Orchestrate. Automate. Accelerate. (like a PM)

October 3, 2018
Jadon Montero
Senior Product Manager, SOAR
Orchestration & Automation

ORCHESTRATE
Your Teams and Tools

AUTOMATE
Manual, Repetitive Tasks

ACCELERATE
Security and IT Operations
AUTOMATE

Streamline your manual, repetitive tasks with connect-and-go workflows.
ORCHESTRATE

Connect your teams and tools for clear communication and complete integration across your tech stack.
ACCELERATE

Supercharge your operations with automation that creates efficiency without sacrificing control.
Commonly Automated Use Cases

Increase efficiency across your organization

- Automated Patching
- Malware Investigation & Containment
- Provisioning & Deprovisioning
- Privilege Escalation Investigations
- Email Phishing Investigations
- Threat Hunting
- Security Alert Data Enrichment
- Much More
The Need for Security Orchestration & Automation
The global cybersecurity workforce will be short by around 1.8 million people by 2022, representing a rise of around 20 percent since 2015, according to a new report by Frost & Sullivan.
The average enterprise uses **75** security products to secure their network.
Stat: The Cisco 2017 Security Capabilities Benchmark Study found that organizations can investigate only 56 percent of the security alerts they receive on a given day. Half of the investigated alerts (28 percent of all security alerts) are deemed legitimate; less than half of legitimate alerts are remediated. In addition, 44 percent of security operations managers see more than 5000 security alerts per day.

Too Many Alerts

Thousands competing for the security team’s attention per day.
REPEETITIVE, MANUAL PROCESSES
REPETITIVE, MANUAL PROCESSES
REPEATITIVE, MANUAL PROCESSES
REPETITIVE, MANUAL PROCESSES
REPEATITIVE,
MANUAL
PROCESSES
Barriers to Successfully Automating Security
One size does not fit all
Teams Lack Time for Custom Automation
OPERATING IN SILOS
Thinking Like a Product Manager
PM Toolkit: User Personas
Security User Personas

Then I was hacked, and as a result one of my patients was murdered.
Realistic User Personas

The Ross
AppSec-obsessed Engineer
- Experienced in C#, Go, Java
- Regularly vets code for vulns
- Is always on the cutting edge of tech
- Likes beers, brews his own

The Stabby
Manager with Most Commits on Team
- Go superstar and Thought Leader
- Releases features on time
- Mistrusts new tech w/ age and wisdom
- Wine >= whiskey > beer

The Jadon
How did he pass the interview?
- Wrote a song in college in Haskell
- Has had Github access revoked 2x
- Considers the Snapchat UI "new tech"
- D. All of the above
Automation IS a Product!

- Must play nicely with 3rd party tools
- Must be reliable
- Must update with an environment
PM Toolkit: Taking Inventory
Your Goal is Deceivingly Difficult...

The diagram illustrates a security workflow involving various steps, including an alarm, asking an employee if it is them, confirming via 2FA, and escalating to security. The user interface includes options for responding "Yes" or "No, that wasn't me."
Holacracy® is a new way of structuring and running your organization that replaces the conventional management hierarchy. Instead of operating top-down, power is distributed throughout the organization, giving individuals and teams more freedom to self-manage, while staying aligned to the organization’s purpose.
Know your Process

Request for access?

- IT validation with managers / system owners
- Manually creating accounts

Access Granted
Know your Tools
Know your Talent

WORKFLOW BUILDING BLOCKS

- Trigger
- Action
- Filter
- Pattern Match
- Loop
- Human Decision
- Automated Decision
- Artifact
PM Toolkit: Dedicated Sprint Buffer
Make Time on Your Roadmap....
PM Toolkit: User Stories
User Stores

Who are you?

What do you need?

Why?
PM Toolkit in Action: OSSEC Enrichment and Remediation
Practical OSSEC

GIAC (GCIH) Gold Certification

Author: Chad Robertson, chadrober@gmail.com
Advisor: Egan Hadsell

Accepted: July 5, 2011

Abstract

OSSEC is a simple to install host-based intrusion detection system. The difficulty is in tuning the installation so that the resulting alerts are pertinent to the environment. Agents can be installed on a variety of systems; Web servers, mail servers, VMWare servers, WAFs. All of these server types likely produce logs with very different syntax. Each log type requires custom decoders and rules to be created for OSSEC to alert appropriately if none are included by default or found within the community. Resulting alerts must be ranked by level of criticality based on not only one single log event but possibly the presence of other events occurring during small windows of time. All of this must result in notification being sent to the appropriate party and at the appropriate level to allow them to respond to the incident. This paper will briefly discuss installing OSSEC agents on both Windows and Linux systems. It will then explore how to configure rulesets and decoders for various commonly found enterprise servers. Finally, it will describe the process of tuning rulesets so that the resulting alerts are both valuable and pertinent.
TOO MANY ALERTS, TOO LITTLE TIME...
COMPOUNDED BY SEVERAL ALERT TYPES

- OSSEC Alerts
  - Rootcheck Alerts
  - Rules Alerts
    - Network
    - Non-Network
  - Syscheck Alerts
CONTEXTUAL REMEDIATION IS KEY

Image for different communication stack: slack, email, hipchat.

Image for different endpoint tools: carbon black, crowdstrike, etc.

Image for different technology stack: amazon, okta vs duo, etc.
Jon Schipp
Director of Security Engineering, Rapid7
ALL PATHS BEGIN WITH A PARSER

```plaintext
*** Alert 1471016950.7633: - ossec,rootcheck,
2018 Aug 12 15:13:30 (connect.dev.local) any->rootcheck
Rule: 510 (level 7) -> 'Host-based anomaly detection event
(rootcheck).
Src IP: 116.31.116.16
User: root
Port '35436'(tcp) hidden. Kernel-level rootkit or trojaned version of
netstat.
```

```json
{
"alert": {
"timestamp": "2018 Aug 12 15:13:30",
"user": "root",
"alert_id": 1471016950.7633,
"logs": [
"Port '35436'(tcp) hidden. Kernel-level rootkit or trojaned version of netstat."
],
"level": 7,
"rule_id": 510,
"agent": "connect.dev.local",
"category": "ossec,rootcheck,",
"rule_name": "Host-based anomaly detection event (rootcheck).",
"source_ip": "116.31.116.16"
}
}
```
On a timer, bind() to all TCP/UDP ports where an agent is installed. If it fails then a rootkit is likely installed.

As an analyst in the SOC, I would like for all incoming rootcheck alerts to be parsed for a port, retrieve the offending process, and kill it on the endpoint.

```
$ Stop-Process -Verbose -Force -id 24260
```
REMEDIATE!
KILL THE PROCESS.

Highlights:

- Simple, 4 step workflow
- As technical as your team desires
- Cb, powershell can be replaced with any endpoint tool or custom services
  - SSH, Symantec, Endgame, Check Point
- Can also rollback Windows Registry Keys
On an interval, check file hashes and generate alerts for changes.

As an analyst in the SOC, I want all hashes from syscheck alerts to be analyzed by at least two 3rd party tools, and for the aggregated info to be emailed to me.
ENRICH! LOOKUP HASH AND NOTIFY THE SOC

Highlights:

● Decision steps for hash existence and found malware
  ○ Less noise as reports are generated on demand
● No single point of failure because multiple 3rd parties are leveraged
● Can add in any number of OS tools to reduce overhead
● Can replace email depending on your communication stack
Customizable pattern matching on network logs, for example: ssh brute force attacks, tcp wrappers, and apache logs.

As an analyst in the SOC, I would like for all incoming network rule alerts to kick off bogon and geoIP lookups for relevant IPs and immediately block them by modifying EC2 VPC ingress and egress rules.
BOGONS AND MARTIAN PACKETS??!!!
ENRICH AND REMEDIATE!

Bogon & GeoIP Lookup -> Update VPC Ingress/Egress Rule

Highlights:

- Filtering logic to decide if a sourceIP is private or public
- Allows you to do any number of lookups on dynamic threat intel feeds
- Easily sub in remediations for a physical infrastructure
HOW WOULD YOU REMEDIATE IN YOUR ENV?
HOW WOULD YOU REMEDIATE IN YOUR ENV?

```
[root@localhost ~]# grep -h 'description.*sudo' /var/ossec/rules/* | awk -F 'description>' '{ print $2 }' | sed 's/<\/>/'
Initial group for sudo messages
Failed attempt to run sudo
Successful sudo to ROOT executed
First time user executed sudo.
Three failed attempts to run sudo
Unauthorized user attempted to use sudo.
```
HOW WOULD YOU REMEDIATE IN YOUR ENV?

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>apache_rules.xml</td>
<td>apparmor_rules.xml</td>
<td>arwatch_rules.xml</td>
<td>asterisk_rules.xml</td>
<td>attack_rules.xml</td>
<td>cimserver_rules.xml</td>
</tr>
<tr>
<td>clam_av_rules.xml</td>
<td>courier_rules.xml</td>
<td>cisco-ios_rules.xml</td>
<td>clam_av_rules.xml</td>
<td>clirules.xml</td>
<td>dovecot_rules.xml</td>
</tr>
<tr>
<td>dropbear_rules.xml</td>
<td>exim_rules.xml</td>
<td>firewalld_rules.xml</td>
<td>firewall_rules.xml</td>
<td>ftpd_rules.xml</td>
<td>hordeimp_rules.xml</td>
</tr>
<tr>
<td>ids_rules.xml</td>
<td>imapd_rules.xml</td>
<td>local_rules.xml</td>
<td>mailscanner_rules.xml</td>
<td>mcafee_av_rules.xml</td>
<td>msql_rules.xml</td>
</tr>
<tr>
<td></td>
<td>msauth_rules.xml</td>
<td>ms_dhcp_rules.xml</td>
<td>ms-exchange_rules.xml</td>
<td>ms_ftpd_rules.xml</td>
<td>mysql_rules.xml</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ms_se_rules.xml</td>
<td>named_rules.xml</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>netscreenfw_rules.xml</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>nginx_rules.xml</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>openbsd_rules.xml</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>opensmtpd_rules.xml</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ossec_rules.xml</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>pam_rules.xml</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>php_rules.xml</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>pix_rules.xml</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>policy_rules.xml</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>postfix_rules.xml</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>postgresql_rules.xml</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>proftpd_rules.xml</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>pure-ftp_rules.xml</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>raccoon_rules.xml</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>roundcube_rules.xml</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>rules_config.xml</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>sendmail_rules.xml</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>smbd_rules.xml</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>solaris_bsm_rules.xml</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>sonicwall_rules.xml</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>spamd_rules.xml</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>squid_rules.xml</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>sshd_rules.xml</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>symantec-av_rules.xml</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>symantec-ws_rules.xml</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>syslog_rules.xml</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>syslogon_rules.xml</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>systemd_rules.xml</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>telnetd_rules.xml</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>trend-osce_rules.xml</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>unbound_rules.xml</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>vmfire3d_rules.xml</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>vmware_rules.xml</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>vpn_concentrator_rules.xml</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>vpopmail_rules.xml</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>vsftpd_rules.xml</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>web_appsec_rules.xml</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>web_rules.xml</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>wordpress_rules.xml</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>zeus_rules.xml</td>
</tr>
</tbody>
</table>
Think like a PM and use the toolkit!