ARMOR | SECURECON 2019 | DALLAS, TEXAS

HOW ARMOR UTILIZES THE SIEM TO PROVIDE SECURITY AT SCALE:

A LOOK INTO SCALABLE SECURITY PRACTICES

NICK ROBINETT

Product Owner

PAUL SROUFE

Director of Engineering

AGENDA

1. Event Abstraction
2. Event Correlation
3. Rules Engine
4. Investigation
5. Q & A

NICK ROBINETT

PRODUCT OWNER

Contact me at:
nick.robinett@armor.com

PAUL SROUFE

DIRECTOR OF ENGINEERING

Contact me at:
paul.sroufe@armor.com

SECURITY AT SCALE MEANS:

PROVIDING REAL-TIME **ANALYSIS** &
CORRELATION FROM YOUR LOG DATA.

EVENT ABSTRACTION

EVENT ABSTRACTION

EVENT ABSTRACTION

Why develop rules for one device when you can abstract the data and build a ruleset that can be used for all relevant device types?

FIREWALL DEVICES

EVENT ABSTRACTION

Example: Cisco ASA Firewall Deny

Message:

%ASA-2-106001: 2 Inbound TCP connection denied

Abstracted Event:

ACL DENY

EVENT ABSTRACTION

Example: Juniper JunOS

Message:

FW: xe-0/0/2.0 D tcp

Abstracted Event:

ACL DENY

EVENT ABSTRACTION

DEVICE SPECIFIC EVENTS -> SIEM ABSTRACTED “PARSED” EVENTS

LEEF:2.0|Check Point|VPN-1 & FireWall-1|1.0|Drop|cat=VPN-1 & FireWall-1
devTime=1567029239 srcPort=137 layer_name=Rulebase Network layer_uuid=f822a85b-69ff-4236-a38d-cb6bcfc0098a match_id=155 parent_rule=0 rule_action=Drop rule_name=Cleanup rule rule_uid= 235b8732-2309-4cae-956d-13ef8ce7ea5b action=Drop ifdir=inbound ifname=eth5 logid=0 loguid={0x5d66f7f8,0x1b,0xf33c400a,0x3bdaf7af} origin= 10.100.0.26 originsicname=CN\=checkpoint,O\=checkpoint..i7ngdz sequencenum=1 version=5 dst=10.0.0.25 inzone=Internal outzone=Local proto=17 service=137 service_id=nbname src=10.100.0.26 \n

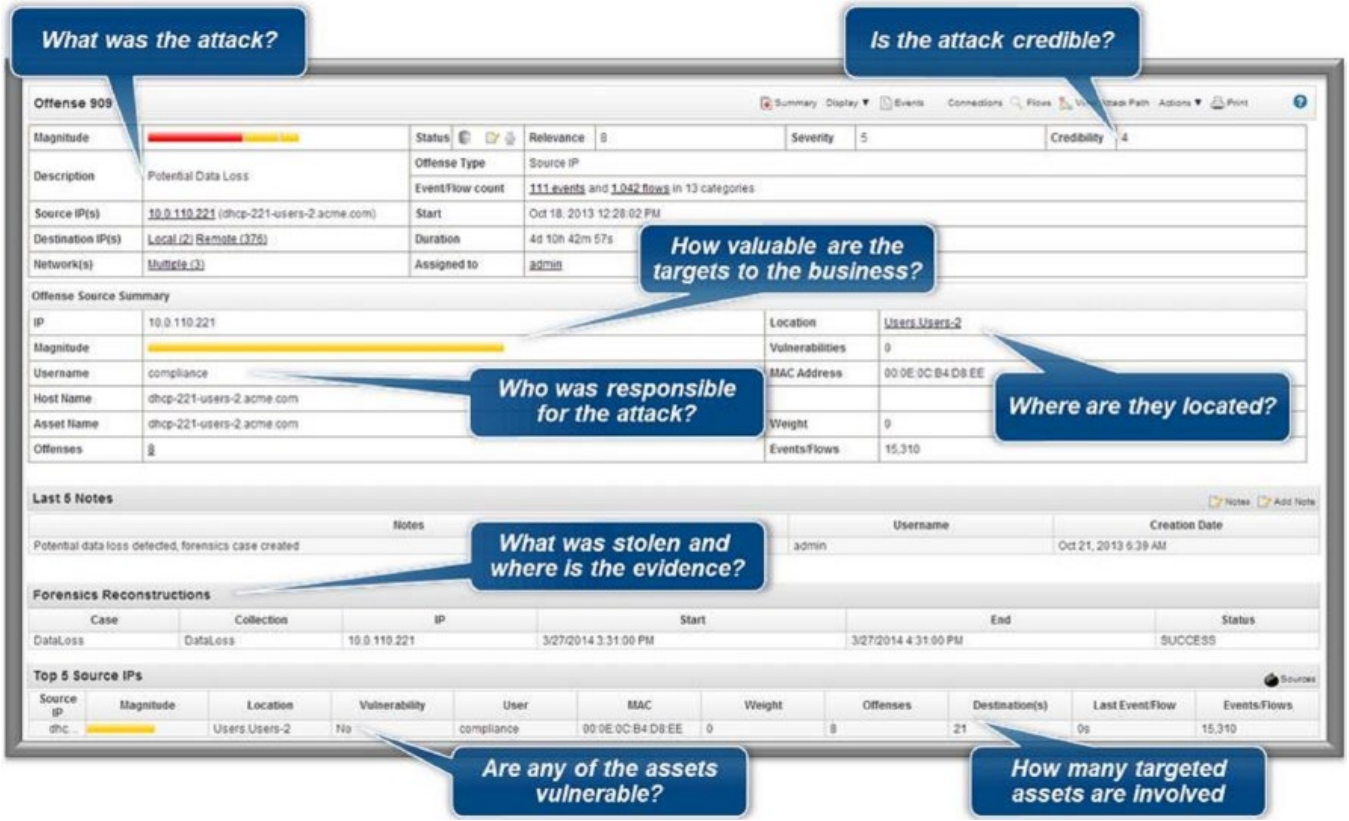
- Event Classification
- Source IP
- Source Port
- Destination IP
- Destination Port
- Context

EVENT ABSTRACTION

DEVICE SPECIFIC EVENTS -> SIEM ABSTRACTED "PARSED" EVENTS

LEEF:2.0|Check Point|VPN-1 & FireWall-
1|1.0 Drop|cat=VPN-1 & FireWall-1
devTime=1567029239 srcPort=137
layer_name=Rulebase Network layer_uuid=
f822a85b-69ff-4236-a38d-cb6bcfc0098a match_id=155
parent_rule=0 rule_action=Drop
rule_name=Cleanup rule rule_uid= 235b8732-
2309-4cae-956d-13ef8ce7ea5b action=Drop
ifdir=inbound ifname=eth5 logid=0
loguid={0x5d66f7f8,0x1b,0xf33c400a,0x3bdaf7af}
origin= 10.100.0.26
originsicname=CN\=checkpoint,O\=checkpoint..i7ng
dz sequencenum=1 version=5 dst=10.0.0.25
inzone=Internal outzone=Local proto=17
service=137 service_id=nbname
src=10.100.0.26 \n

- Event Classification: ACL DENY
- Source IP: 10.100.0.26
- Source Port: 137
- Destination IP: 10.0.0.25
- Destination Port: 137
- Context: Local to Local


What was the attack?
Is the attack credible?
How valuable are the targets to the business?
Who was responsible for the attack?
Where are they located?
What was stolen and where is the evidence?
Are any of the assets vulnerable?
How many targeted assets are involved
Offense 909
Magnitude
Status
Relevance 8
Severity 5
Credibility 4
Description Potential Data Loss
Offense Type Source IP
Event/Flow count 111 events and 1,042 flows in 13 categories
Source IP(s) 10.0.110.221 (dhcp-221-users-2.acme.com)
Start Oct 18, 2013 12:28:02 PM
Destination IP(s) Local (2) Remote (376)
Duration 4d 10h 42m 57s
Network(s) Multiple (3)
Assigned to admin
Offense Source Summary
IP 10.0.110.221
Location Users.Users-2
Magnitude
Vulnerabilities 0
Username compliance
MAC Address 00:0E:0C:B4:D8:EE
Host Name dhcp-221-users-2.acme.com
Asset Name dhcp-221-users-2.acme.com
Weight 9
Offenses 8
Events/Flows 15,310
Last 5 Notes
Notes
Add Note
Notes
Username
Creation Date
Potential data loss detected, forensics case created
admin
Oct 21, 2013 9:39 AM
Forensics Reconstructions
Case
Collection
IP
Start
End
Status
DataLoss
DataLoss
10.0.110.221
3/27/2014 3:31:00 PM
3/27/2014 4:31:00 PM
SUCCESS
Top 5 Source IPs
Sources
Source IP
Magnitude
Location
Vulnerability
User
MAC
Weight
Offenses
Destination(s)
Last Event/Flow
Events/Flows
dhc...
Users.Users-2
No
compliance
00:0E:0C:B4:D8:EE
0
8
21
0s
15,310

EVENT CORRELATION

Event Correlation: The process of taking in a **massive amount of events** and pin-pointing the importance by **analyzing the relationship between each event**.

EVENT CORRELATION - ADVANCED

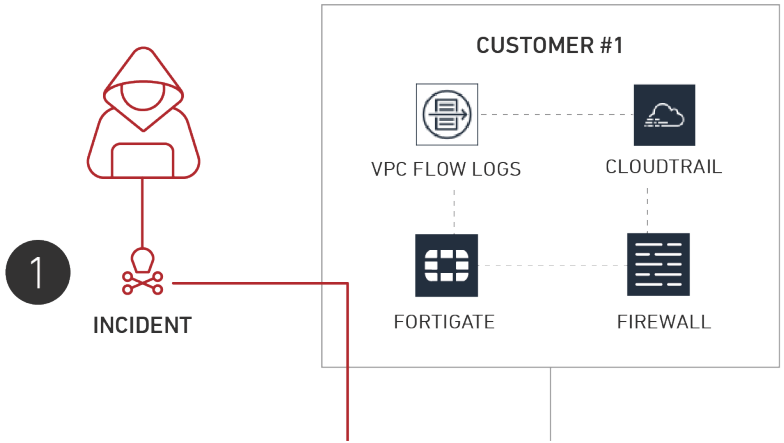
Customer Environment

EVENT CORRELATION - ADVANCED

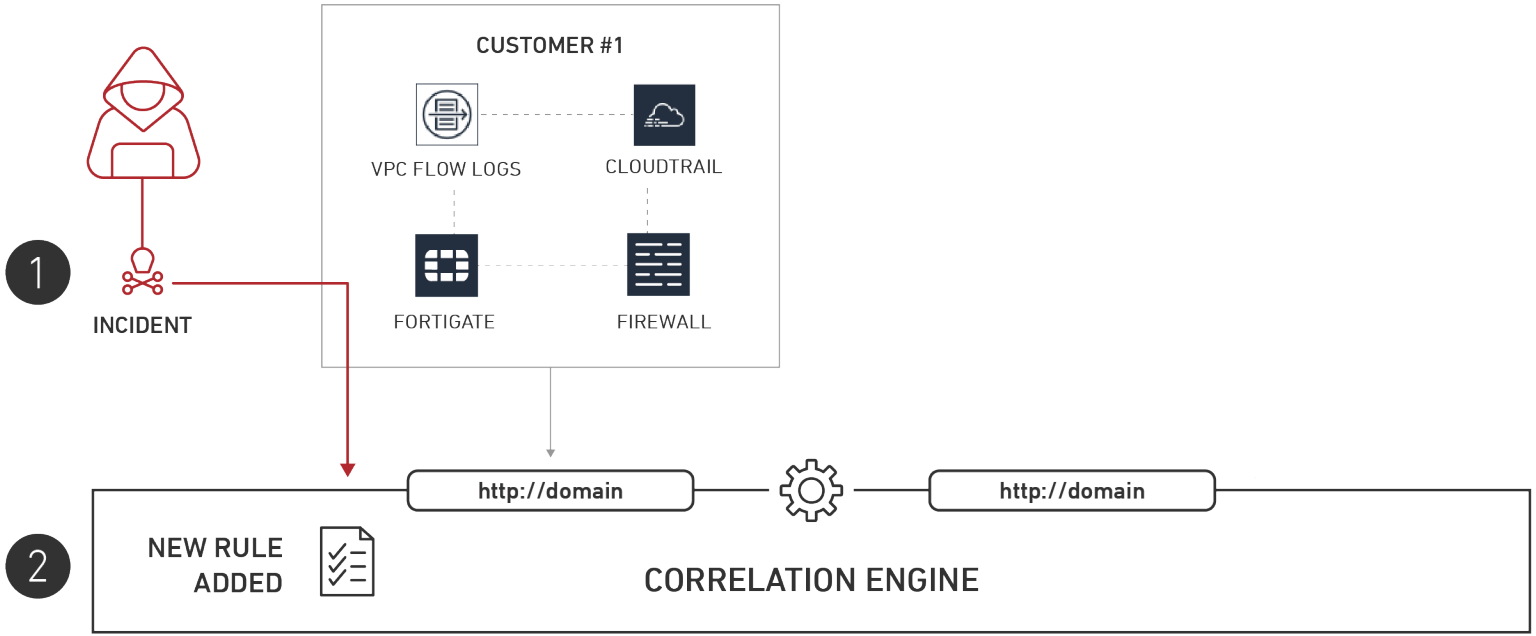
Customer Environment

EVENT CORRELATION - ADVANCED

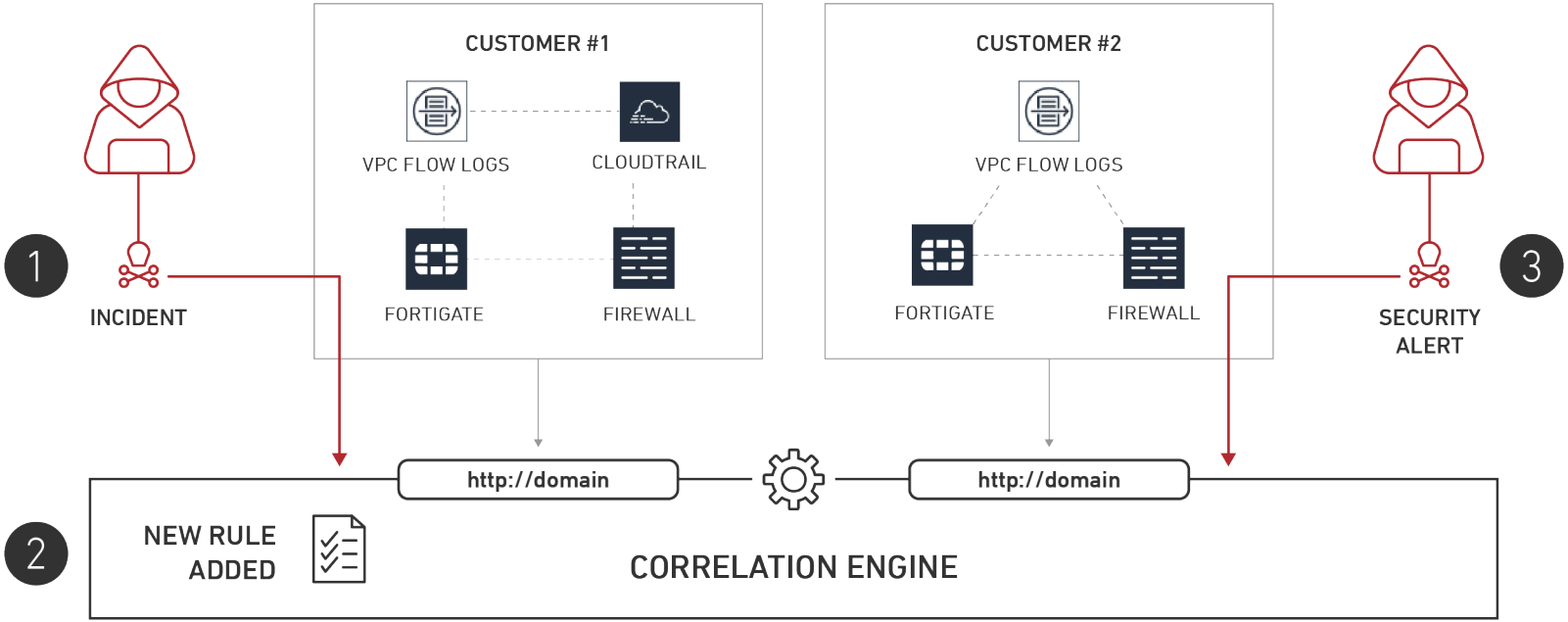
EVENT CORRELATION



EVENT CORRELATION

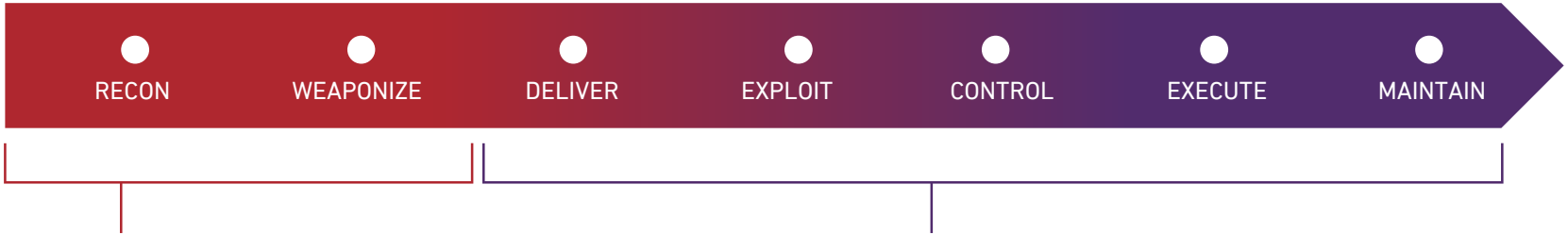


EVENT CORRELATION – ADVANCED



RULES ENGINE

RULES ENGINE



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

RULES ENGINE - FIREWALL

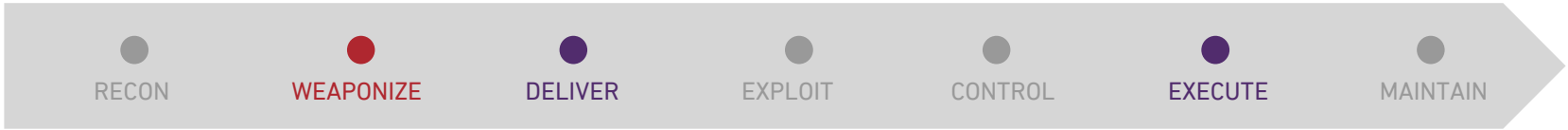
PRE-ATT&CK™

- 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

RULES ENGINE — WAF



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

INVESTIGATION

INVESTIGATION

AUTOMATED RESPONSES TO SECURITY ALERTS WITH REMEDIATION ACTIONS.

[HIGH] Possible Successful Brute Force Attack <Tenant ID> <Customer Name> - mm/dd/yyyy

Queue: Security-Security Operations
Priority: 2
Product Categorization 1: Security
Product Categorization 2: Access Control
Operational Categorization 1: Incident Response
Operational Categorization 2: None

Hello <Customer name>,

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:
||Domain||Log Source||Source IP||Login Time||
|domain <for WEB events only>|<machinename or log source>|SrcIP|Timestamp of Login Event|

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

ARMOR SOC

OUR SECURITY OPERATIONS CENTER IS THERE TO PROVIDE FURTHER INVESTIGATION FOR YOUR SECURITY INCIDENTS.

CONCLUSION

1. Large amounts of data flow through the SIEM and are parsed for security value.
2. SIEM rules and correlation identify threats from your monitored log data.
3. Notification of potential threats and incidents are reported with steps to remediate.

Q & A

NICK ROBINETT

Product Owner

PAUL SROUFE

Director of Engineering

ARMOR | SECURECON 2019 | DALLAS, TEXAS

THANK YOU.

WWW.ARMOR.COM