The State of S.O.A.R. 2019

L.Nemekhbayar

MNSEC 2019

About me

- L.Nemekhbayar
- 2005-2018 : software developer
- Now : security administrator @ Golomt Bank

CHALLENGES FACING INFOSEC

Too many alerts

~ 10000-12000 for an average team

More services

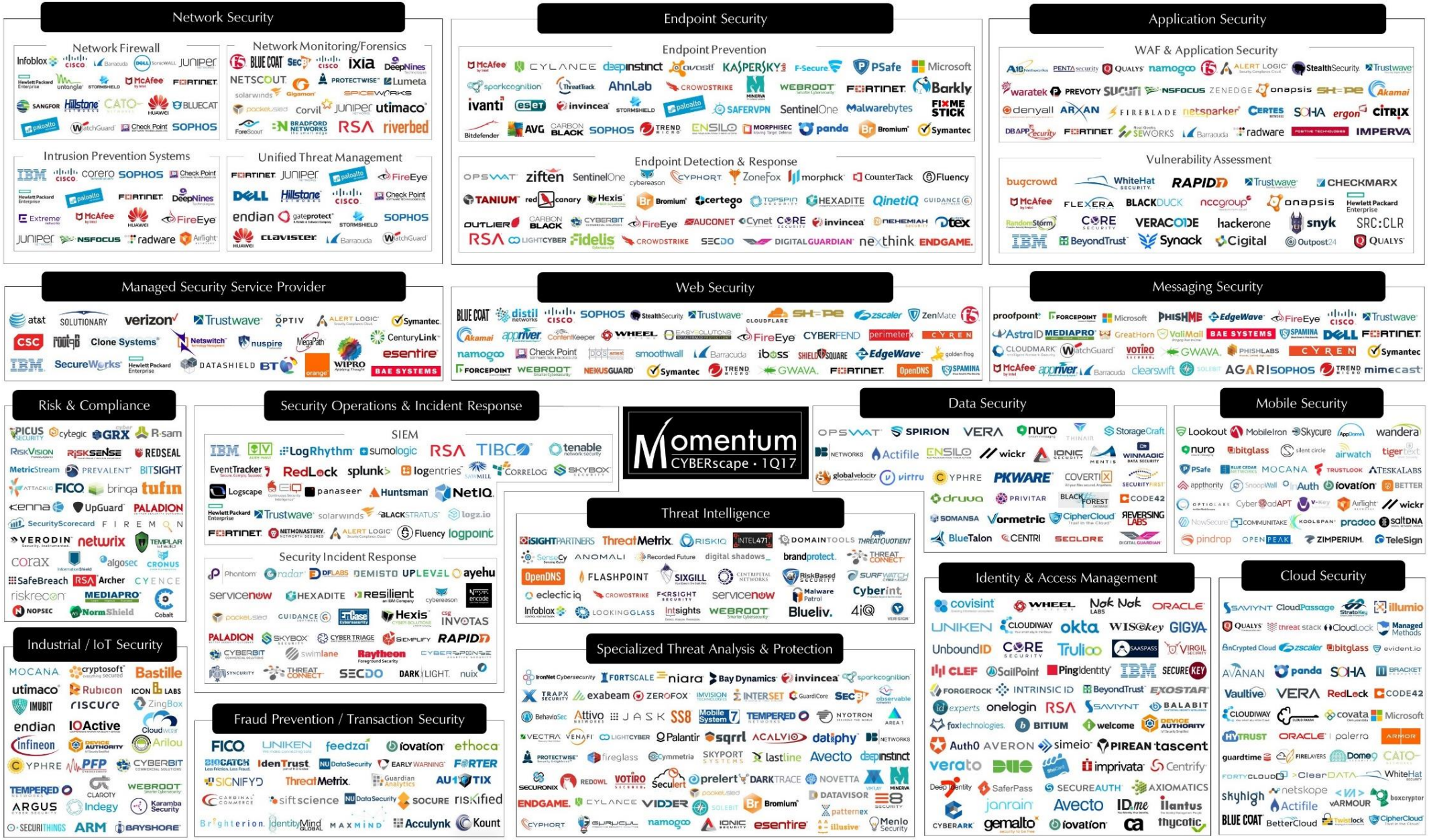
More data

More devices

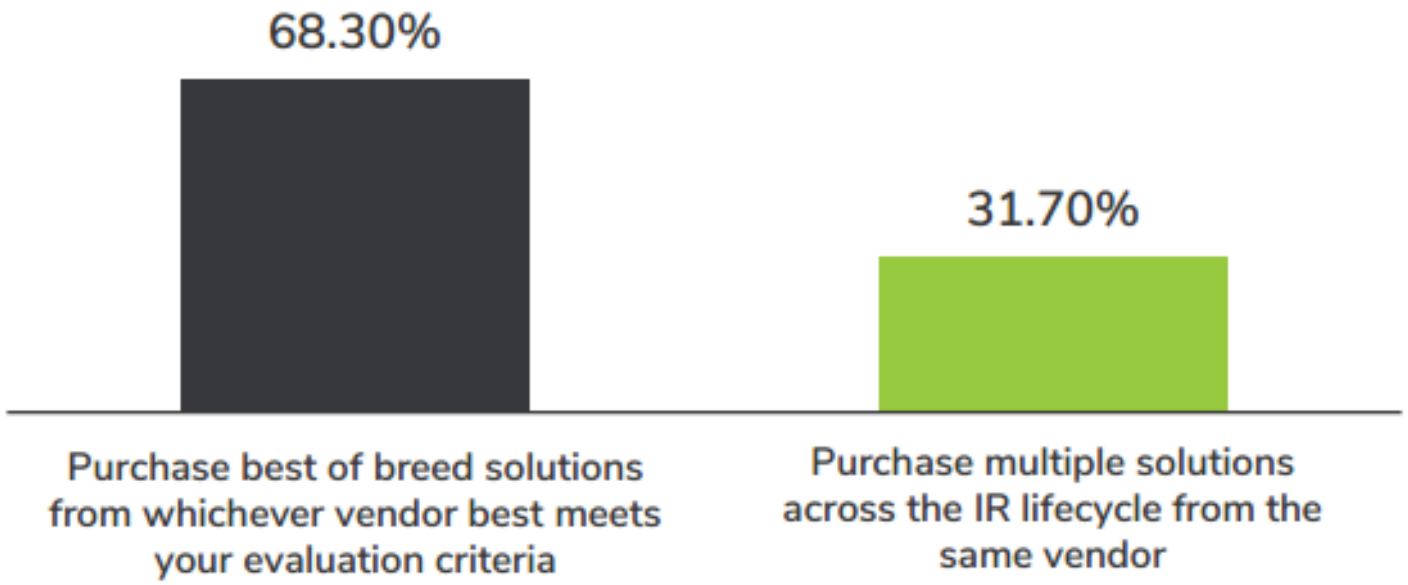
False positives

Duplicates

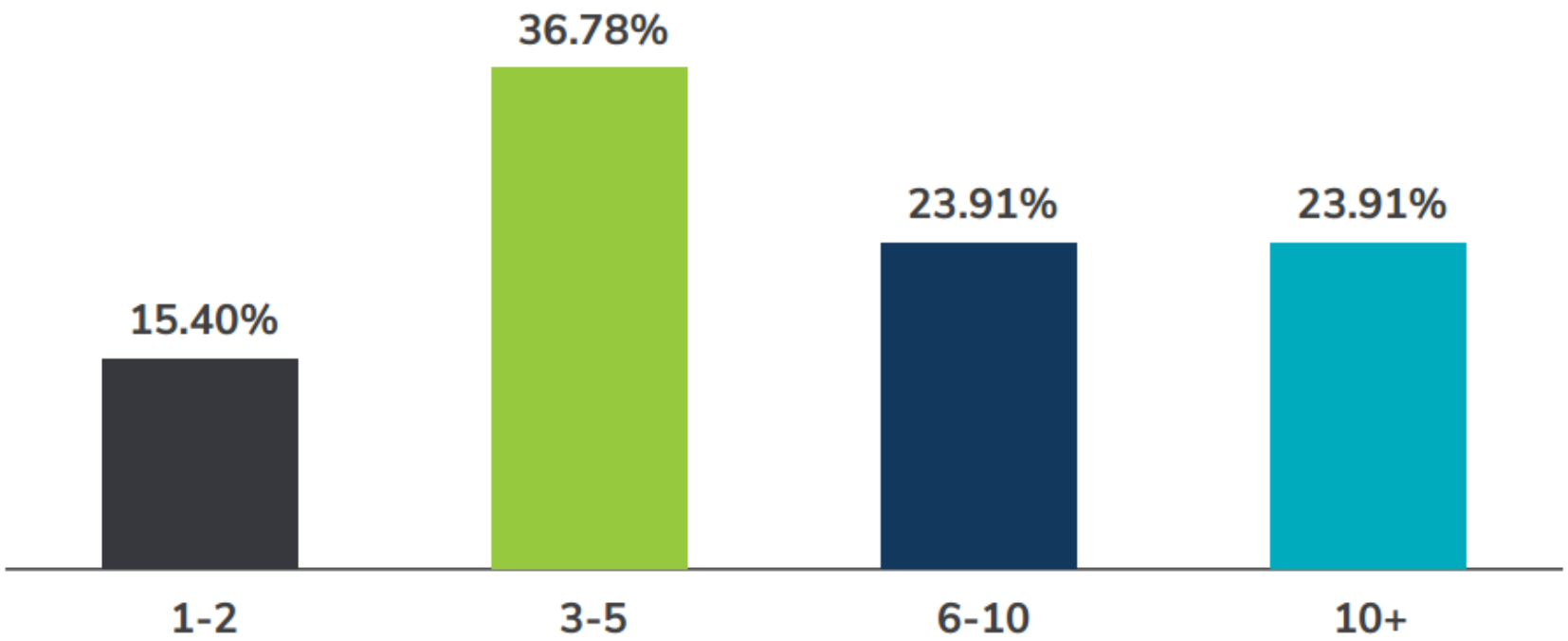
Too many security products !


Network Security
Network Firewall
Network Monitoring/Forensics
Intrusion Prevention Systems
Unified Threat Management
Endpoint Security
Endpoint Prevention
Endpoint Detection & Response
Application Security
WAF & Application Security
Vulnerability Assessment
Managed Security Service Provider
Web Security
Messaging Security
Risk & Compliance
Security Operations & Incident Response
SIEM
Security Incident Response
Momentum
CYBERscape · 1Q17
Data Security
Mobile Security
Threat Intelligence
Specialized Threat Analysis & Protection
Identity & Access Management
Cloud Security
Industrial / IoT Security
Fraud Prevention / Transaction Security

EVALUATING SOLUTIONS FOR IR ACTIVITIES / PROCESSES



NUMBER OF SECURITY PRODUCTS MANAGED



Staff and skills shortage

U.S. Bureau of Labor Statistics : employment of security analysts to grow by 28 percent from 2016 to 2026

Long training cycles : ~ 8 months

Low retention : ~ 2 years

Strenuous and highly paid jobs

Must act quickly !

Discover early

Respond quickly

Contain quickly

Remediate quickly

No unified process

Dispersed or lacking documentation

Lack of communication

Hybrid environments

Siloed workforce / tools

Boring / tedious tasks

False positives

Duplicates

Reports, post-mortems

Repeating tasks

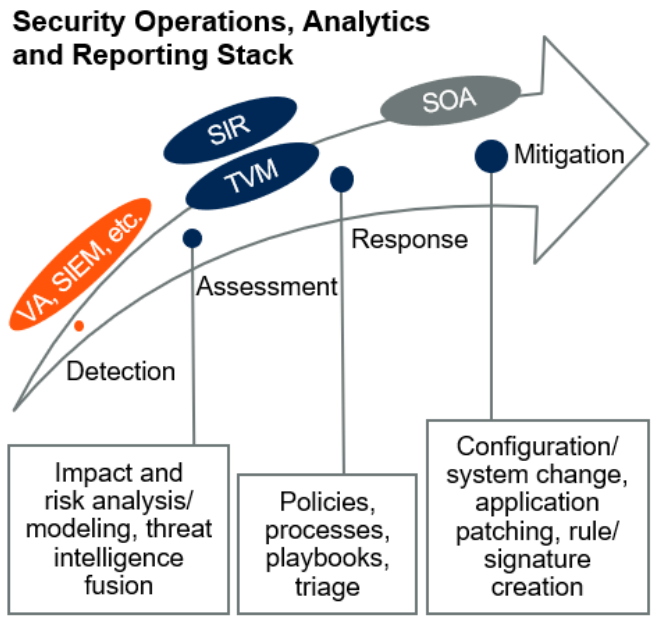
Context switching

S O A R ?

Security **O**rchestration **A**utomation **R**esponse

Term coined by Gartner in late 2017

Convergence of SOAR Types



SOAR Use Cases

- SOC Optimization
- Threat Monitoring and Response
- Threat Investigation and Hunting
- Threat Intelligence Management

SOAR = SIR + SOA + TVM — **SOAR = SOA + SIR + TIP**

2015 — **2017** — **2019**

Source: Gartner
TVM = threat vulnerability management; VA = vulnerability assessment
ID: 389446

POSSIBILITIES OF SOAR

Orchestration

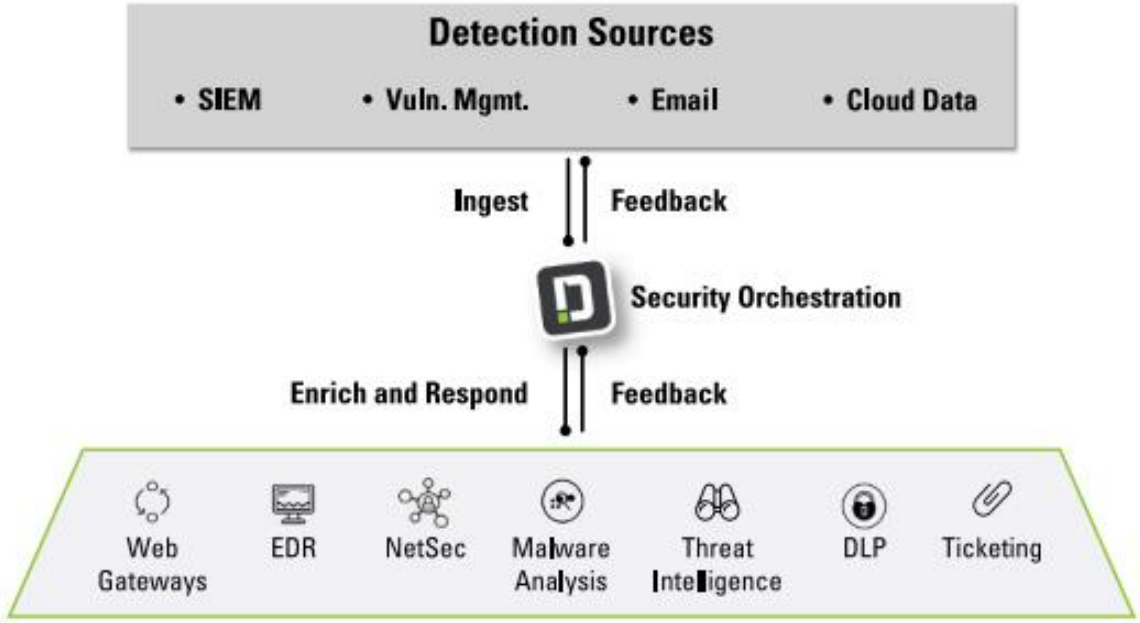
Make people communicate

Make tools communicate

Correlation between events

Centralize incident management

Centralize data & knowledge



Automation

Reduce false-positives & duplicates

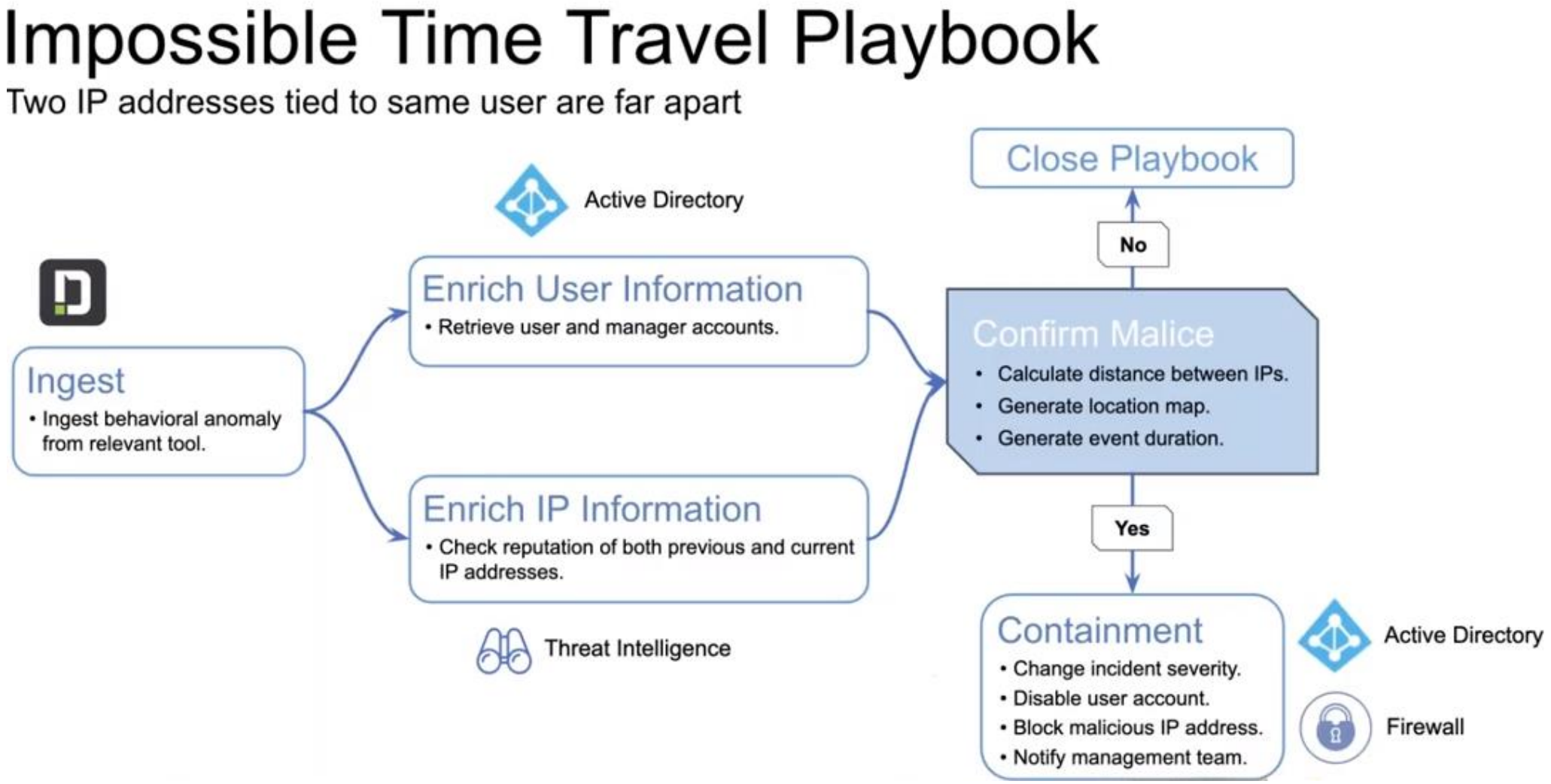
Machine Learning

Faster response times

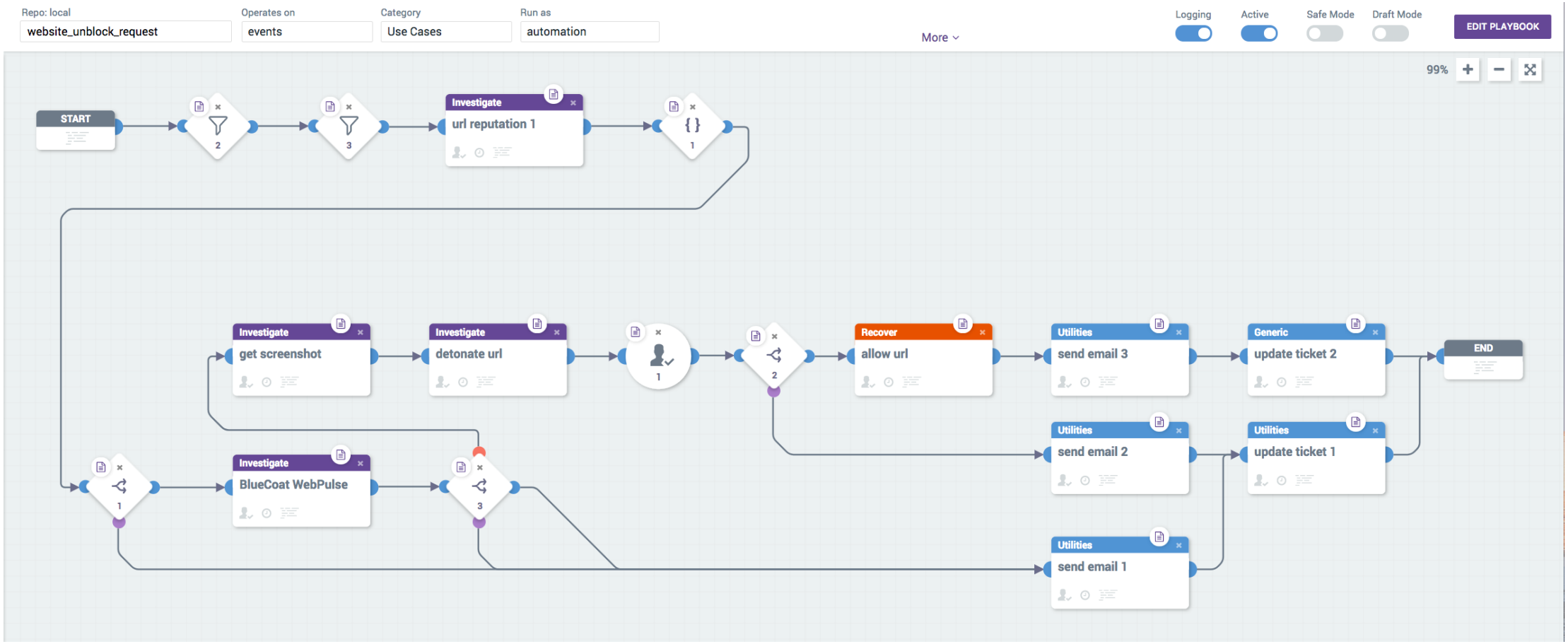
Reduce human errors

Generate reports

Response


Impossible Time Travel Playbook
Two IP addresses tied to same user are far apart
Close Playbook
Active Directory
No
Enrich User Information
• Retrieve user and manager accounts.
Ingest
• Ingest behavioral anomaly from relevant tool.
Confirm Malice
• Calculate distance between IPs.
• Generate location map.
• Generate event duration.
Enrich IP Information
• Check reputation of both previous and current IP addresses.
Yes
Threat Intelligence
Containment
• Change incident severity.
• Disable user account.
• Block malicious IP address.
• Notify management team.
Active Directory
Firewall

Playbook example



Use cases

Reactive

Phishing / malware ->block URL / IP

Leaked password -> disable user account, notify user

Malicious traffic -> launch packet capture

Collect host data

Proactive

Check for vulnerabilities

Check certificate expiration

Threat hunting

Security audit

Compliance check

What SOAR is NOT ?

~~A replacement for analysts~~

~~A SIEM~~

(although SIEMs do have some SOAR capabilities)

~~A solution to all your problems~~

THE FUTURE

Gartner :

- Increase in awareness
- SOAR usage 5% -> 30% by end of 2022
- Market to grow to up to $550 million in the next five years

Acquisitions

February 2016	FireEye (Helix) acquired Invotas
April 2016	IBM acquired Resilient Systems
June 2016	ServiceNow acquired Brightpoint Security
June 2017	Microsoft acquired Hexadite
July 2017	Rapid7 acquired Komand
February 2018	Splunk acquired Phantom Cyber
February 2019	Palo Alto Networks acquired Demisto

RESERVES

Mature security ecosystem ?

Appliance integration possibilities ?

Learning curve ?

Machine Learning not yet decisive

Still a moving market, consolidations

SOURCES

- Market Guide for SOAR Solutions
  - Gartner
  - June 2019
- The State of SOAR 2019
  - Virtual Intelligence Briefing on behalf of Demisto (Palo Alto Networks)
  - August 2019

THANK YOU !