



---

# MITRE ATT&CK Report

REPORT:  
**AIQ REPORT**


ASSESSMENT:  
**FIN6**

---

Report Generated on  
**01/27/2024 - 08:58 pm (UTC)**


Report Generated by:  
**username: IVAN NATHAN**  
**email: ivannathan56@gmail.com**

OVERALL STATUS




16

UNIQUE SCENARIOS




2

TOTAL ASSETS




32

TOTAL RESULTS



2

PREVENTED









13

DETECTED

## TEST OVERVIEW

Total tests (8)

TESTS	SCENARIOS	USER PRIVILEGES*	ASSETS	TECHNOLOGIES	PREVENTION	DETECTION
Execution	2	SYSTEM	2		<div><div></div></div> 100%	<div><div></div><div></div></div> 50%50%
Persistence	1	SYSTEM	2		<div><div></div></div> 100%	<div><div></div><div></div></div> 50%50%
Defense Evasion	2	SYSTEM	2		<div><div></div></div> 100%	<div><div></div><div></div></div> 50%50%
Credential Access	1	SYSTEM	2	No detections	<div><div></div></div> 100%	<div><div></div></div> 100%
Discovery	5	SYSTEM	2		<div><div></div><div></div></div> 20%80%	<div><div></div><div></div></div> 50%50%
Collection	2	SYSTEM	2		<div><div></div></div> 100%	<div><div></div><div></div><div></div></div> 25%50%25%
Command And Control	1	SYSTEM	2		<div><div></div></div> 100%	<div><div></div><div></div></div> 50%50%
Exfiltration	2	SYSTEM	2	No detections	<div><div></div></div> 100%	<div><div></div></div> 100%

\* User Privileges are SYSTEM for Linux and MacOS assets

Prevented

Not Prevented

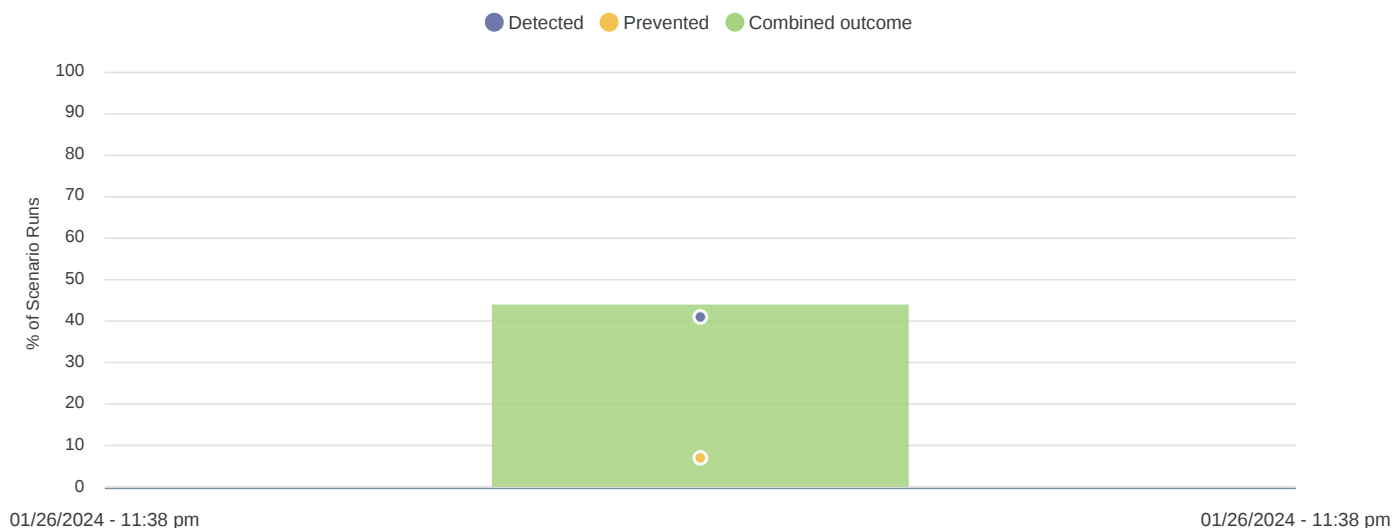
Other

Detected

Not Detected

Other

## HISTORICAL RUN RESULTS



## MITRE PREVENTION RESULTS HEATMAP

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
	Command and Scripting Interpreter 05 Scenarios 0% Prevented	Boot or Logon Automation Execution 01 Scenarios 0% Prevented		Masquerading 01 Scenarios 0% Prevented	OS Credential Dumping 01 Scenarios 0% Prevented	Network Service Scanning 01 Scenarios 34% Prevented		Archive Collected Data 02 Scenarios 0% Prevented	Application Layer Protocol 03 Scenarios 0% Prevented	Automated Exfiltration 01 Scenarios 0% Prevented	
	PowerShell 0% Prevented	Registry Run Keys / Startup Folder 0% Prevented		Match Legitimate Name or Location 0% Prevented	NTDS 0% Prevented	Permission Groups Discovery 01 Scenarios 34% Prevented		Archive via Library 0% Prevented	Web Protocols 0% Prevented		
	Windows Command Shell 0% Prevented			Modify Registry 01 Scenarios 0% Prevented		Local Groups 0% Prevented		Archive via Custom Method 01 Scenarios 0% Prevented	Non-Standard Port 01 Scenarios 0% Prevented		
	Scheduled Task/Job 01 Scenarios 0% Prevented			Subvert Trust Controls 01 Scenarios 0% Prevented		Domain Groups 0% Prevented		Automated Collection 01 Scenarios 0% Prevented	Web Service 01 Scenarios 0% Prevented		
	Scheduled Task 0% Prevented			Code Signing 0% Prevented		Remote System Discovery 01 Scenarios 34% Prevented		Data Staged 01 Scenarios 0% Prevented	Bidirectional Communication 0% Prevented		
	System Services 01 Scenarios 0% Prevented										
	Service Execution 0% Prevented										
	Windows Management Instrumentation 03 Scenarios 0% Prevented										

MITRE DETECTION RESULTS HEATMAP



MITRE ATT&CK TACTIC RESULTS (AMONG ALL ASSETS EXERCISED)

No Results

\* Percentages are truncated

# THREAT ASSESSMENT (AMONG ALL ASSETS EXERCISED)



Execution  
100% not blocked (4)



Persistence  
100% not blocked (2)



Defense Evasion  
100% not blocked (4)



Credential Access  
100% other (2)



Discovery  
20% blocked (2)  
80% not blocked (8)



Collection  
100% not blocked (4)



Command And Control  
100% not blocked (2)



Exfiltration  
100% not blocked (4)

*\* Percentages are truncated*

# EFFECTIVENESS OF SECURITY TECHNOLOGIES

AttackIQ measured the detection efficacy for the security technologies responsible for securing your organization.

Not all scenario runs have detection results: *(Why? AttackIQ does not currently support detection for all scenarios)*

	<div>Panorama (Via PAN Panorama)</div> <div>6 of 32 scenario runs support detection results</div>	<div>0.0%</div> <div>detected</div>	<div>100.0%</div> <div>(6 not detected)</div>
	<div>CB EDR</div> <div>13 of 32 scenario runs support detection results</div>	<div>100.0%</div> <div>(13 detected)</div>	<div>0.0%</div> <div>not detected</div>

Scenario runs without detection results are not represented in the above percentages.

