Security Orchestration, Automation, and Response (SOAR)

Demisto

Tudor Cristea
Cortex Sales Eastern Europe
Palo Alto Networks
Emerging Challenges in Security Operations
As threats escalate, SecOps is more important than ever

We continue to see an escalation in the volume, sophistication, and impact of data breaches, which only seem to be getting worse.

<table>
<thead>
<tr>
<th>Year</th>
<th>Malicious programs registered</th>
<th>New Malicious programs registered</th>
</tr>
</thead>
<tbody>
<tr>
<td>1998</td>
<td>Morris Worm</td>
<td>47M</td>
</tr>
<tr>
<td></td>
<td>Space agency breach</td>
<td></td>
</tr>
<tr>
<td>2004</td>
<td>Identity theft</td>
<td>182M</td>
</tr>
<tr>
<td></td>
<td>95M records stolen</td>
<td></td>
</tr>
<tr>
<td>2007</td>
<td>DNS attacks</td>
<td>142M</td>
</tr>
<tr>
<td></td>
<td>Botnets</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sabotage</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Anti-spam</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SQL attacks</td>
<td></td>
</tr>
<tr>
<td>2010</td>
<td>Social engineering</td>
<td>145M</td>
</tr>
<tr>
<td></td>
<td>DDoS attacks</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Malicious email</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ransomware Botnets</td>
<td></td>
</tr>
<tr>
<td>2013</td>
<td>Banking malware</td>
<td>250M</td>
</tr>
<tr>
<td></td>
<td>Keyloggers</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ransomware</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Botnets</td>
<td></td>
</tr>
<tr>
<td>2016</td>
<td>Ransomware Cryptominer</td>
<td>925M</td>
</tr>
<tr>
<td></td>
<td>Certificate attacks</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Bitcoin wallet</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Android hacks</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Insider threats</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cloud migration</td>
<td></td>
</tr>
<tr>
<td>Present</td>
<td>Cyberwarfare Fileless attacks</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Automated &amp; AI attacks</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cloud migration</td>
<td></td>
</tr>
<tr>
<td></td>
<td>S3 buckets</td>
<td></td>
</tr>
</tbody>
</table>

1998: Morris Worm
2004: Identity theft
2007: DNS attacks
2010: Social engineering
2013: Banking malware
2016: Ransomware Cryptominer
Present: Cyberwarfare Fileless attacks

925M + New Malicious programs registered
Why security teams struggle

- **Gaps in Prevention**: Legacy tools generate too many alerts
- **Lack of Time**: Manual tasks across siloed tools take too long
- **Limited Context**: It takes days to investigate threats

- **174k alerts per week**
- **30+ point products**
- **4+ days to complete an investigation**
The reality (and complexity) of security operations
How SecOps must transform to reduce risk

<table>
<thead>
<tr>
<th>Maturity</th>
<th>Low (Reactive)</th>
<th>Medium</th>
<th>High (Proactive)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detection</td>
<td>RULE-BASED</td>
<td>CORRELATED RULE-BASED</td>
<td>ANALYTICS-BASED</td>
</tr>
<tr>
<td>Context</td>
<td>LOG AGGREGATION</td>
<td>SILOED DATA COLLECTION</td>
<td>INTEGRATED RICH DATA</td>
</tr>
<tr>
<td>Automation</td>
<td>NONE</td>
<td>PARTIAL</td>
<td>FULL</td>
</tr>
</tbody>
</table>

**Efficiency**

**MTTR/MTTD & Risk**
Palo Alto Networks
Unique Approach
Reinventing SecOps with Cortex

Prevent everything you can

Everything you can’t prevent, detect and investigate fast

Automate response and get smarter with each incident

Traps & Next-Generation Firewall

Cortex XDR & AutoFocus

Demisto
Reinventing SecOps with Cortex - the platform for SecOps
Solving all key challenges in a more efficient way with higher security outcomes
Use Case: Phishing Response
The Problem: Phishing response is hard

High Alert Volumes
Phishing attacks are frequent, easy to execute, and act as the entry vector for most security attacks

Disjointed Processes
Security teams must coordinate across email inboxes, threat intel, NGFW, ticketing, and other tools for phishing response

Ever-Present and Growing
95% of all attacks on enterprise networks are a result of spear phishing

Our Approach to Phishing response

Before (w/o SOAR)

Check indicator reputation

1. Threat Intelligence
2. Email

Collect context

1. SIEM
2. Security Analyst

Detonate file

1. Malware Analysis

Quarantine

1. EDR
2. Raise severity
3. Open Ticket

Manual triage

After (w/ Demisto)

Email

Ingest

Extract

1. IP, domain, attachment

Threat Intelligence

1. SIEM

Sandbox

1. Enrich
2. Respond
3. Mail

Ticketing

Severity

Inform Analyst

Automated playbooks
Key Differentiators: Automate and standardize phishing response

- **Product Integrations**
  Demisto integrates with all security tools commonly used for phishing enrichment and response

- **Intuitive Response Playbooks**
  OOTB and custom task-based workflows enable security teams to coordinate across teams, products, and infrastructures

- **Automated Actions**
  1000s of automated actions across security tools make scalable phishing response a reality
What is SOAR?

Security Orchestration, Automation, and Response

**Orchestration**
- Playbooks, runbooks, workflows
- Logically organized plan of action
- Controlling, activating security product stack from central location

**Automation**
- Automated scripts
- Extensible product integrations
- Machine execution of playbook tasks

**Response**
- Case management
- Analysis and reporting
- Communication and collaboration
Respond, automate, and manage with Demisto

Alert sources

Respond and automate

Manage incidents

Collaborate and learn

Playbook-based orchestration with 300+ vendor integrations

Ingest, search and query ALL security incidents

Collaborate with other security analysts

© 2019 Palo Alto Networks. All Rights Reserved.
Why Demisto?

Demisto is a workflow automation engine

Respond to incidents with **speed** and **scale**

- **100s** of product integrations
- **1000s** of security actions
- Visual playbook editor
Why Demisto?

Demisto is a security ticketing system

- Standardize process across products, teams and use cases
- Ingest, search, and query ALL security alerts
- SLA/Metric tracking
- Dashboards and Reporting

Workflow Automation Engine

Security Ticketing System

Collaboration Platform
Why Demisto?

Demisto is a collaboration platform

Improve investigation quality by working together

- Virtual War Room
- Real-time security actions
- Auto-documentation
Before Demisto

- Disparate alert sources
- Lack of defined process
- Repetitive and manual actions
- Lack of product interconnectivity
After Demisto

All alerts flowing into one console

Standardized and enforceable processes

Automated high-quantity actions

Cross-product coordination
Breadth of Demisto integrations

Analytics and SIEM
- Cortex
- Fortinet
- McAfee
- Splunk
- Sumo Logic
- DEVO
- exabeam
- LogRhythm
- Micro Focus
- Radar
- Venio

Threat Intelligence
- Bitcove
- Anomali
- Cymon
- domainTools
- Foresight Security
- OpenPhish
- Recorded Future
- Virus Total

Malware Analysis
- paloalto
- FireEye
- Intezar
- JIRA
- Koodous
- Reversing Labs
- ReversingLabs
- SandBox
- Carbon Black
- Cuckoo
- Cisco
- cuckoo
- avast SecureLine
- avast SecureLine

Endpoint
- paloalto
- FireEye
- Intezar
- JIRA
- Koodous
- Reversing Labs
- ReversingLabs
- SandBox
- Carbon Black
- Cuckoo
- Cisco
- cuckoo
- avast SecureLine
- avast SecureLine

Network Security
- Check Point
- PRTG
- Signal Sciences
- zscaler
- VECTRA
- Tufin

Authentication
- CyberArk
- Duo
- Active Directory
- Okta

Email Gateway
- BitDam
- Mimecast
- proofpoint
- Symantec

Ticketing
- Cherwell
- Easy VISTA
- Freshdesk
- Jira Software

Messaging
- Exchange
- Slack
- Twilio
- PagerDuty
- Zoom

Cloud
- Google Cloud
- Microsoft
- Netskope

...and more!
Demisto's process modularity and automation has helped us stay agile as we onboard new technologies. Demisto is really the constant 'music page' that keeps our security orchestra going.

Sean Hastings, Senior Information Security Analyst
Demisto value

- **Standardize and scale processes**
  - Reduced weekly alerts from 10,000 to 500

- **Lower response times with automation**
  - Reduced response times from 3 days to 25 minutes

- **Coordinate actions across security products**
  - Automated 30% of incidents for 1 FTE time saved

*Real stats from Demisto customers*