Information Security Policy

ShopSecure

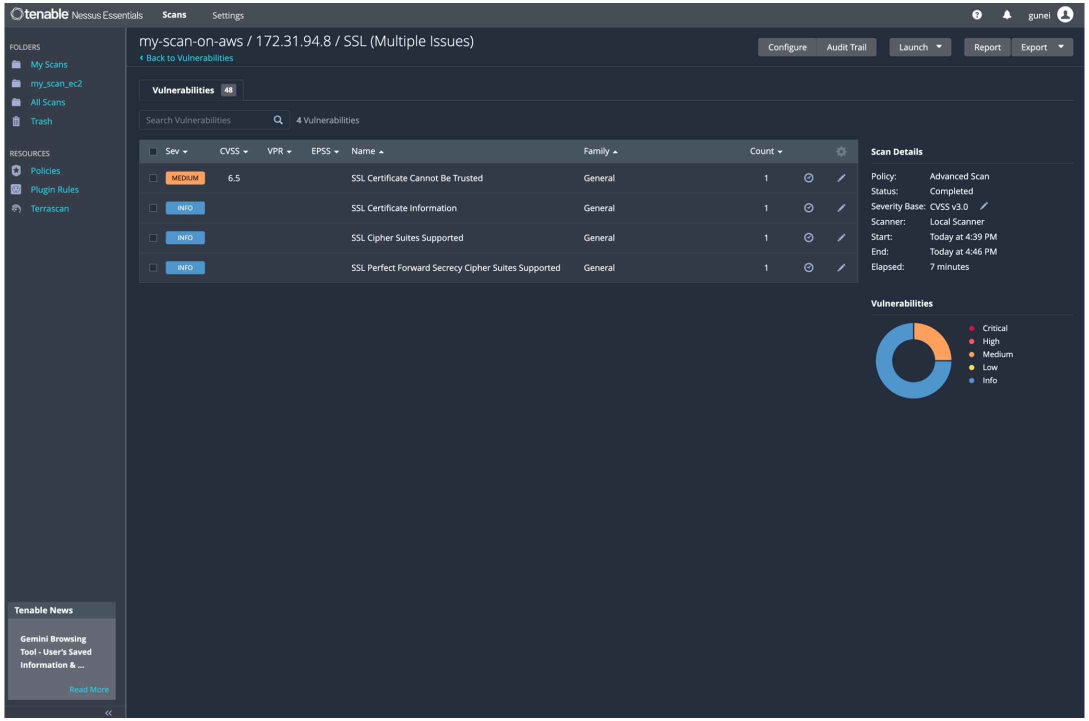
Overview

- Introduce ShopSecure and the GRC framework’s goals, setting the context for the presentation.
- ShopSecure Context: Fictional e-commerce startup with 50 employees, using AWS S3, EC2, and Splunk SIEM.
- GRC Goals: Ensure secure operations, mitigate risks (e.g., no MFA, public S3 buckets), and comply with ISO 27001/NIST CSF.
- Framework Scope: Uses Prowler, Nessus, Splunk, FAIR, COBIT, and MITRE ATT&CK to address risks in risk_analysis.xlsx.
- Objective: Reduce incidents by 20% and achieve 100% compliance within 6 months.

Risk Assessment (1)

- Summarize key findings from Prowler, Nessus, Splunk, and their mapping to STRIDE and MITRE ATT&CK, using risk_analysis.xlsx.
- Findings with high risk-score: No MFA (T1078.004, Risk Score: 20), public S3 buckets (T1133, Risk Score: 15), no CloudTrail logging (T1562.002, Risk Score: 12), untrusted SSL certificates (T1040, Risk Score: 25).
- Tools: Prowler (AWS misconfigurations), Nessus (vulnerabilities)
- STRIDE/MITRE ATT&CK being applied
- Impact: High-risk issues (e.g., S3 exposure, ALE: €27.6M–€51.5B) threaten data breaches, unauthorized access, severe financial loss.

Risk Assessment (2)



my-scan-on-aws / 172.31.94.8 / SSL (Multiple Issues)

‹ Back to Vulnerabilities

4 Vulnerabilities

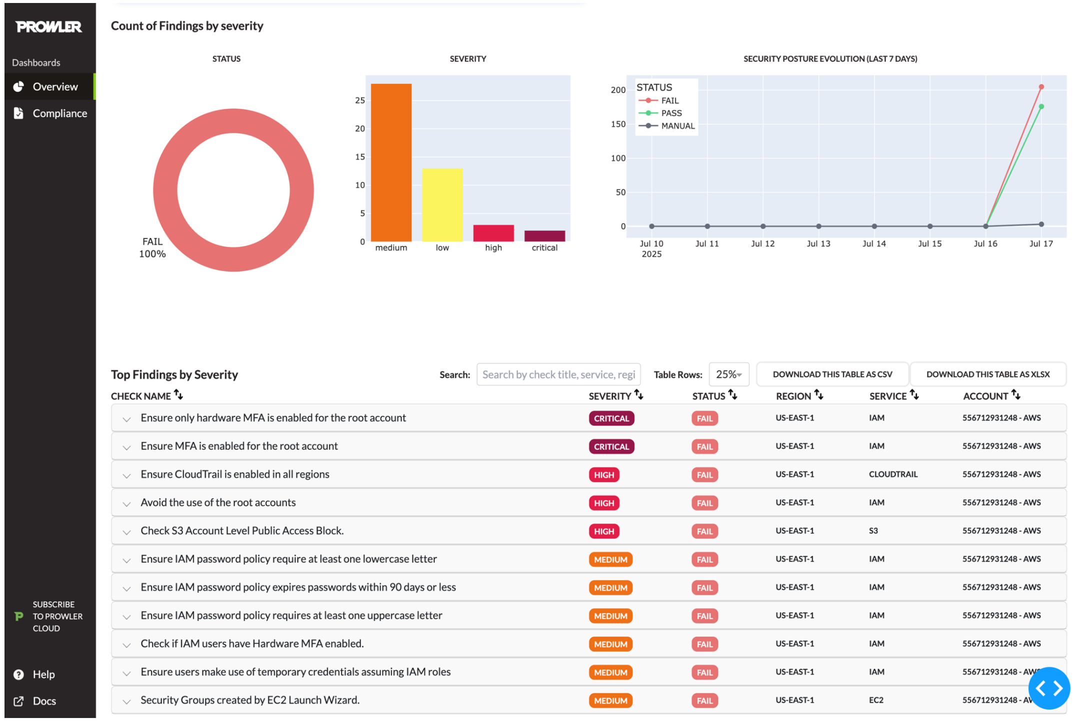
Sev	CVSS	VPR	EPSS	Name	Family	Count
MEDIUM	6.5			SSL Certificate Cannot Be Trusted	General	1
INFO				SSL Certificate Information	General	1
INFO				SSL Cipher Suites Supported	General	1
INFO				SSL Perfect Forward Secrecy Cipher Suites Supported	General	1

Scan Details

Policy:	Advanced Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 4:39 PM
End:	Today at 4:46 PM
Elapsed:	7 minutes

Vulnerabilities

Gemini Browsing Tool - User's Saved Information & ...

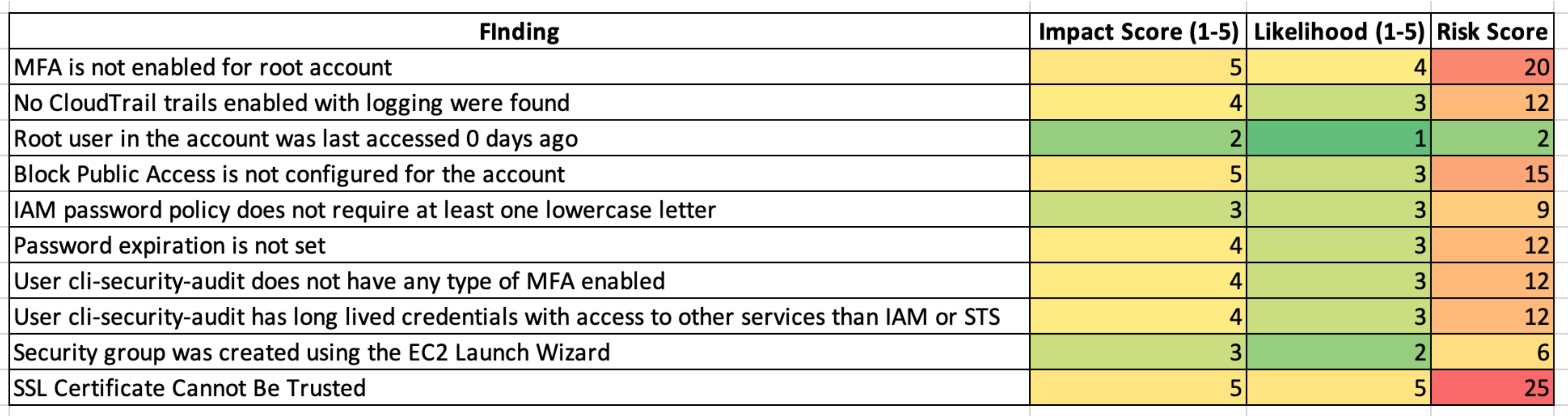


Count of Findings by severity

Top Findings by Severity

CHECK NAME	SEVERITY	STATUS	REGION	SERVICE	ACCOUNT
Ensure only hardware MFA is enabled for the root account	CRITICAL	FAIL	US-EAST-1	IAM	556712931248 - AWS
Ensure MFA is enabled for the root account	CRITICAL	FAIL	US-EAST-1	IAM	556712931248 - AWS
Ensure CloudTrail is enabled in all regions	HIGH	FAIL	US-EAST-1	CLOUDTRAIL	556712931248 - AWS
Avoid the use of the root accounts	HIGH	FAIL	US-EAST-1	IAM	556712931248 - AWS
Check S3 Account Level Public Access Block.	HIGH	FAIL	US-EAST-1	S3	556712931248 - AWS
Ensure IAM password policy require at least one lowercase letter	MEDIUM	FAIL	US-EAST-1	IAM	556712931248 - AWS
Ensure IAM password policy expires passwords within 90 days or less	MEDIUM	FAIL	US-EAST-1	IAM	556712931248 - AWS
Ensure IAM password policy requires at least one uppercase letter	MEDIUM	FAIL	US-EAST-1	IAM	556712931248 - AWS
Check if IAM users have Hardware MFA enabled.	MEDIUM	FAIL	US-EAST-1	IAM	556712931248 - AWS
Ensure users make use of temporary credentials assuming IAM roles	MEDIUM	FAIL	US-EAST-1	IAM	556712931248 - AW
Security Groups created by EC2 Launch Wizard.	MEDIUM	FAIL	US-EAST-1	EC2	556712931248 - A

Risk Assessment (3)

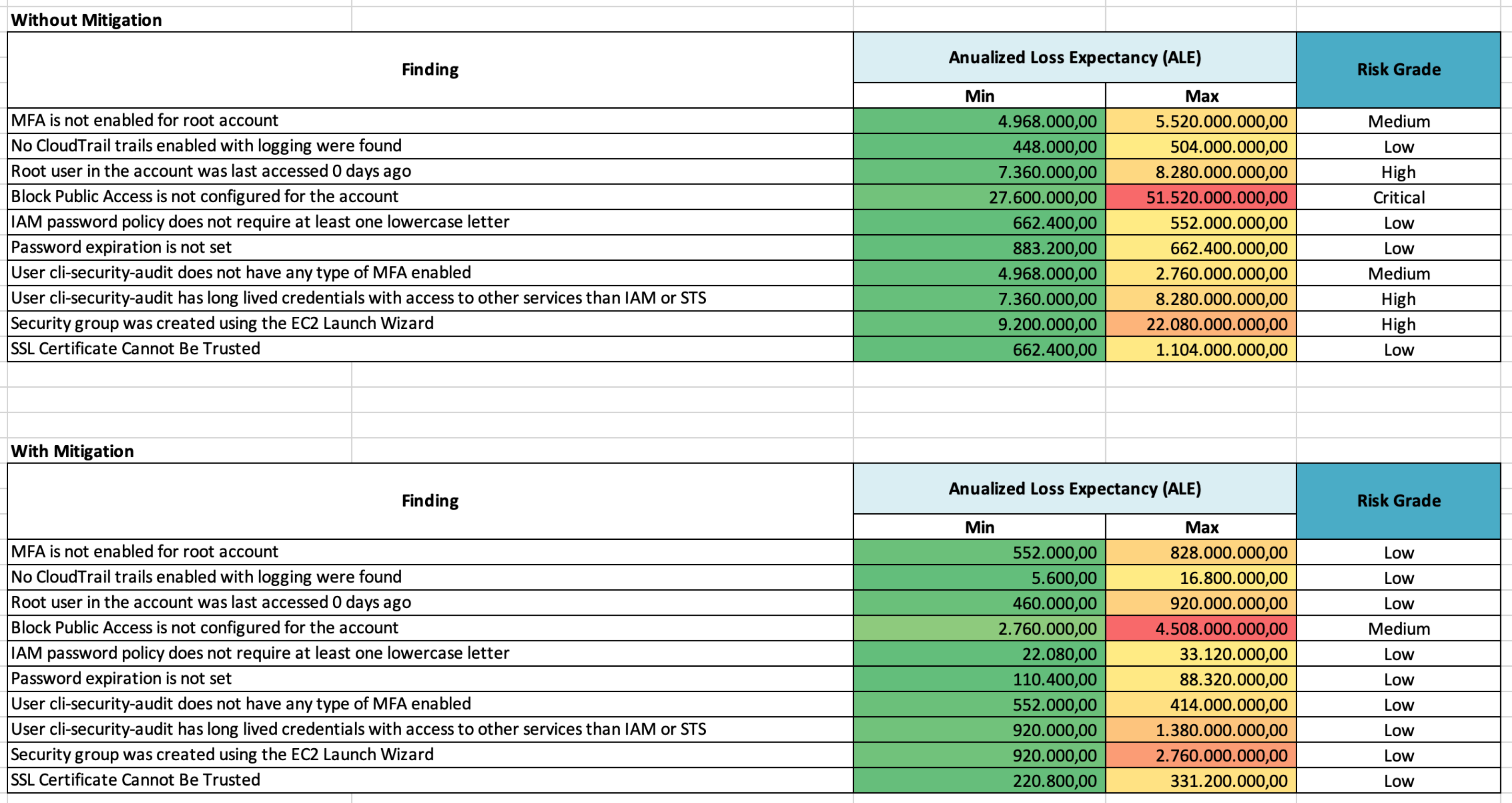


FInding	Impact Score (1-5)	Likelihood (1-5)	Risk Score
MFA is not enabled for root account	5	4	20
No CloudTrail trails enabled with logging were found	4	3	12
Root user in the account was last accessed 0 days ago	2	1	2
Block Public Access is not configured for the account	5	3	15
IAM password policy does not require at least one lowercase letter	3	3	9
Password expiration is not set	4	3	12
User cli-security-audit does not have any type of MFA enabled	4	3	12
User cli-security-audit has long lived credentials with access to other services than IAM or STS	4	3	12
Security group was created using the EC2 Launch Wizard	3	2	6
SSL Certificate Cannot Be Trusted	5	5	25

FAIR Analysis (1)

- Highlight risk quantification and mitigation impacts from the FAIR Analysis sheet in risk_analysis.xlsx.
- Critical Risks: Public S3 buckets (ALE: €27.6M–€51.5B, Critical), no MFA (ALE: €5.5M–€552M, Medium), untrusted SSL (ALE: €662K–€1.1B, Low).
- Mitigations: as mentioned in risk_analysis.xlsx -> FAIR Analysis
- Prioritization: Focus on high-ALE risks (S3, MFA) with cost-effective mitigations (e.g., €2,000 for S3, €1,000 for MFA).

FAIR Analysis (2)



Without Mitigation

Finding	Anualized Loss Expectancy (ALE)		Risk Grade
	Min	Max	
MFA is not enabled for root account	4.968.000,00	5.520.000.000,00	Medium
No CloudTrail trails enabled with logging were found	448.000,00	504.000.000,00	Low
Root user in the account was last accessed 0 days ago	7.360.000,00	8.280.000.000,00	High
Block Public Access is not configured for the account	27.600.000,00	51.520.000.000,00	Critical
IAM password policy does not require at least one lowercase letter	662.400,00	552.000.000,00	Low
Password expiration is not set	883.200,00	662.400.000,00	Low
User cli-security-audit does not have any type of MFA enabled	4.968.000,00	2.760.000.000,00	Medium
User cli-security-audit has long lived credentials with access to other services than IAM or STS	7.360.000,00	8.280.000.000,00	High
Security group was created using the EC2 Launch Wizard	9.200.000,00	22.080.000.000,00	High
SSL Certificate Cannot Be Trusted	662.400,00	1.104.000.000,00	Low

With Mitigation

Finding	Anualized Loss Expectancy (ALE)		Risk Grade
	Min	Max	
MFA is not enabled for root account	552.000,00	828.000.000,00	Low
No CloudTrail trails enabled with logging were found	5.600,00	16.800.000,00	Low
Root user in the account was last accessed 0 days ago	460.000,00	920.000.000,00	Low
Block Public Access is not configured for the account	2.760.000,00	4.508.000.000,00	Medium
IAM password policy does not require at least one lowercase letter	22.080,00	33.120.000,00	Low
Password expiration is not set	110.400,00	88.320.000,00	Low
User cli-security-audit does not have any type of MFA enabled	552.000,00	414.000.000,00	Low
User cli-security-audit has long lived credentials with access to other services than IAM or STS	920.000,00	1.380.000.000,00	Low
Security group was created using the EC2 Launch Wizard	920.000,00	2.760.000.000,00	Low
SSL Certificate Cannot Be Trusted	220.800,00	331.200.000,00	Low

GRC Framework

- Summarize the governance structure from grc_policy.docx, aligned with COBIT, ISO/IEC 27001:2022, NIST CSF, and MITRE ATT&CK.
- Governance: CISO oversees SIEM system; IT team implements mitigations, CEO reviews quarterly
- Processes: Monthly risk reviews, 24-hour incident response.
- KPIs: 100% MFA, 100% S3 Block Public Access, 90% alert resolution.
- Standards: ISO/IEC 27001:2022, NIST CSF, mitigates all MITTRE ATT&CK findings.

Outlook

- Outline actionable recommendations and timelines based on risk_analysis.xlsx mitigations.
- Prioritize Mitigations: Enable MFA (€1,000, T1078.004), S3 Block Public Access (€2,000, T1133), CloudTrail logging (€1,000, T1562.002) by 01/10/2025.
- Enhance SIEM: Deploy a system correlation rules (e.g., failed logins >10).
- Compliance: Achieve ISO 27001 and NIST CSF certification within 6 months.
- Monitoring: Conduct monthly Prowler/Nessus scans, quarterly CEO reviews.