312:certificate/eb92c724-2643-4b46-8b71-131213121312	us-east-1	WARN	*.example.com.com is using EMAIL validation.
ACM	ACM Certificate Validation	ACM certificates should be configured to use DNS validation.	arn:aws:acm:us-east-1:131213121312:certificate/1ccfbc69-eccb-4079-933a-131213121312	us-east-1	WARN	stage.api.cloudsploit.com is using EMAIL validation.

```
INFO: Scan complete
~/Projects/cloudsploit/scans$
```

TechMagic

CYBR

Using Prowler with Security Hub for AWS Assessments

Christophe Limpalair
Founder & Trainer
at Cybr



Victoria Shutenko
Security Engineer &
Web App Pentester at
TechMagic



Feature	AWS Security tool		
	Prowler	CloudSploit	Notes
Customization Options	High (custom checks possible)	Moderate (limited custom checks)	Prowler allows more flexibility in tailoring checks.
Ease of Use	Good, command-line interface	Very good, with user-friendly dashboard	CloudSploit may be easier for less technical users.
Reporting formats	Text, CSV, JSON-OCSF, JSON ASFF	JSON, HTML	Prowler allows for significant customization of the reports and supports more formats.
Integration	Good, with AWS services like Security Hub	Moderate, fewer direct AWS integrations	Prowler provides better integration with AWS Security Hub.
Community Support	Strong, with frequent updates	Good, less active than Prowler	Prowler's community-driven development is a strong point.

TechMagic

CYBR

Christophe Limpalair
Founder & Trainer at Cybr



Victoria Shutenko
Security Engineer & Web App Pentester at TechMagic



How to set up Prowler using AWS Codebuild?

1. Prerequisites

- IAM Permissions: Create an IAM role for CodeBuild with permissions to access necessary AWS resources.
- Add *SecurityAudit* Policy to the created role.

```
Effect": "Allow",
"Action":
"sts:AssumeRole"
"s3:Get*",
"s3:PutObject",
"s3:PutObjectAcl",
"s3:DeleteObject",
"s3:DeleteObjectVersion"
"securityhub:BatchImportFindings",
"logs:CreateLogGroup",
"logs:CreateLogStream",
"logs:PutLogEvents"
```

TechMagic

CYBR

Christophe Limpalair
Founder & Trainer at Cybr



Victoria Shutenko
Security Engineer & Web App Pentester at TechMagic



What is *SecurityAudit* Policy?

The security audit template grants access to read security configuration metadata. It is useful for software that audits the configuration of an AWS account.

SecurityAudit is an AWS managed policy.

Using Prowler with Security Hub for AWS Assessments

Christophe Limpalair
Founder & Trainer
at Cybr



Victoria Shutenko
Security Engineer &
Web App Pentester at
TechMagic



Set up Prowler scan role

IAM > Roles > ProwlerScanRole

ProwlerScanRole Info

Delete

Summary

Edit

Creation date
May 19, 2024, 16:19 (UTC+03:00)

ARN
arn:aws:iam::[redacted]:role/service-role/ProwlerScanRole

Last activity
5 hours ago

Maximum session duration
1 hour

Permissions | Trust relationships | Tags | Access Advisor | Revoke sessions

Permissions policies (2) Info
You can attach up to 10 managed policies.

Simulate | Remove | Add permissions

Filter by Type

Search

All types

1

Policy name	Type	Attached entities
ProwlerAdditionalPolicy	Customer managed	1
SecurityAudit	AWS managed - job function	1

TechMagic

CYBR

Christophe Limpalair
Founder & Trainer at Cybr



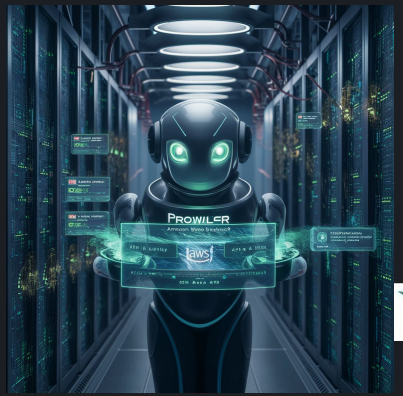
Victoria Shutenko
Security Engineer & Web App Pentester at TechMagic



How to start with the Prowler Codebuild?

2. Set Up AWS CodeBuild

- Turn on SecurityHub notifications and add Prowler Integration
- Create a new build project in AWS CodeBuild.
- Configure the project settings. Add BuildSpec, add env variables and assign the created IAM role (ProwlerScanRole).



TechMagic

CYBR

Using Prowler with Security Hub for AWS Assessments

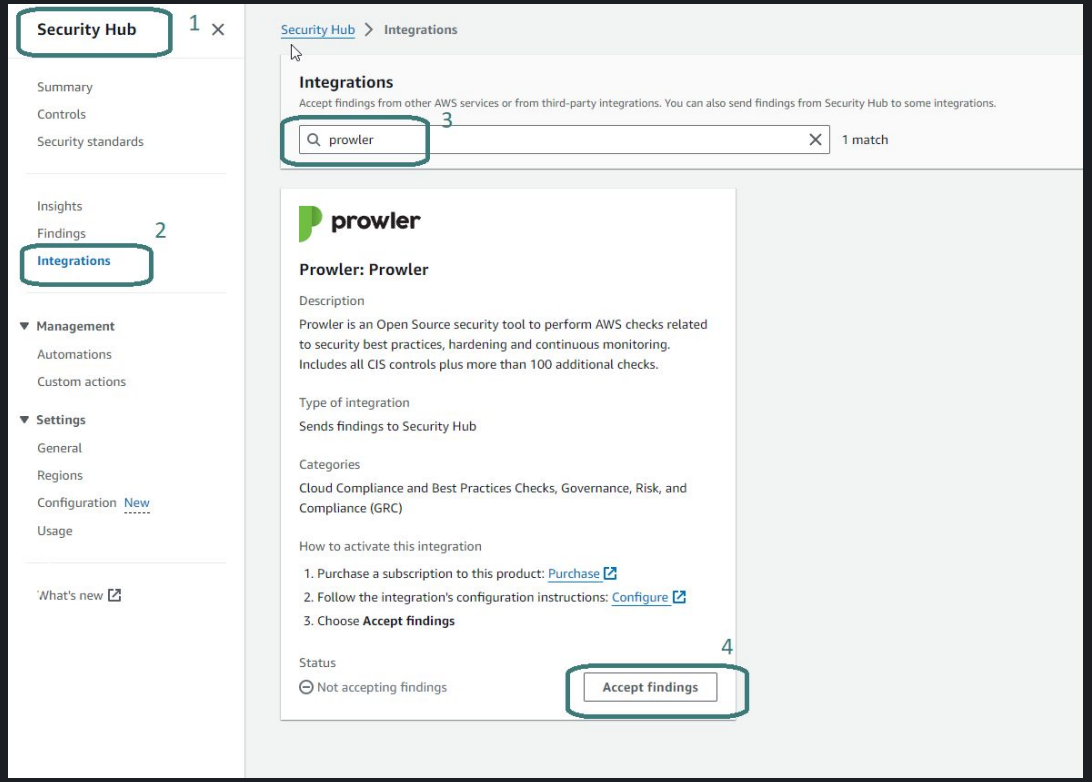
Christophe Limpalair
Founder & Trainer
at Cybr



Victoria Shutenko
Security Engineer &
Web App Pentester at
TechMagic



SecurityHub Prowler Integration



TechMagic

CYBR

Using Prowler with Security Hub for AWS Assessments

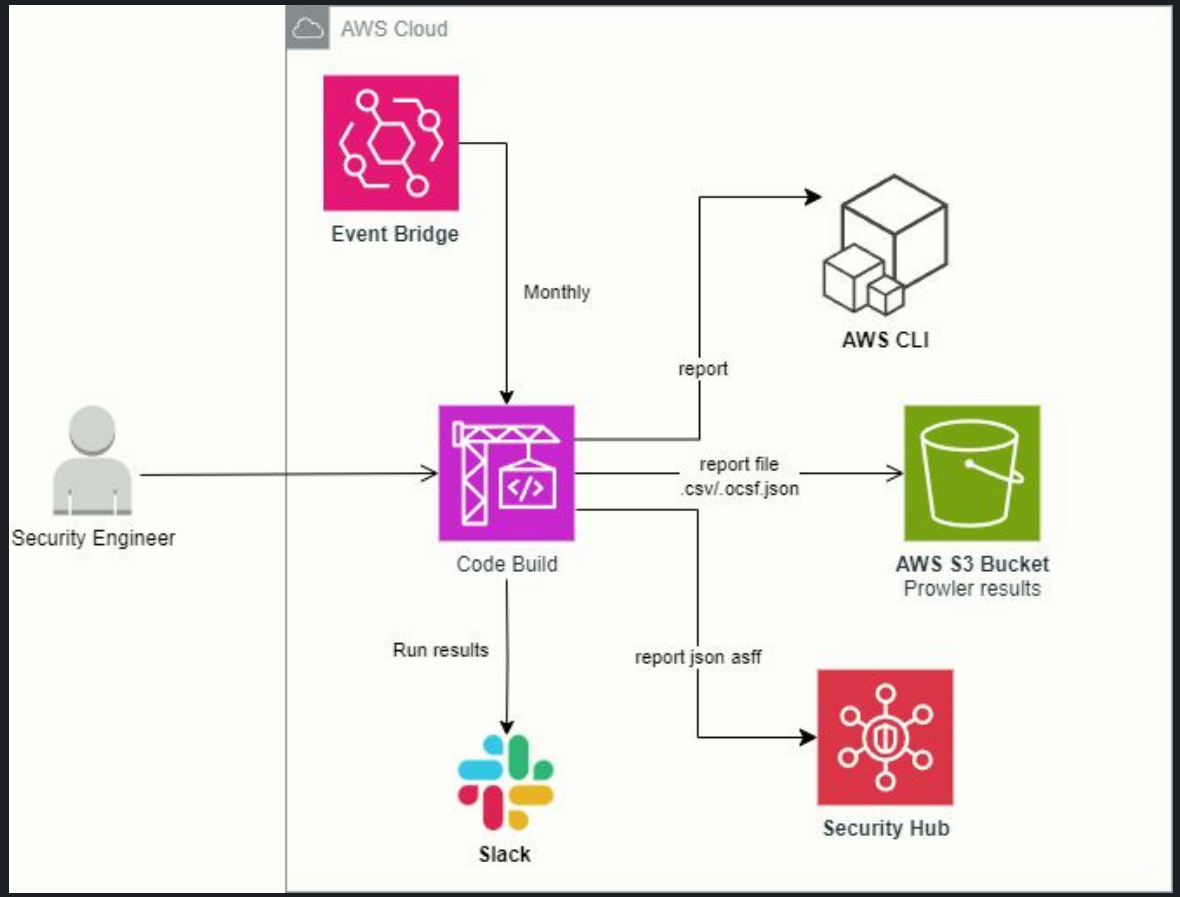
Christophe Limpalair
Founder & Trainer
at Cybr



Victoria Shutenko
Security Engineer &
Web App Pentester at
TechMagic



Final configuration



TechMagic

CYBR

Using Prowler with Security Hub for AWS Assessments

Christophe Limpalair
Founder & Trainer
at Cybr



Victoria Shutenko
Security Engineer &
Web App Pentester at
TechMagic



Slack notification:

Prowler notifications APP 9:01 PM

Prowler CIS Compliance Report

CIS Compliance Percentage: `50`%

Check the detailed results in **AWS SecurityHub**:

https://console.aws.amazon.com/securityhub/home?region=us-east-1#/dashboard.

TechMagic

CYBR

Using Prowler with Security Hub for AWS Assessments

Christophe Limpalair
Founder & Trainer
at Cybr



Victoria Shutenko
Security Engineer &
Web App Pentester at
TechMagic





Prowler CodeBuild Demo

TechMagic

CYBR

Using Prowler with Security Hub for AWS Assessments

Christophe Limpalair
Founder & Trainer
at Cybr



Victoria Shutenko
Security Engineer &
Web App Pentester at
TechMagic



Service	Parameters		
	Cost Estimate monthly	Findings Ingestion	Features
Prowler (CodeBuild) + Security Hub	CodeBuild: $0.60 Security Hub: $0.03 Total: $0.63/month	Charges for each finding ingested into Security Hub	Comprehensive security checks, customizable, single-run simplicity
AWS Config + Security Hub	AWS Config : $90.00 + $3.00 = $93.00 Security Hub: $0.03 Total: $93.03/month	Charges for each finding related to configuration changes ingested	Configuration management and compliance tracking

- Security Hub pricing
- AWS Config pricing
- Codebuild pricing

TechMagic

CYBR

Using Prowler with Security Hub for AWS Assessments

Christophe Limpalair
Founder & Trainer
at Cybr



Victoria Shutenko
Security Engineer &
Web App Pentester at
TechMagic



Reviewing Prowler findings: tips and tricks

1. Schedule Regular Reviews
2. Benchmark Against Standards
3. Prioritize Findings
4. Integrate with CI/CD
5. Track and Document Remediation
6. Leverage Dashboards and Alerts
7. Review Historical Trends
8. Engage with Stakeholders
9. Educate and Train
10. Continuous Improvement



TechMagic

CYBR

Using Prowler with Security Hub for AWS Assessments

Christophe Limpalair
Founder & Trainer
at Cybr



Victoria Shutenko
Security Engineer &
Web App Pentester at
TechMagic



About TechMagic

- Penetration testing services: Web and Mobile Application, Cloud infrastructure
- pentest
- Managed security services: embedding security practices into SDLC
- Security awareness team training on identification and mitigation of common
- security risks
- Compliance guidance: ISO, SOC2 certification preparation

We trusted by ACORN·i Elements.cloud bamboo XaaS DEPLOYR GOOD&CO Coach Solutions InstaSwift

Book call or drop me an email victoria.shutenko@techmagic.co

TechMagic

CYBR

Using Prowler with Security Hub for AWS Assessments

Christophe Limpalair
Founder & Trainer
at Cybr



Victoria Shutenko
Security Engineer &
Web App Pentester at
TechMagic



🔒 About Cybr.com

Learn AWS cloud security hands-on

Access training Courses, 🧪 Hands-On Labs,
and Ebooks on AWS Cloud Security



Christophe Limpalair
Founder & Trainer at Cybr



Victoria Shutenko
Security Engineer & Web App Pentester at TechMagic



Resource Links

- Github demo project:
  - https://github.com/bjknbrrr/ProwlerCodeBuild
- Cybr's Hands-On Labs:
  - https://cybr.com/hands-on-labs
- Learn more about TechMagic Cyber Security Services:
  - https://www.techmagic.co/security-testing-services

TechMagic

CYBR





Thank you for attending!

Any questions?

Christophe Limpalair
https://linkedin.com/in/christophelimpalair

Victoria Shutenko
https://linkedin.com/in/victoria-s-a44050b8/

LIVE

Upcoming webinars
https://cybr.com/webinars