

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
 Infoblox, Cisco, Palo Alto, Juniper, SolarWinds, Fortinet, McAfee, Palo Alto, Sangfor, Hillstone, Cato, Huawei, Bluecat, Palo Alto, WatchGuard, Check Point, Sophos

Network Monitoring/Forensics
 Blue Coat, Ixia, DeepNines, Netscout, Protectwise, Lumeta, Solarwinds, Gigamon, Spiceworks, PacketSight, Corvill, Juniper, Utimaco, Forescout, Bradford Networks, RSA, Riverbed

Intrusion Prevention Systems
 IBM, Cisco, Coreo, Sophos, Check Point, Palo Alto, Fortinet, DeepNines, Extreme, McAfee, Huawei, FireEye, Juniper, NSFOCUS, Radware, Avlight

Unified Threat Management
 Fortinet, Juniper, Palo Alto, FireEye, Dell, Hillstone, Cisco, Check Point, Endian, Gateprotect, Stormshield, Sophos, Huawei, Clavister, Barracuda, WatchGuard

Endpoint Security

Endpoint Prevention
 McAfee, Cylance, Deep Instinct, Avast, Kaspersky, F-Secure, P-Safe, Microsoft, SparkCognition, ThreatStack, AhnLab, CrowStrike, Minserva, Webroot, Fortinet, Barkly, Ivanti, ESET, Invincea, Stormshield, Palo Alto, Safervpn, SentinelOne, Malwarebytes, FixMe Stick, BitDefender, AVG, Carbon Black, Sophos, Trend Micro, Emsisoft, Morphisec, Panda, Bromium, Symantec

Endpoint Detection & Response
 Opswat, Ziften, SentinelOne, Cyberason, Cyphort, ZoneFox, Morphick, CounterTack, Fluency, Tanium, Canary, Hexis, Bromium, Certego, Ippon, Hexadite, Qinetiq, Guidance, Outlier, Carbon Black, Cyberbit, FireEye, Auconet, Cynet, Core, Invincea, Nehemiah, Dtex, RSA, LightCyber, Fidelis, CrowStrike, Secdo, DigitalGuardian, Nextthink, Endgame

Application Security

WAF & Application Security
 Akamai, Imperva, Cloudflare, Sucuri, Cloudbricks, Palo Alto, Fortinet, Radware, Akamai, Wafwaggle, Penta Security, Qualys, Namogoo, Alert Logic, StealthSecurity, Trustwave, Wafatek, Prevoty, Sucuri, NSFOCUS, Zenedge, Onapsis, SH-PE, Akamai, Denyall, Arxan, Fireblade, Netsparker, Certes, SOHA, Ergon, Citrix, DBAppSecurity, Fortinet, Secworks, Barracuda, Radware, Imperva, Imperva

Vulnerability Assessment
 Bugcrowd, WhiteHat Security, Rapid7, Trustwave, Checkmarx, McAfee, Flexera, BlackDuck, Nccgroup, Onapsis, Hewlett Packard Enterprise, Rapid7, Core Security, Veracode, Hackerone, Snyk, SRC:CLR, IBM, BeyondTrust, Synack, Cigital, Outpost24, Qualys

Managed Security Service Provider

at&t, Solutionary, Verizon, Trustwave, Optiv, Alert Logic, Symantec, CSC, Clone Systems, Netswitch, Nuspire, MegaPath, CenturyLink, IBM, SecureWorks, Hewlett Packard Enterprise, Datashield, BT, Wipro, BAE Systems

Web Security

Blue Coat, Distil Networks, Cisco, Sophos, StealthSecurity, Trustwave, SH-PE, Zscaler, ZenMate, Akamai, Arxan, ContentKeeper, Wheel, Easy Solutions, Cloudflare, FireEye, Cyberfend, Perimeter8, Cyren, Namogoo, Check Point, Smoothwall, Barracuda, Iboss, ShieldSquare, EdgeWave, Golden Frog, Forcepoint, Webroot, NexuSGuard, Symantec, Trend Micro, Gwava, Fortinet, OpenDNS, Spamhaus

Messaging Security

Proofpoint, Forcepoint, Microsoft, PhishME, EdgeWave, FireEye, Cisco, Trustwave, AstralID, Mediapro, GreatHorn, VailMail, BAE Systems, Spamina, Dell, Fortinet, Cloudmark, WatchGuard, Votiro, Gwava, PhishLabs, Cyren, Symantec, McAfee, Arxan, Barracuda, Clearswift, Agari, Sophos, Trend Micro, Mimecast

Risk & Compliance

Picus Security, Cyteq, GRX, R-Sam, RiskVision, RiskSense, RedSeal, MetriStream, Prevalent, Bitsight, AttackIQ, FICO, Brinqa, Tufin, Kenna, UpGuard, Paladion, SecurityScorecard, Firemon, Verodin, Netwrix, Temporal, Corax, Algosec, Cronus, SafeBreach, RSA, Archer, Cyence, Riskrecon, Mediapro, Nopsec, NormShield, Cobalt

Security Operations & Incident Response

SIEM
 IBM, LogRhythm, Sumologic, RSA, TIBCO, Tenable Security, EventTracker, RedLock, Splunk, Logentries, Correlog, Skybox, Logscale, Panaseer, Huntsman, NetIQ, Hewlett Packard Enterprise, Trustwave, Solarwinds, Blackstratus, Logz.io, Fortinet, Netmonastery, Alert Logic, Fluency, Logpoint

Security Incident Response
 Phantom, Radar, DR Labs, Demisto, Uplevel, Ayehu, ServiceNow, Hexadite, Resilient, Cyberason, Phantom, PacketSight, Guidance, InPass, Hexis, Invotas, Paladion, Skybox, CyberTrage, Simplify, Rapid7, Cyberbit, Swimlane, Raytheon, CyberResponse, Styncity, ThreatConnect, Secdo, DarkLight, Nuix

Momentum

CYBERscape • 1Q17

Data Security

Opswat, Spirion, Vera, Nuro, StorageCraft, Actifile, ENSILO, Wickr, Ignic Security, WinMagic, Global Velocity, Virtu, Yphre, PKware, Covertix, Somansa, Vormetric, CipherCloud, Reversing Labs, BlueTalon, Centri, Seclore, Digital Guardian

Mobile Security

Lookout, MobileIron, Skycore, Wandera, Nuro, Bitglass, Silent Circle, Airwatch, TigerTect, P-Safe, Mocana, Trustlook, Ateskalabs, Appthority, SnopWall, Auth, Iovation, Better, OptiLabs, CyberodAPT, V-Key, Arlight, Wickr, NewSecure, Communitake, Koollspan, Pradeo, SaltDNA, Pindrop, OpenPeak, Zimperium, TeleSign

Industrial / IoT Security

Mocana, Cryptosoft, Bastille, Utimaco, Rubicon, Icon Labs, Imubit, Riscure, ZingBox, Endian, IOActive, CloudKnox, Infineon, Divis Authority, Anilox, Yphre, PEP, Cyberbit, Tempered, Clarity, Webroot, Argus, Indegy, Karamba Security, Securithings, ARM, Bayshore

Fraud Prevention / Transaction Security

Fico, Uniken, Feedzai, Iovation, Ethoca, Biocatch, IdenTrust, NuDataSecurity, EarlyWarnings, Forter, Sicnifyd, ThreatMetrix, Guardian Analytics, AU10TIX, Cardinal Commerce, Siftscience, NuDataSecurity, Secure Riskified, Brighterion, IdentibMind, MaxMind, Acculynk, Kount

Threat Intelligence

iSightPartners, ThreatMetrix, RiskIQ, Intel471, DomainTools, ThreatQuotient, SenseCy, Anomali, Recorded Future, Digital Shadows, BrandProtect, ThreatConnect, OpenDNS, Flashpoint, Sixgill, Central Intelligence Agency, RiskBased Security, SurfWatch, ElecticIQ, CrowStrike, Farsight Research, ServiceNow, Malware Patrol, Infoblox, LookingGlass, Webroot, Blueliv, 4iQ, Verisign

Specialized Threat Analysis & Protection

Intel Cybersecurity, Fortscale, Nianta, Bay Dynamics, Invincea, SparkCognition, TrapX Security, Exabeam, ZeroFox, Imvision, Intersect, GuardCore, Sec3, BehaviorSec, Attivo, JASK, SS8, Mobile System7, Tempered, NYOTRON, Vectra, Venafi, LightCyber, Palantir, Sqrl, ACALVIO, Dataphy, Protectwise, Fireglass, Cymmetria, Skyport, Lastline, Avecto, DeepInstinct, Redowl, Votiro, Seculert, Preler, DarkTrace, Novetta, Endgame, Cylance, Vidder, Bromium, DataVisor, Securix, Patternex, Menlo Security, Cyphort, Surscout, Namogoo, Ignic Security, Esentire, Illusive

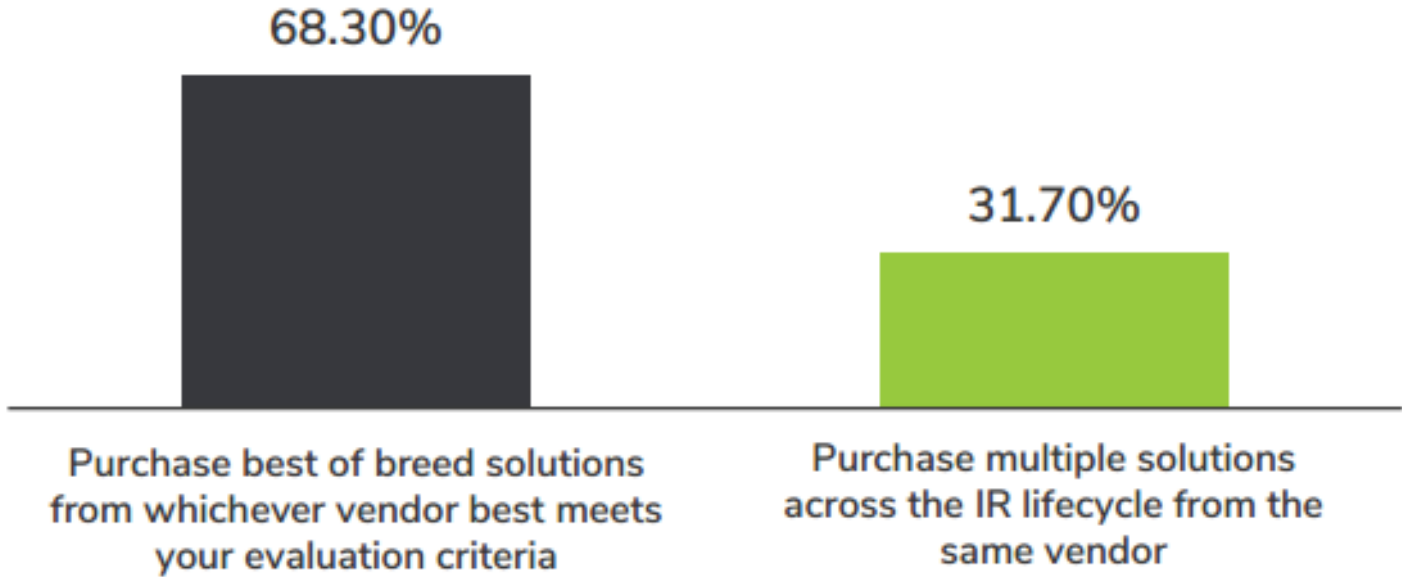
Identity & Access Management

Covisint, Wheel, Oracle, Uniken, CloudWay, Okta, WIS@key, GIGYA, UnboundID, Core, Truicoo, SaaSPASS, Virgil Security, Clef, SailPoint, Pingidentity, IBM, SecureKey, Forgerock, Intrinsic ID, BeyondTrust, Exostar, Id experts, Onelogin, RSA, Saviynt, Balabit, Fax Technologies, Bitium, Welcome, Device Authority, Auth0, AVeron, Simeio, Pirean, Tascent, Verato, Imperva, Centrify, Deep Identity, SaferPass, SecureAuth, Axionatics, Cyberark, Genalto, Iovation, Ca, Thycotic

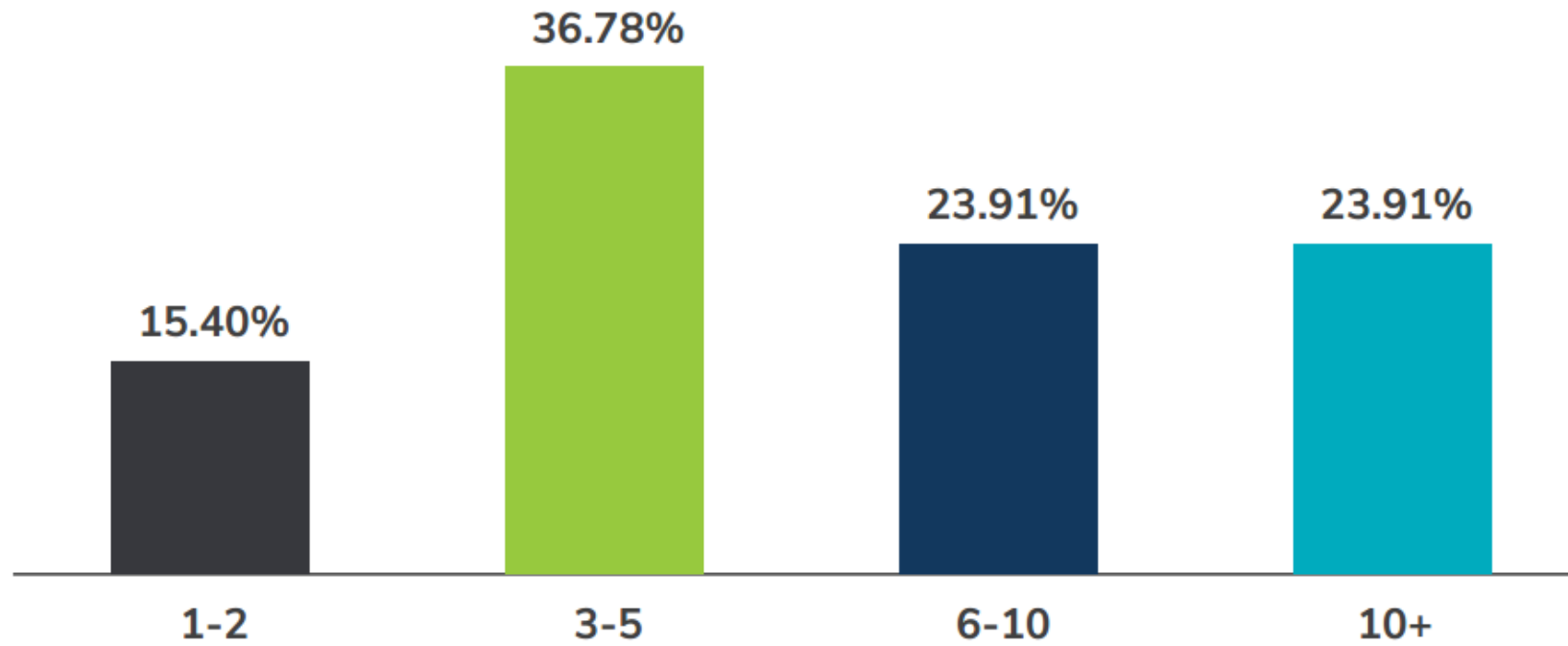
Cloud Security

Saviynt, CloudPassage, Illumio, Qualys, Threat Stack, CloudLock, Managed Methods, Bncrypted Cloud, Zscaler, Bitglass, Evidentio, Avanan, Panda, SOHA, Bracket, Vaultive, Vera, RedLock, Code42, CloudWay, Covata, Microsoft, HyTrust, Oracle, Palerra, Armor, Guardtime, FireLayers, Dome, Cato, FortyCloud, ClearData, WhiteHat, Skyhigh, Netskope, ID.me, Iantus, Boxcryptor, Blue Coat, BetterCloud, Twisslock, CipherCloud

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



SOAR?

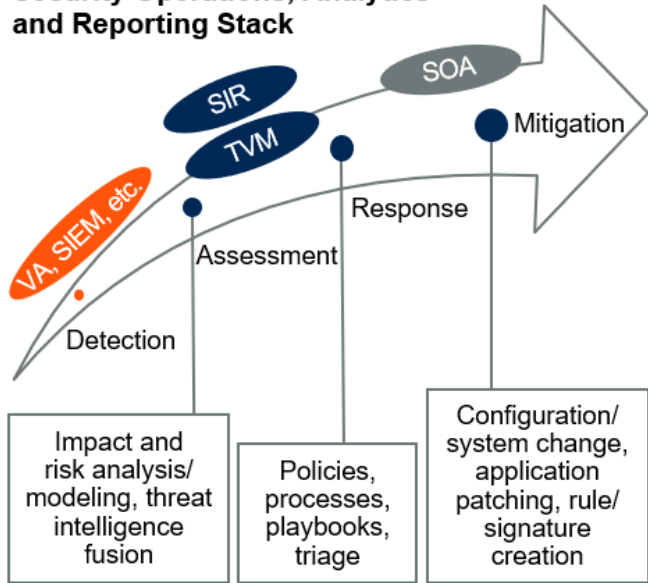
Security Orchestration Automation Response

Term coined by Gartner in late 2017

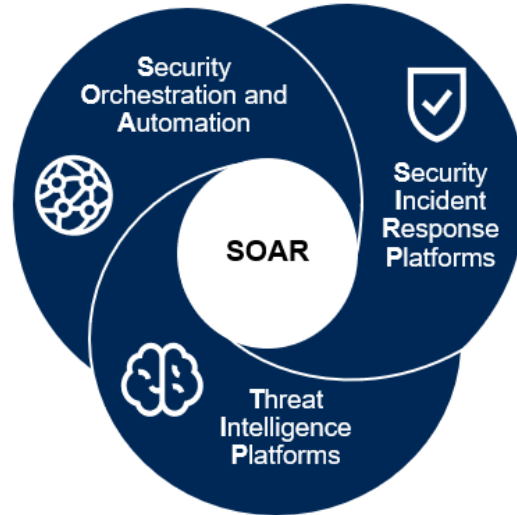
Gartner[®]

Convergence of SOAR Types

Security Operations, Analytics and Reporting Stack



SOAR = SIR + SOA + TVM



SOAR = SOA + SIR + TIP

SOAR Use Cases
• SOC Optimization
• Threat Monitoring and Response
• Threat Investigation and Hunting
• Threat Intelligence Management

2015

2017

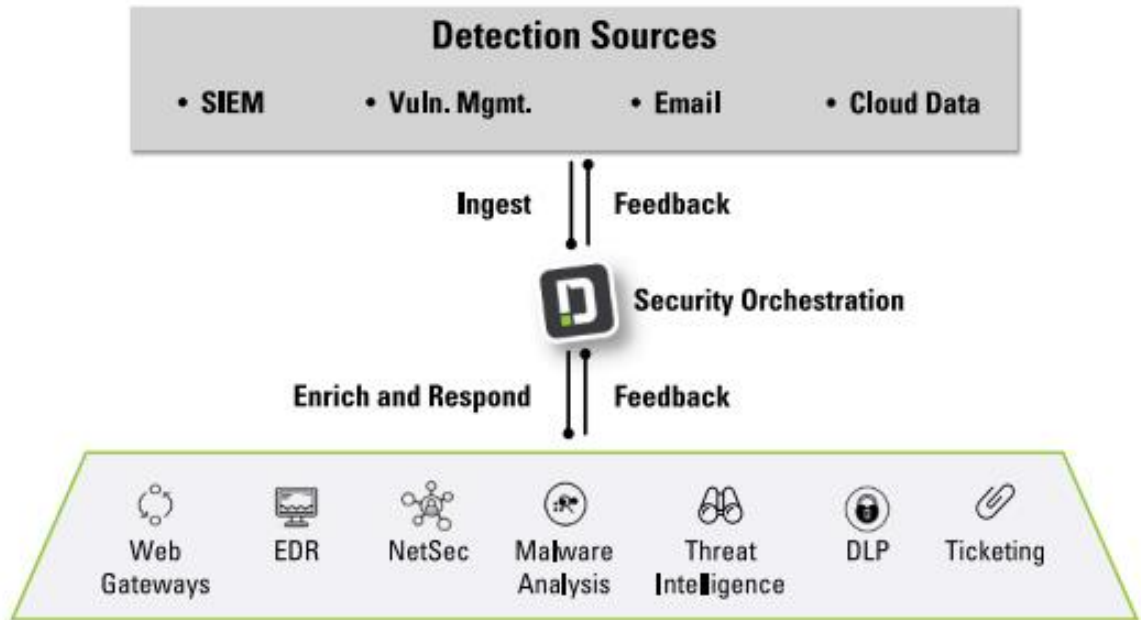
2019

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

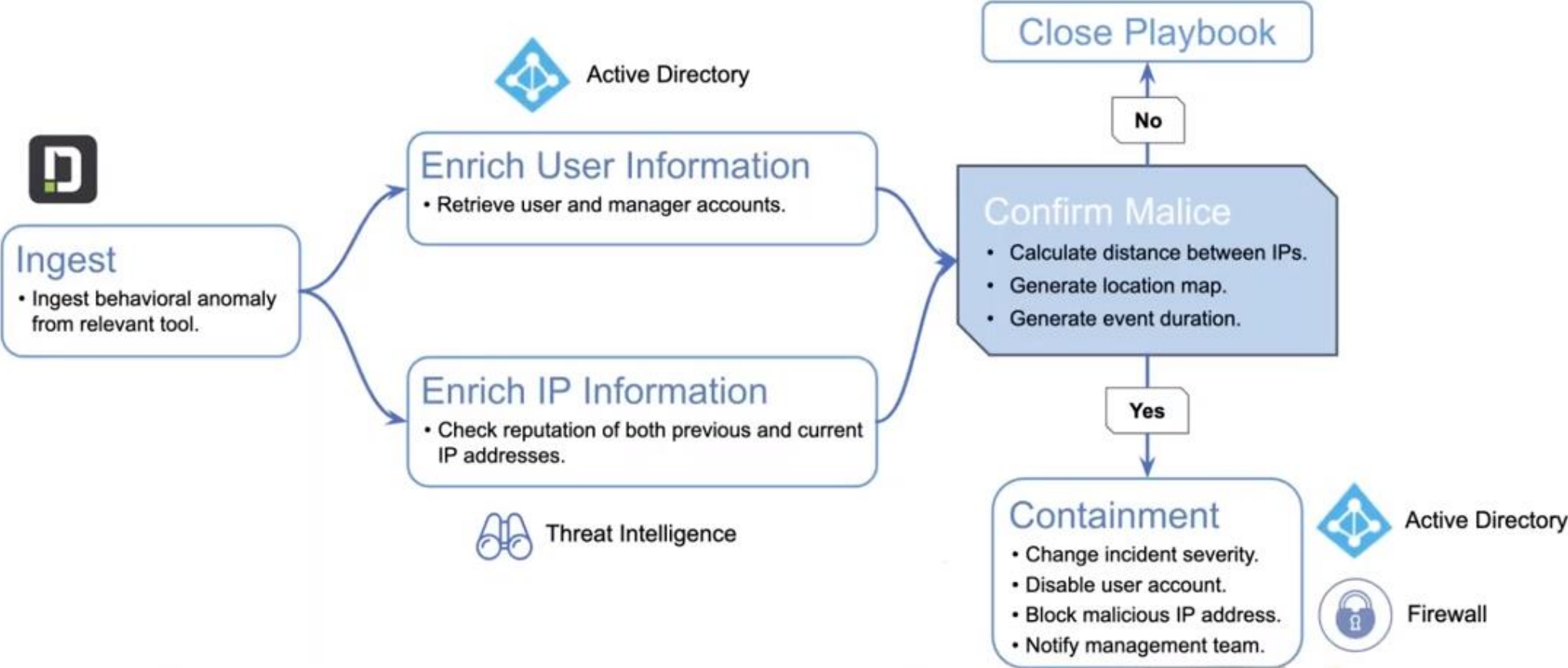
Reduce human errors

Generate reports

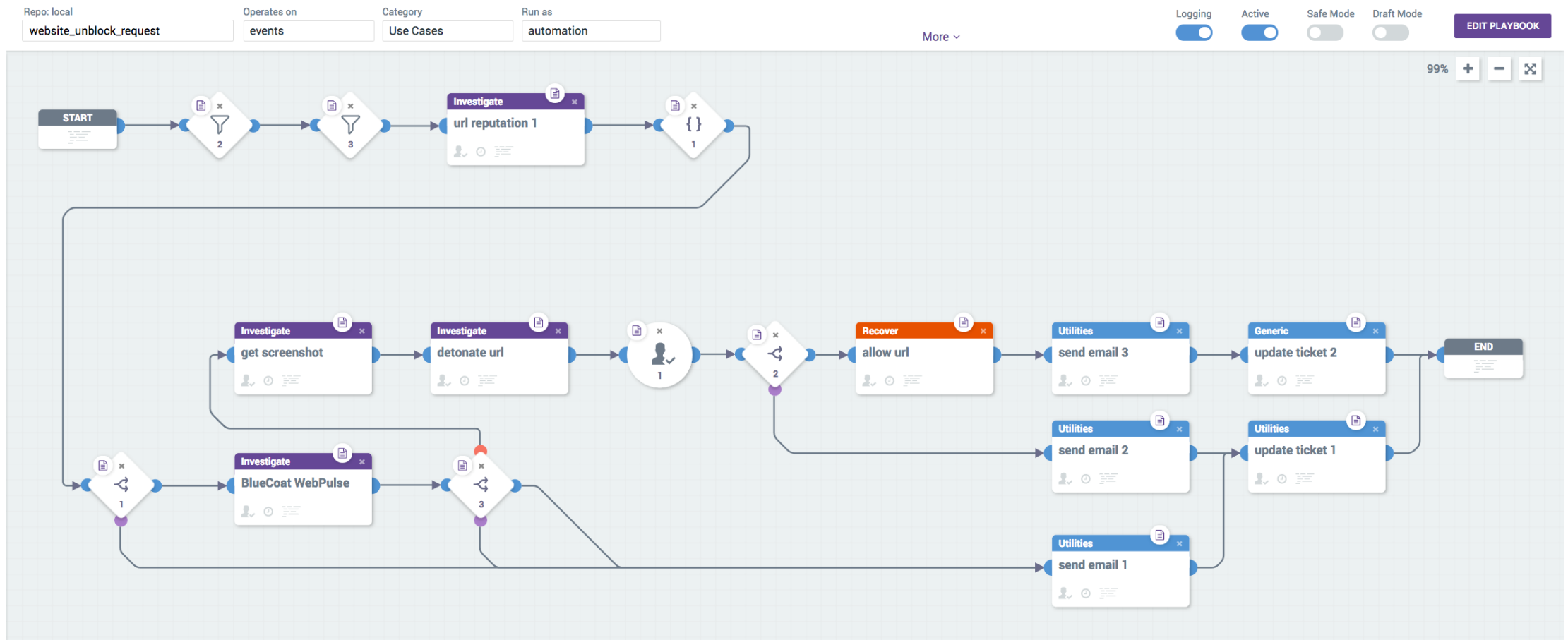
Response

Impossible Time Travel Playbook

Two IP addresses tied to same user are far apart



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 !

