Harnessing the Power of Behavioral Analytics for Improving SOC Efficiency

Sep 4, 2019

Mel Shakir
SVP Product Development, Securonix
How to Improve SOC Efficiency?

- **Accurate Threat Detection**: Low False Positives
- **Better Risk Prioritization**: Prioritizing Threats by Impact & Stage of Attack
- **Rapid Incident Triage**: Consistent, Automated Workflows
- **Faster Hunting**: Analyst Training Derived IoC Relationships
## Current State of Affairs

### Alert Fatigue
- **6 months**
  - Average time before T1 analysts quit their jobs due to its repetitive nature

### Increased Risk Exposure
- **80%**
  - Organizations receiving 500+ critical alerts investigate only 11 to 25 alerts/day

### Slow Response Time
- **107 days**
  - An adversary is able to survive in the enterprise due to missed alerts

### Skill Shortage
- **2 million**
  - Shortage of cybersecurity professionals in 2019

---

**Analysis & Planning**
- 11%

**Execution**
- 25%

**64%**
- Manual Processes
- Repetitive Tasks
- Disintegrated Tools
Analytics Driven Threat Detection
Fewer High-Risk Alerts + Entity Context

Legacy SIEM Approach:

- SIEM
- Lots of Low Value Alerts
- SOAR
- Lots of Low Value Incidents

Next Gen SIEM Approach:

- SIEM Alerts
- User Entity Attribution
- Behavior Analytics
- Threat Chains
- SOAR

- Too Many Low Value Alerts
- Fewer High-Risk Alerts + Entity Context
- Fast, Efficient Response

© 2019 Securonix. All Rights Reserved. Confidential
## Sample Machine Learning Models

<table>
<thead>
<tr>
<th>Model</th>
<th>Algorithm</th>
<th>Threats Detected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rare behavior detection</td>
<td>• MinMax clustering algorithm (Securonix Proprietary)</td>
<td>• Zero day process/service execution</td>
</tr>
<tr>
<td></td>
<td>• Good-Turing</td>
<td>• Data exfiltration</td>
</tr>
<tr>
<td></td>
<td>• Fuzzy Matching</td>
<td>• Account sharing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Privilege escalation and misuse</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Network reconnaissance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Account/Password Spraying</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Personal email account egress</td>
</tr>
<tr>
<td>Frequency/Amount spike detection</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enumeration detection</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Peer outlier detection</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Land Speed Analyzer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Traffic Analyzer</td>
<td>• Random Forest Regression and Entropy estimation</td>
<td>• C2 Communication</td>
</tr>
<tr>
<td></td>
<td>• Online Kernel based clustering</td>
<td>• Domain Generation Algorithm (DGA)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Lateral movement</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Network circumvention</td>
</tr>
<tr>
<td>Phishing Analyzer</td>
<td>• Fuzzy Matching</td>
<td>• Phishing detection</td>
</tr>
<tr>
<td></td>
<td>• Weighted Levenshtein Distance</td>
<td>• Impersonation detection</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• BEC (compromise)</td>
</tr>
<tr>
<td>Response Bot</td>
<td>• Mondrian forests</td>
<td>• To learn from analyst case disposition for the application to prioritize threats for analysts going forward</td>
</tr>
</tbody>
</table>
Behavior Analytics Example 1

**Super Enrichment**
David is a contractor

**Event Rarity**
User badges in at an odd time – 5 AM

**Peer Analysis**
Access design files (IP) never accessed by peers

**Behavior Analysis**
Transfer data to USB – Spike in files copied

**INSIDER THREAT MODEL (STAGES)**

- INHERENT USER RISK
- ACCOUNT MISUSE
- DATA COMPROMISE
- EXFILTRATION

© 2019 Securonix. All Rights Reserved. Confidential
Behavior Analytics Example 2

Rules Engine
John gets a phishing email

DGA + Third Party Intel
He clicks on it and is directed to a malicious site

Beaconing Pattern
His machine is compromised and starts communicating with CNC

Spike in files accessed
Large number of files accessed and modified (encrypted)

RANSOMWARE THREAT MODEL (STAGES)

- RECON
- DELIVERY
- INSTALLATION
- EXPLOITATION
Analytics Assisted Risk Prioritization
Risk Prioritization by Scoring Entity Behavior
Risk Prioritization using Threat Chains

Cyber Threat Chain

Stage 1: Recon
- Risk Score: 0.6
- Policy: Spam Email
- Duration: 2 days
- Event: User receives Spam
  - Low Risk

Stage 2: Exploitation
- Risk Score: 0.53
- Policy: Suspicious Windows Remote Login Source Anomaly
- Duration: 5 days
- Event: Suspicious login and malware infection
  - Medium Risk

Stage 3: Installation
- Risk Score: 0.63
- Policy: Unusual Process on a Host
- Duration: 15 days

Stage 4: Command & Control
- Risk Score: 75.8
- Policy: Robotic Beaconing Traffic Detected
- Event: System Compromise
  - High Risk
Analytics Driven Triage
- Securonix SIEM threats are mapped to SOAR playbooks
• Playbooks can be launched automatically or manually

• Securonix SIEM recommends playbooks to execute
Recommended Triage Actions

Replicating Analyst actions enables SOC to respond faster and consistently to threats while reducing the overhead on Analysts

• Learn Tier 3 Analyst actions

• Recommend actions to Tier 1 Analyst or take automated action

• Result → Consistent triage; Reduce number of escalations to Tier 2/3 Analyst
• Multiple Playbooks can be launched simultaneously
• Status of Playbook(s) is seen from the SIEM UI
Analytics Assisted Hunting
Actionable Context: Derived IoC Relationships

Improved tracking of relationship of IoC’s linked to the same violator

PRE-ATT&CK™  Enterprise ATT&CK™

Recon  Weaponize  Deliver  Exploit  Control  Execute  Maintain

ATT&CK™ Technique

Phishing Email  Visit to Malicious Site  Malware Detection  Beaconing  Lateral Movement  Exfiltration

Observed Indicators of Compromise

Sender Email Address  Account name  Source IP Address, Hostname  Source IP Address, Hostname  Account name, Hostname  Account name

Recipient Email Address  Destination IP Address  Destination IP Address, Hostname  Destination IP Address, Hostname  Destination IP Address, Hostname  Destination IP Address, Hostname

Web link  Web URL  Process name  Web Domain  File Attachments  File Attachments

User

IP Address  Account Name

MAC Address  Hostname

Email
Link & Graph Analysis
Securonix Solution Overview
Securonix Solution
Features best MTTR from detection to remediation

- Single Integrated Solution → Securonix Next Generation SIEM with UEBA, and SOAR add-on

**Rapid, Playbook-Driven Investigations w/ Adaptive Learning**

- **Advanced Threat Detection**
  - User Entity Attribution
    - Context for faster investigations
  - Machine Learning
    - High-fidelity alerts reduce false positives

- **Prioritized Threats**
  - Threats Chains
    - Prioritize threats using MITRE kill-chain
  - Response Bot
    - Learns L3 analyst actions eliminating L1 guesswork

- **Faster Hunting**
  - Rapid Searching
    - Of evidence with integrated SDL platform
  - Link Analysis
    - Connects IoC’s for visual investigations

- **Rapid Incident Triage**
  - Automated Playbooks
    - Mapped to Securonix threats for fast, consistent threat triage
  - 275+ Connectors
    - And 3000+ actions provides more automation and rapid TTV

Multi-tenant support for On-premise and Securonix Cloud Privacy Features for GDPR compliant SOC workflows
Securonix Solution Benefits
Maximizes cost savings through integration, automation and higher efficiency

Solution Benefits

- **Faster Investigations / Measurable ROI**
  - SIEM with UEBA and SOAR automation results in less operational overhead in training and enablement
  - Measure and boost SOC efficiency with SLA tracking

- **Prioritized Threats / Improved Efficiency**
  - High fidelity alerts allow a SOC to scale with fewer analysts

- **Rapid Time to Value (TTV)**
  - Large number of OOTB connectors and integrations allows new use cases to be rapidly implemented

Challenges Addressed

- **Alert Fatigue**
  - Average time before T1 analysts quit their jobs due to its repetitive nature
  - 6 months

- **Slow Response Time**
  - Organizations receiving 500+ critical alerts investigate only 11 to 25 alerts/day
  - 80%

- **Increased Risk / Exposure**
  - An adversary is able to survive in the enterprise due to missed alerts
  - 107 days

- **Lack of skilled professionals**
  - Predicted shortage of cybersecurity professionals by 2019
  - 2 million

Delivering SOC Efficiencies with Security Orchestration Automation and Response (SOAR)
General Dynamics Whitepaper, Jun 2018
Faster Investigations

- Automated playbook reduces “Suspicious activity” triage time from 19-37 min to 11-26 seconds

Delivering SOC Efficiencies with Security Orchestration Automation and Response (SOAR)
General Dynamics Whitepaper, Jun 2018
### Measurable ROI

- **Solution Metrics Include:** Resolved incidents, Mean dwell time (MDT), Mean time to resolve (MTTR), Full time employee (FTE) Gained, Playbooks & Actions Run, Time saved, Dollars saved ($)

<table>
<thead>
<tr>
<th></th>
<th>Time Per to Complete</th>
<th>Weekly Incidents</th>
<th>Time Spent</th>
<th>Time</th>
<th>Cost Savings</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Annually</td>
<td>Savings (Hours)</td>
<td>Savings (%)</td>
</tr>
<tr>
<td><strong>Manual</strong></td>
<td>45</td>
<td>50</td>
<td>390</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td><strong>Semi-Automated</strong></td>
<td>22</td>
<td>75</td>
<td>190</td>
<td>200</td>
<td>75%</td>
</tr>
<tr>
<td><strong>Automated</strong></td>
<td>1.4</td>
<td>100</td>
<td>12</td>
<td>378</td>
<td>98%</td>
</tr>
</tbody>
</table>

**Cost Savings**

- **Manual:** 0%
- **Semi-Automated:** 75%
- **Automated:** 98%

**Time Per to Complete:** Minutes

**Weekly Incidents:** Incidents

**Time Spent:** Hours

**Time:** Hours

**Cost Savings:** Dollars saved ($150/h)

---

**FASTER RESPONSE**

**INCREASE MORALE**

**MANAGE ALERTS**

© 2019 Securonix. All Rights Reserved. Confidential
Rapid TTV with OOTB Threats & Playbooks

- Securonix Insider and Cyber threats / use cases mapped to Securonix SOAR Playbooks

- Insider - Data Exfiltration
- Malware Beaconing
- Ransomware
- DNS Attack

- Phishing - Business Email Compromise
- Lateral Movement
- System Lock Down
- Brute Force

- Identity Compromise
- File Quarantine
- Deploy Patch
- Vulnerability Scan

Sample Playbooks
Insider Playbook leverages additional playbooks

- Data Exfiltration
- Cross Channel Egress
- Privilege Abuse Triage
- Create Case for L3 Analyst
- HR/Legal Workflow

**Inherent Risk Indicator Triaging**

- Is user in watchlist?

**Verify Document Sensitivity**

- Check internal network shares
- Check document classification system
- Check past internal communications

**Is document sensitive?**

- Yes
- No

**Data Exfiltration**

- Insurer Threat Model Alert

**Cross Egress Channel**

- Privilege Abuse Triage

- Is user meeting criteria?

- Yes
- No

**Create Case for L3 Analyst**

- Attach logs as Evidence

- Initiate HR/Legal workflow

© 2019 Securonix. All Rights Reserved. Confidential
Cyber - Malware Beaconing Playbook

Malware Beaconing Playbook leverages additional playbooks
- Vulnerability Scan
- System Lock Down
- Deploy Patch
Rapid TTV with Wide-Ranging Integrations

- 275+ Connectors and 3000+ actions
- List grows every 3 weeks
- Latest List at https://documentation.securonix.com/connectors/
Securonix Solution Flows

Multifaceted bi-directional integration improves analyst experience

- Securonix SIEM launches Securonix SOAR playbooks - automated or manually
- Securonix SOAR attaches context, launches actions, attaches evidence in SIEM UI
- Securonix utilizes advanced machine learning to learn actions and make recommendations

Detection

Algorithms

Learn

Actions

Hunting

Auto Launch Playbook(s)

Entity Risk Score

Create Case

Recommended Actions

Manually Launch Playbook

Get External Context

Launch Actions

Gather Evidence

Launch Actions

SECURONIX SIEM

Threats

SECURONIX SOAR

Playbooks & Actions
Demo Video (2 min)
Questions?
Thank You!