ARMOR | SECURECON 2019 | DALLAS, TEXAS

REALIZING VALUE FROM THE ARMOR SOC

CHRIS STOUFF

Chief Security Officer

AGENDA

1 Intro

2 Every Client is Unique

3 SOC & TRU

4 Realizing Value

5 Q & A

ARMOR. MAKING CLOUD SECURITY SIMPLE
I want to learn more about
SECURITY-AS-A-SERVICE
SECURE HOSTING
LOGIN
Armor Defense, Inc.

CHRIS STOUFF

Chief Security Officer

Contact me at:
chris.stouff@armor.com

EVERY CLIENT IS UNIQUE.

SNOWFLAKES.

http://thescienceexplorer.com/nature/snowflakes-are-not-unique-we-thought

ARMOR SECURITY OPERATIONS

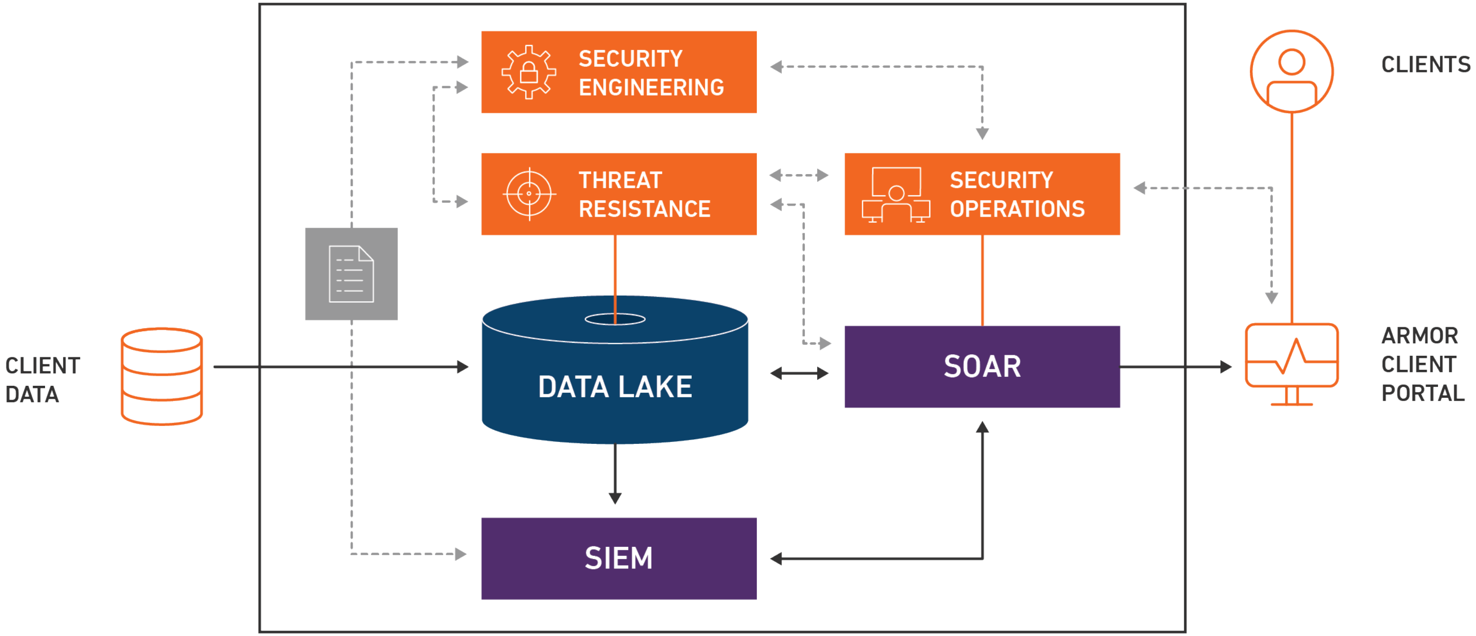
1 24/7 Detection

2 Incident Response

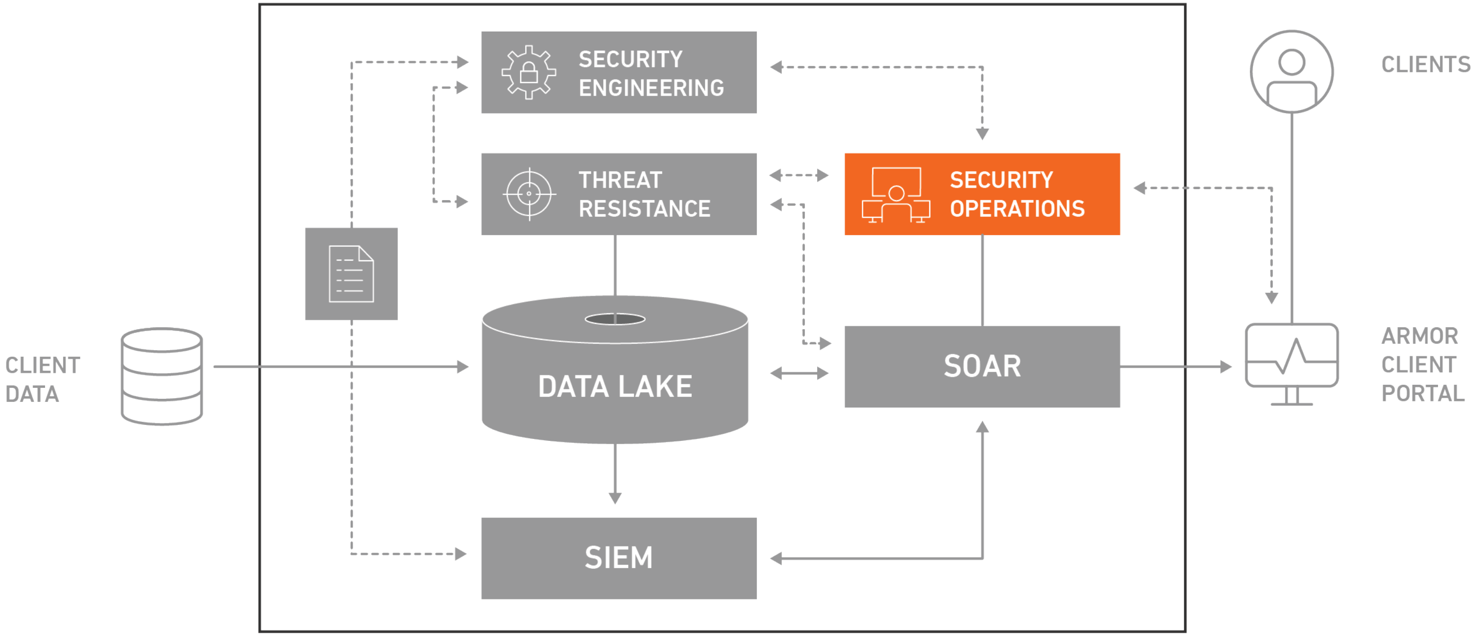
3 Remediation

SOC & TRU

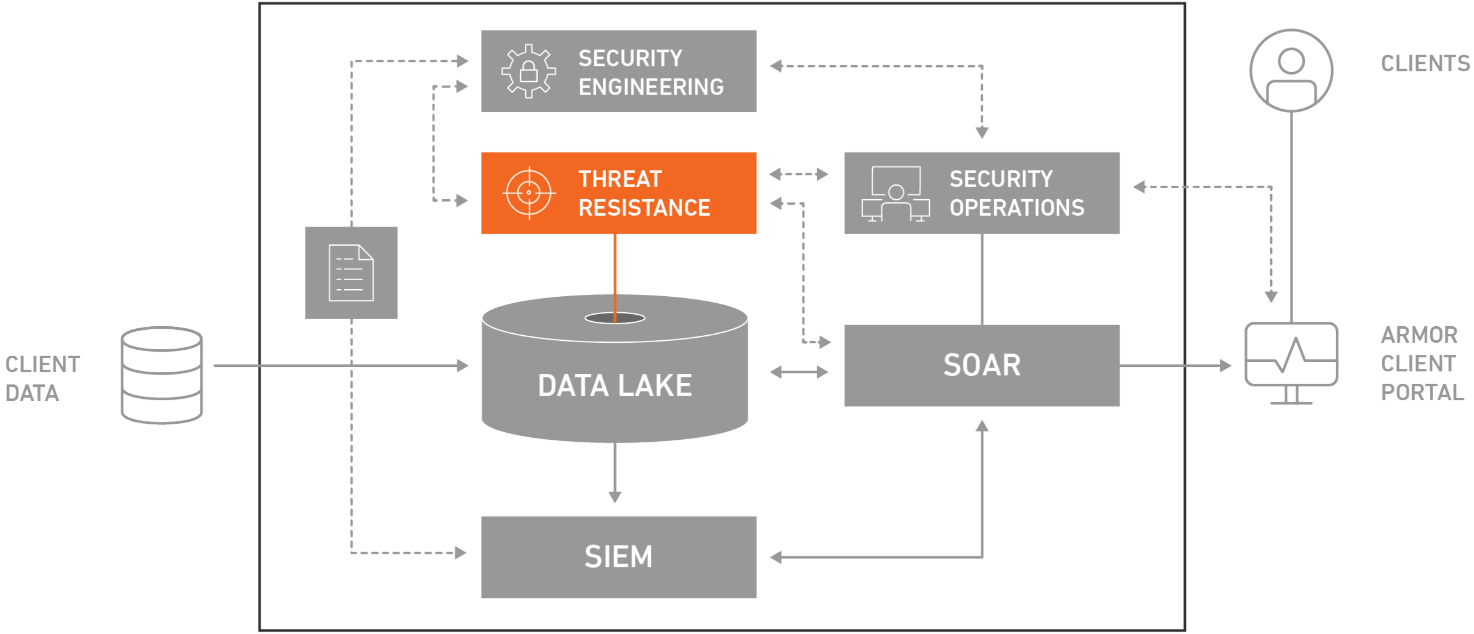
THE ART OF DETECTION



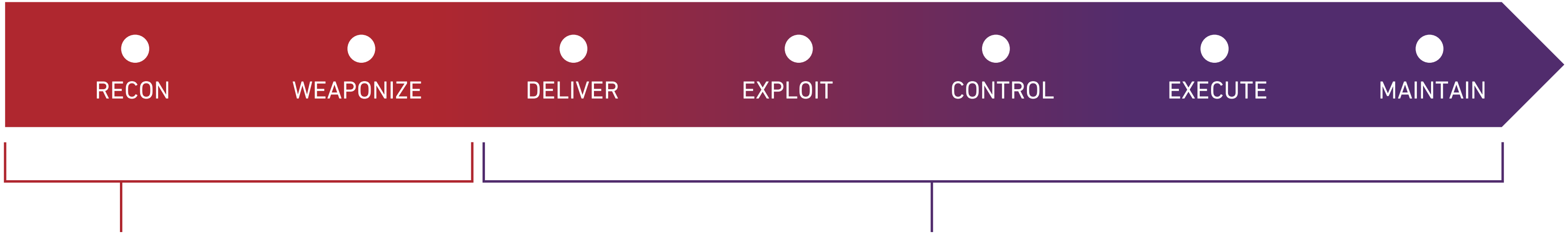
DETECTION & RESPONSE



THREAT INTELLIGENCE & HUNTING



THE ART OF DETECTION – USING MITRE ATT&CK FRAMEWORK



RECON

WEAPONIZE

DELIVER

EXPLOIT

CONTROL

EXECUTE

MAINTAIN

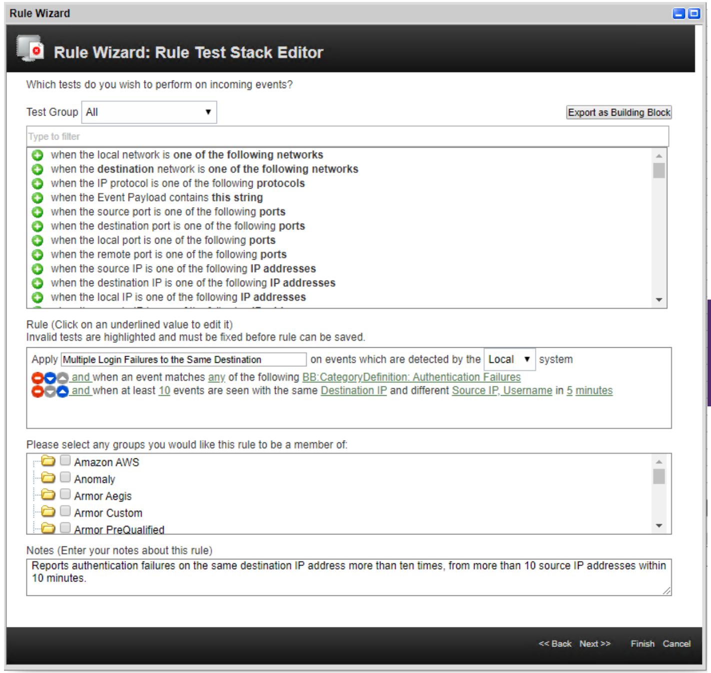
PRE-ATT&CK™

- Priority Definition: Planning, Direction
- Target Selection
- Information Gathering: Technical, People, Organizational
- Weakness Identification: Technical, People, Organizational
- Adversary OpSec
- Establish & Maintain Infrastructure
- Persona Development
- Build Capabilities
- Test Capabilities
- Stage Capabilities

ENTERPRISE-ATT&CK

- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Exfiltration
- Command & Control

BRUTE FORCE ATTACK - T1110



Rule Wizard

Rule Wizard: Rule Test Stack Editor

Which tests do you wish to perform on incoming events?

Test Group: All ▾ — Export as Building Block

Type to filter

- when the local network is **one of the following networks**
- when the **destination** network is **one of the following networks**
- when the IP protocol is one of the following **protocols**
- when the Event Payload contains **this string**
- when the source port is one of the following **ports**
- when the destination port is one of the following **ports**
- when the local port is one of the following **ports**
- when the remote port is one of the following **ports**
- when the source IP is one of the following **IP addresses**
- when the destination IP is one of the following **IP addresses**
- when the local IP is one of the following **IP addresses**

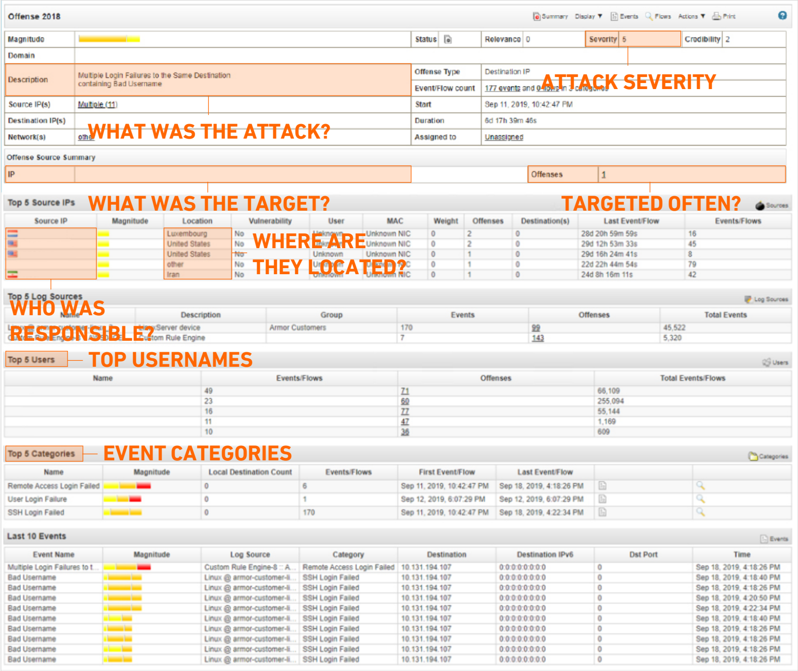
Rule (Click on an underlined value to edit it)
Invalid tests are highlighted and must be fixed before rule can be saved.

Apply Multiple Login Failures to the Same Destination on events which are detected by the Local ▾ system
and when an event matches any of the following BB:CategoryDefinition: Authentication Failures
and when at least 10 events are seen with the same Destination IP and different Source IP, Username in 5 minutes

Please select any groups you would like this rule to be a member of:

- □ Amazon AWS
- □ Anomaly
- □ Armor Aegis
- □ Armor Custom
- □ Armor PreQualified

Notes (Enter your notes about this rule)
Reports authentication failures on the same destination IP address more than ten times, from more than 10 source IP addresses within 10 minutes.



Offense 2018

Magnitude		Status		Relevance	0	Severity 5	Credibility 2
Domain							
Description	Multiple Login Failures to the Same Destination containing Bad Username	Offense Type	Destination IP				
		Event/Flow count	177 events and 0 flows in 3 categories				
Source IP(s)	Multiple (11)	Start	Sep 11, 2019, 10:42:47 PM				
Destination IP(s)		Duration	6d 17h 39m 46s				
Network(s)	other	Assigned to	Unassigned				

Offense Source Summary

IP		Offenses	1

Top 5 Source IPs

Source IP	Magnitude	Location	Vulnerability	User	MAC	Weight	Offenses	Destination(s)	Last Event/Flow	Events/Flows
		Luxembourg	No	Unknown	Unknown NIC	0	2	0	28d 20h 59m 59s	16
		United States	No	Unknown	Unknown NIC	0	2	0	29d 12h 53m 33s	45
		United States	No	Unknown	Unknown NIC	0	1	0	29d 16h 24m 41s	8
		other	No	Unknown	Unknown NIC	0	1	0	22d 22h 44m 54s	79
		Iran	No	Unknown	Unknown NIC	0	1	0	24d 8h 16m 11s	42

Top 5 Log Sources

Name	Description	Group	Events	Offenses	Total Events
Linux @ armor-customer-linux-[illegible]	LinuxServer device	Armor Customers	170	99	45,522
Custom Rule Engine-8 :: AWSQRADAR[illegible]	Custom Rule Engine		7	143	5,320

Top 5 Users

Name	Events/Flows	Offenses	Total Events/Flows
	49	71	66,109
	23	60	255,094
	16	77	55,144
	11	47	1,169
	10	36	609

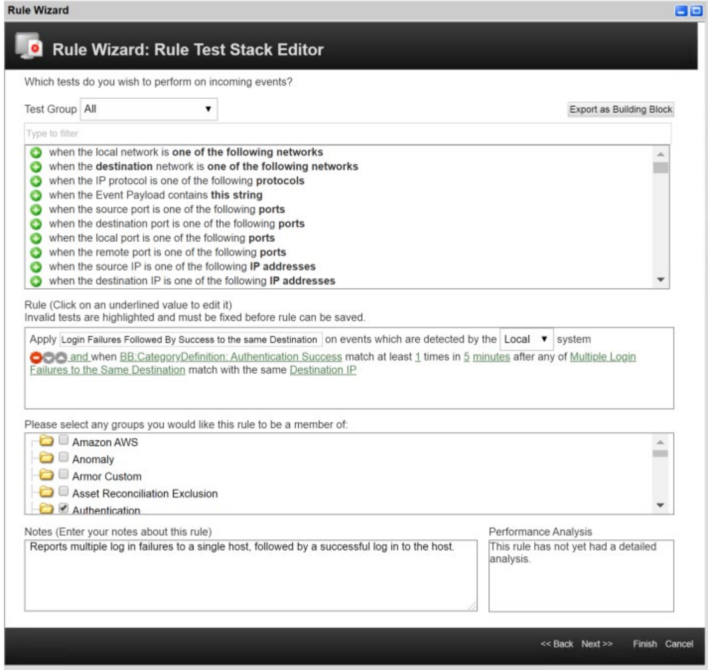
Top 5 Categories

Name	Magnitude	Local Destination Count	Events/Flows	First Event/Flow	Last Event/Flow		
Remote Access Login Failed		0	6	Sep 11, 2019, 10:42:47 PM	Sep 18, 2019, 4:18:26 PM		
User Login Failure		0	1	Sep 12, 2019, 6:07:29 PM	Sep 12, 2019, 6:07:29 PM		
SSH Login Failed		0	170	Sep 11, 2019, 10:42:47 PM	Sep 18, 2019, 4:22:34 PM		

Last 10 Events

Event Name	Magnitude	Log Source	Category	Destination	Destination IPv6	Dst Port	Time
Multiple Login Failures to t...		Custom Rule Engine-8 :: A...	Remote Access Login Failed	10.131.194.107	0:0:0:0:0:0:0:0	0	Sep 18, 2019, 4:18:26 PM
Bad Username		Linux @ armor-customer-li...	SSH Login Failed	10.131.194.107	0:0:0:0:0:0:0:0	0	Sep 18, 2019, 4:18:40 PM
Bad Username		Linux @ armor-customer-li...	SSH Login Failed	10.131.194.107	0:0:0:0:0:0:0:0	0	Sep 18, 2019, 4:18:26 PM
Bad Username		Linux @ armor-customer-li...	SSH Login Failed	10.131.194.107	0:0:0:0:0:0:0:0	0	Sep 18, 2019, 4:20:50 PM
Bad Username		Linux @ armor-customer-li...	SSH Login Failed	10.131.194.107	0:0:0:0:0:0:0:0	0	Sep 18, 2019, 4:22:34 PM
Bad Username		Linux @ armor-customer-li...	SSH Login Failed	10.131.194.107	0:0:0:0:0:0:0:0	0	Sep 18, 2019, 4:18:40 PM
Bad Username		Linux @ armor-customer-li...	SSH Login Failed	10.131.194.107	0:0:0:0:0:0:0:0	0	Sep 18, 2019, 4:18:26 PM
Bad Username		Linux @ armor-customer-li...	SSH Login Failed	10.131.194.107	0:0:0:0:0:0:0:0	0	Sep 18, 2019, 4:18:26 PM
Bad Username		Linux @ armor-customer-li...	SSH Login Failed	10.131.194.107	0:0:0:0:0:0:0:0	0	Sep 18, 2019, 4:18:26 PM
Bad Username		Linux @ armor-customer-li...	SSH Login Failed	10.131.194.107	0:0:0:0:0:0:0:0	0	Sep 18, 2019, 4:18:26 PM

SUCCESSFUL BRUTE FORCE - T1110



Rule Wizard: Rule Test Stack Editor

Which tests do you wish to perform on incoming events?

Test Group: All ▾ | Export as Building Block

Type to filter

- when the local network is **one of the following networks**
- when the **destination** network is **one of the following networks**
- when the IP protocol is one of the following **protocols**
- when the Event Payload contains **this string**
- when the source port is one of the following **ports**
- when the destination port is one of the following **ports**
- when the local port is one of the following **ports**
- when the remote port is one of the following **ports**
- when the source IP is one of the following **IP addresses**
- when the destination IP is one of the following **IP addresses**

Rule (Click on an underlined value to edit it)
Invalid tests are highlighted and must be fixed before rule can be saved.

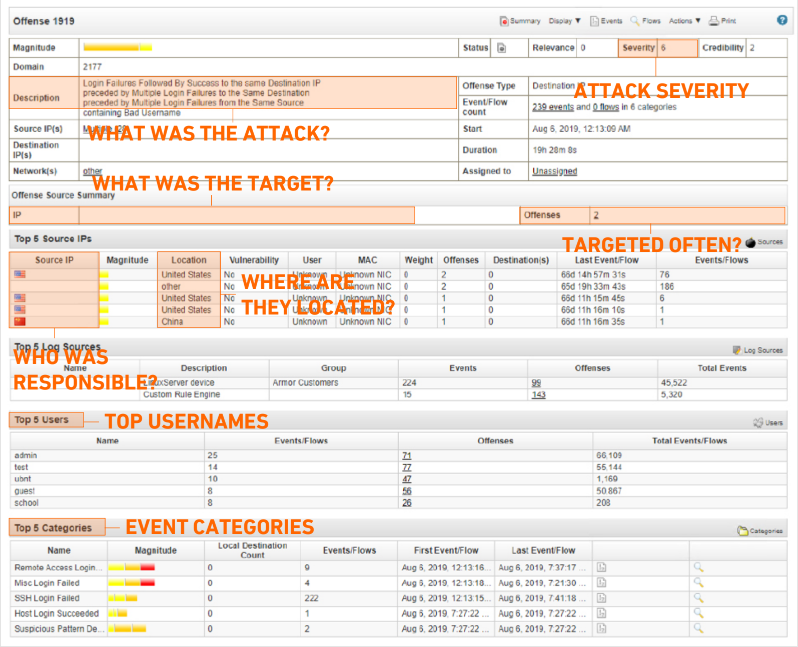
Apply Login Failures Followed By Success to the same Destination on events which are detected by the Local ▾ system
and when BB:CategoryDefinition: Authentication Success match at least 1 times in 5 minutes after any of Multiple Login Failures to the Same Destination match with the same Destination IP

Please select any groups you would like this rule to be a member of:

- □ Amazon AWS
- □ Anomaly
- □ Armor Custom
- □ Asset Reconciliation Exclusion
- ☑ Authentication

Notes (Enter your notes about this rule)
Reports multiple log in failures to a single host, followed by a successful log in to the host.

Performance Analysis
This rule has not yet had a detailed analysis.



Offense 1919

Magnitude		Status		Relevance	0	Severity	6	Credibility	2
Domain	2177								
Description	Login Failures Followed By Success to the same Destination IP preceded by Multiple Login Failures to the Same Destination preceded by Multiple Login Failures from the Same Source containing Bad Username	Offense Type	Destination IP						
		Event/Flow count	239 events and 0 flows in 6 categories						
Source IP(s)	Multiple (28)	Start	Aug 6, 2019, 12:13:09 AM						
Destination IP(s)		Duration	19h 28m 8s						
Network(s)	other	Assigned to	Unassigned						

ATTACK SEVERITY

WHAT WAS THE ATTACK?

WHAT WAS THE TARGET?

Offense Source Summary

IP		Offenses	2

TARGETED OFTEN?

Top 5 Source IPs

Source IP	Magnitude	Location	Vulnerability	User	MAC	Weight	Offenses	Destination(s)	Last Event/Flow	Events/Flows
		United States	No	Unknown	Unknown NIC	0	2	0	66d 14h 57m 31s	76
		other	No	Unknown	Unknown NIC	0	2	0	65d 19h 33m 43s	186
		United States	No	Unknown	Unknown NIC	0	1	0	66d 11h 15m 45s	6
		United States	No	Unknown	Unknown NIC	0	1	0	66d 11h 16m 10s	1
		China	No	Unknown	Unknown NIC	0	1	0	66d 11h 16m 35s	1

WHERE ARE THEY LOCATED?

Top 5 Log Sources

WHO WAS RESPONSIBLE?

Name	Description	Group	Events	Offenses	Total Events
	LinuxServer device	Armor Customers	224	99	45,522
	Custom Rule Engine		15	143	5,320

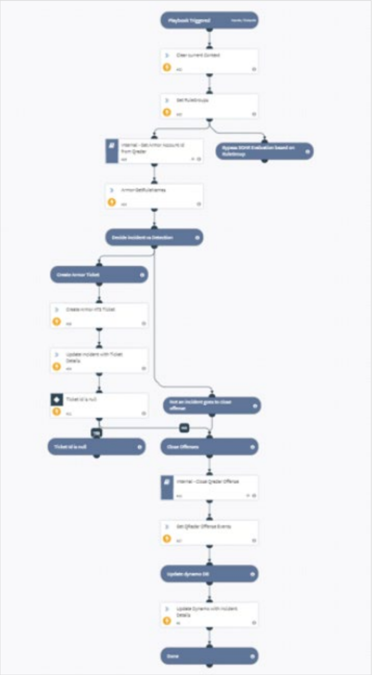
Top 5 Users — TOP USERNAMES

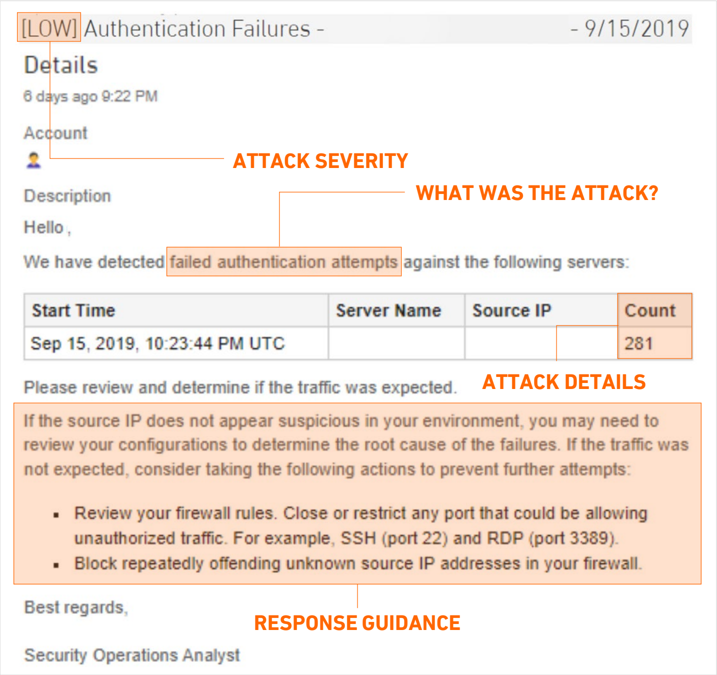
Name	Events/Flows	Offenses	Total Events/Flows
admin	25	71	66,109
test	14	77	55,144
ubnt	10	47	1,169
guest	8	56	50,867
school	8	26	208

Top 5 Categories — EVENT CATEGORIES

Name	Magnitude	Local Destination Count	Events/Flows	First Event/Flow	Last Event/Flow
Remote Access Login...		0	9	Aug 6, 2019, 12:13:16...	Aug 6, 2019, 7:37:17 ...
Misc Login Failed		0	4	Aug 6, 2019, 12:13:18...	Aug 6, 2019, 7:21:30 ...
SSH Login Failed		0	222	Aug 6, 2019, 12:13:15...	Aug 6, 2019, 7:41:18 ...
Host Login Succeeded		0	1	Aug 6, 2019, 7:27:22 ...	Aug 6, 2019, 7:27:22 ...
Suspicious Pattern De...		0	2	Aug 6, 2019, 7:27:22 ...	Aug 6, 2019, 7:27:22 ...

BRUTE FORCE ATTACK - T1110


Playbook Triggered
Clear current Context
Set RuleGroups
Internal - Get Armor Account Id from Qradar
Bypass SOAR Evaluation based on Rulegroup
Armor-GetRuleNames
Decide Incident vs Detection
Create Armor Ticket
Create Armor HTS Ticket
Update incident with Ticket Details
Ticket id is null
Not an incident goes to close offense
Ticket id is null
Close Offenses
Internal - Close Qradar Offense
Get QRadar Offense Events
Update dynamo DB
Update Dynamo with incident Details
Done



[LOW] Authentication Failures - - 9/15/2019

Details

6 days ago 9:22 PM

Account

Description

Hello ,

We have detected failed authentication attempts against the following servers:

Start Time	Server Name	Source IP	Count
Sep 15, 2019, 10:23:44 PM UTC			281

Please review and determine if the traffic was expected.

If the source IP does not appear suspicious in your environment, you may need to review your configurations to determine the root cause of the failures. If the traffic was not expected, consider taking the following actions to prevent further attempts:

- Review your firewall rules. Close or restrict any port that could be allowing unauthorized traffic. For example, SSH (port 22) and RDP (port 3389).
- Block repeatedly offending unknown source IP addresses in your firewall.

Best regards,

Security Operations Analyst

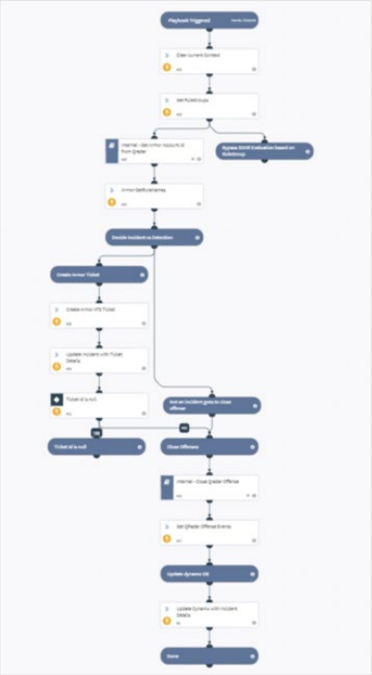
ATTACK SEVERITY

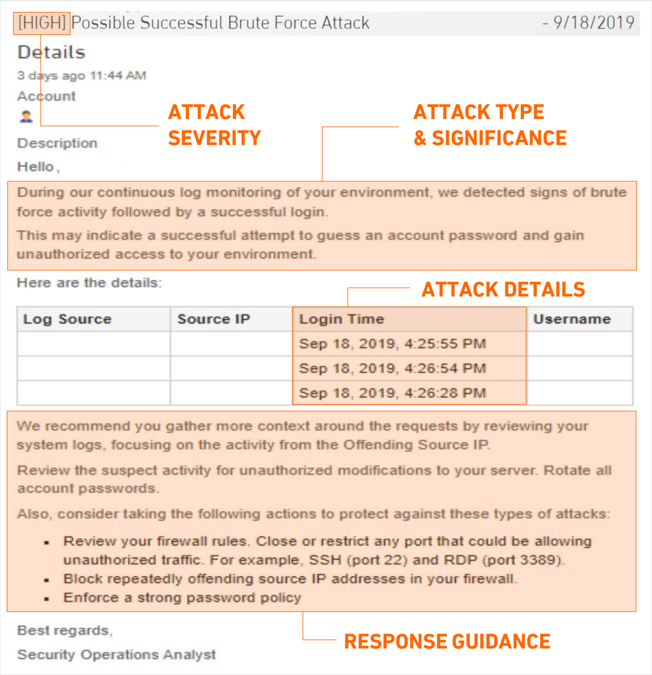
WHAT WAS THE ATTACK?

ATTACK DETAILS

RESPONSE GUIDANCE

SUCCESSFUL BRUTE FORCE - T1110


Playbook Triggered
Clear current Context
Set RuleGroups
Internal - Get Armor Account Id from Qradar
Bypass SOAR Evaluation based on RuleGroup
Armor GetRuleNames
Decide Incident vs Detection
Create Armor Ticket
Create Armor HTS Ticket
Update incident with Ticket Details
Ticket id is null
Not an incident goes to close offense
Ticket id is null
Close Offenses
Internal - Close Qradar Offense
Get QRadar Offense Events
Update dynamo DB
Update Dynamo with incident Details
Done



[HIGH] Possible Successful Brute Force Attack - 9/18/2019

Details

3 days ago 11:44 AM

Account

Description

Hello ,

During our continuous log monitoring of your environment, we detected signs of brute force activity followed by a successful login.

This may indicate a successful attempt to guess an account password and gain unauthorized access to your environment.

Here are the details:

Log Source	Source IP	Login Time	Username
		Sep 18, 2019, 4:25:55 PM	
		Sep 18, 2019, 4:26:54 PM	
		Sep 18, 2019, 4:26:28 PM	

We recommend you gather more context around the requests by reviewing your system logs, focusing on the activity from the Offending Source IP.

Review the suspect activity for unauthorized modifications to your server. Rotate all account passwords.

Also, consider taking the following actions to protect against these types of attacks:

- Review your firewall rules. Close or restrict any port that could be allowing unauthorized traffic. For example, SSH (port 22) and RDP (port 3389).
- Block repeatedly offending source IP addresses in your firewall.
- Enforce a strong password policy

Best regards,

Security Operations Analyst

ATTACK SEVERITY

ATTACK TYPE & SIGNIFICANCE

ATTACK DETAILS

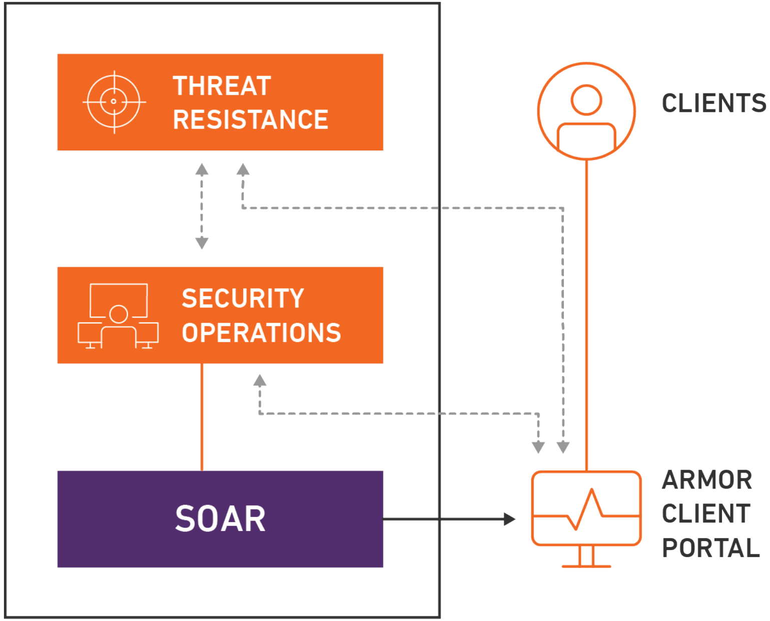
RESPONSE GUIDANCE

CONTINUE THE CONVERSATION ...

- Continuous Care & Feeding
- Tailored Security Outcomes

COMPROMISE OR BREACH?

- Threat Resistance advanced IR support
- Guide Client through IR process

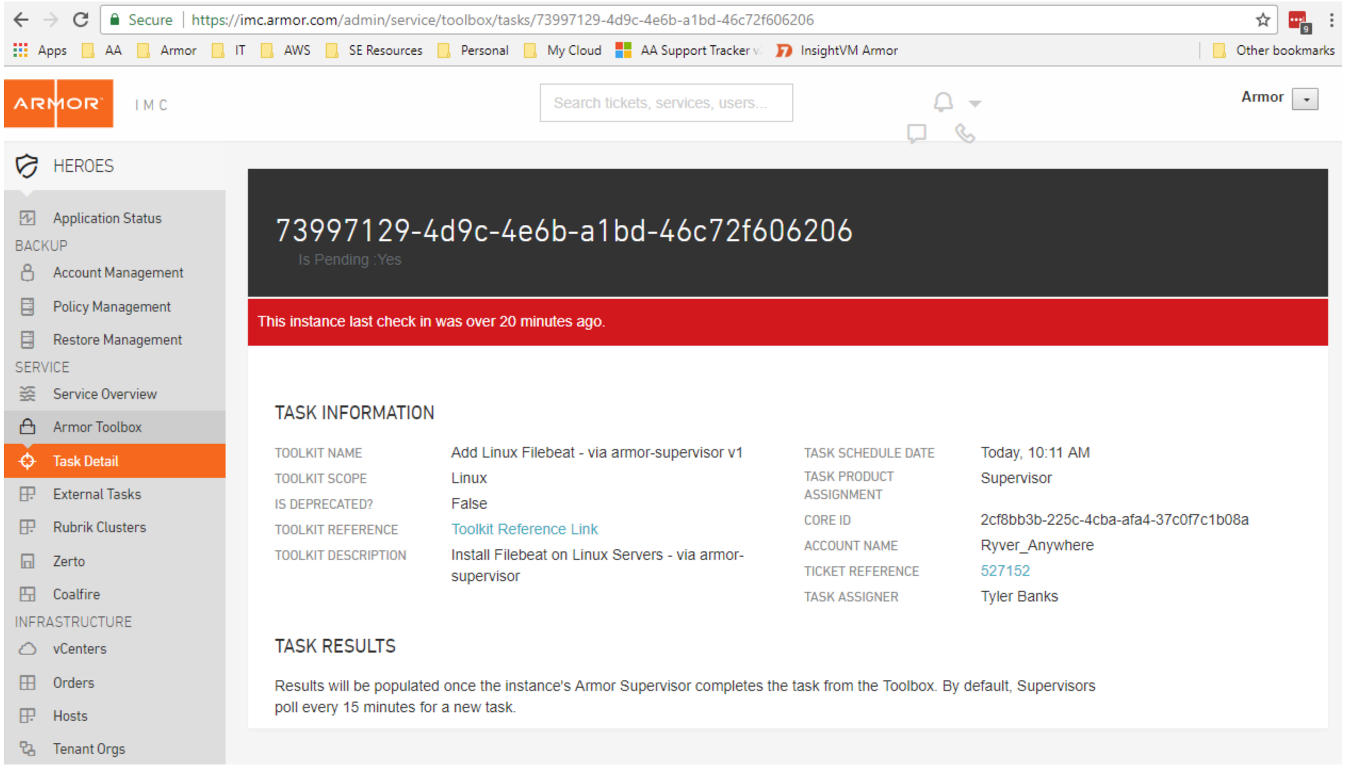


REALIZING VALUE

BROKEN MOLDS

credits: istockphoto/gorodenkoff

ARMOR TOOLBOX



73997129-4d9c-4e6b-a1bd-46c72f606206

Is Pending :Yes

This instance last check in was over 20 minutes ago.

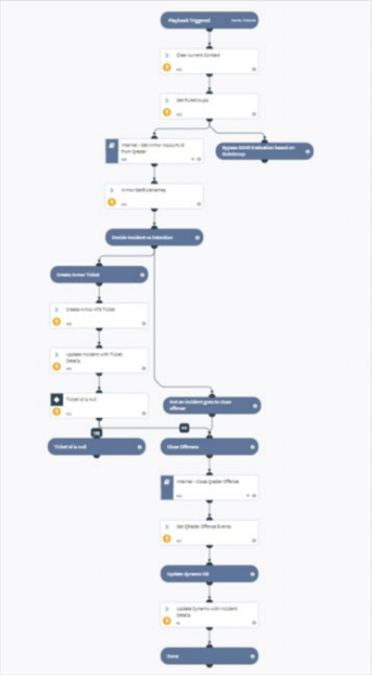
TASK INFORMATION

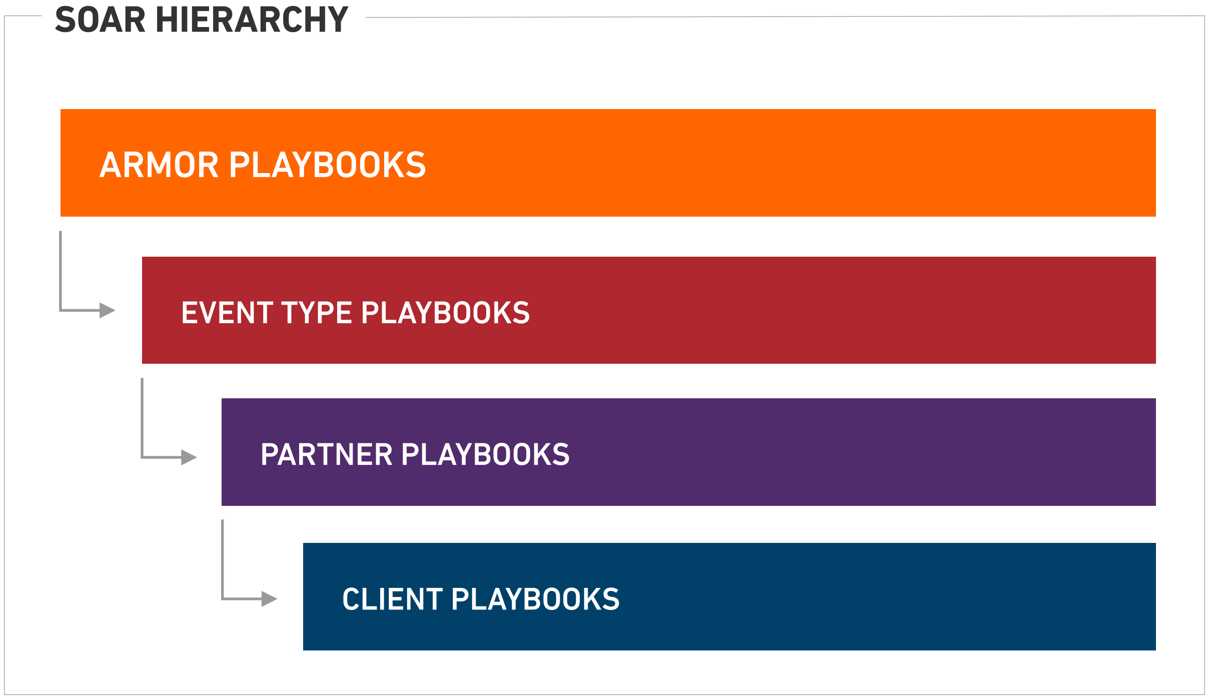
TOOLKIT NAME	Add Linux Filebeat - via armor-supervisor v1	TASK SCHEDULE DATE	Today, 10:11 AM
TOOLKIT SCOPE	Linux	TASK PRODUCT ASSIGNMENT	Supervisor
IS DEPRECATED?	False	CORE ID	2cf8bb3b-225c-4cba-afa4-37c0f7c1b08a
TOOLKIT REFERENCE	Toolkit Reference Link	ACCOUNT NAME	Ryver_Anywhere
TOOLKIT DESCRIPTION	Install Filebeat on Linux Servers - via armor-supervisor	TICKET REFERENCE	527152
		TASK ASSIGNER	Tyler Banks

TASK RESULTS

Results will be populated once the instance's Armor Supervisor completes the task from the Toolbox. By default, Supervisors poll every 15 minutes for a new task.

SECURITY ORCHESTRATION, AUTOMATION & RESPONSE (SOAR)


Playbook Triggered
Clear current Context
Set RuleGroups
Internal - Get Armor Account Id from Qradar
Bypass SOAR Evaluation based on RuleGroup
Armor-GetRuleNames
Decide Incident vs Detection
Create Armor Ticket
Create Armor HTS Ticket
Update incident with Ticket Details
Ticket id is null
Not an incident goes to close offense
Ticket id is null
Close Offenses
Internal - Close Qradar Offense
Get QRadar Offense Events
Update dynamo DB
Update Dynamo with incident Details
Done



SOAR HIERARCHY

ARMOR PLAYBOOKS

EVENT TYPE PLAYBOOKS

PARTNER PLAYBOOKS

CLIENT PLAYBOOKS

Q & A

CHRIS STOUFF

Chief Security Officer

ARMOR

SECURECON
2019 | DALLAS, TEXAS

THANK YOU.

WWW.ARMOR.COM