Prescriptive Risk Solutions, LLC

*March 2017*

# CISO Series on Today's Critical Issues

## Automation & Orchestration

*By Tari Schreider C|CISO, CHS-III, CRISC, ITIL™ v3, MBCI, MCRP, SSCP*

*Chief Cybersecurity Strategist & Author*

*Prescriptive Risk Solutions, LLC.*

EC-Council

http://ciso.eccouncil.org/

# Cybersecurity Countermeasures Sprawl

Today, CISOs have a dizzying array of cybersecurity technologies offering the promise of a securer tomorrow. Each in of themselves performs their appointed mission of protecting assets and information with aplomb. Layer by layer one security technology is stacked upon another hoping to achieve defense in depth. Somehow; however, the bad actors still find a way around our defenses. No wonder CISOs have trouble asking for funding for the next galactic malware cure. CFOs may not say it, but they are thinking it, "if you cannot make what we have work together to reduce our risk, we're just throwing good money after bad."

If there were only way to leverage our growing complexity of desperate cybersecurity technologies and force multiply our limited SecOps personnel with machine agility and speed. Well there is my fine CISO friend, there is. The age of automation and orchestration is dawning. Solutions now exist that allow you to automate your cybersecurity playbooks. With an extensible automation and orchestration platform, you can programmatically curate from your inventory of countermeasures your response to various threat scenarios.

## MARKET ADOPTION

You may have already seen their booths at RSA or received marketing grams from various security automation and orchestration vendors and wondered does this thing have legs? To answer in a word, yes. MarketandMarkets Research published a report in 2016 forecasting the security orchestration market will grow from $826.1 Million in 2016 to $1.682.4 Billion by 2021, at a Compound Annual Growth Rate (CAGR) of 15.3%.

Some companies jumped on the security automation and orchestration train early by announcing integration partnerships.

An example of seemingly early adoption would be the Tufin Orchestration Suite™ integrating with Cisco® Firewalls. These partnerships were generally a space holder to allow vendors to figure this market out and create products that actually live up to the promise of security automation and orchestration.

The field of players is becoming crowded and I expect an aggressive 2017 M&A season to follow on previous year's activity. In 2016, we witnessed IBM acquiring Resilient Systems and FireEye acquiring Invotas as well Cisco Systems acquiring Tail-F in 2014.

## KEY PLAYERS

At my last count, there were over thirty providers of products claiming placement within the security automation and orchestration market. If you attended RSA in February, you should have noticed these products were all the rage. Some claim they are a full automation and orchestration suite while others are carving out narrow niches in areas like policy orchestration or automated incident response.

Below are the ones creating the most chatter:

Bounties paid by companies can average from $200 to $200,000; however, an average reported by bugcrowd was $505.79. With a growing number of bounty hunters and bounty platforms, companies are looking for ways to gain notice by the industry's top bug researchers.  United Airlines for example offers frequent flyer miles.

The following are several bounty programs that standout from the crowd:

- Bradford Networks - Network Sentry
- Cisco Systems – Process Orchestrator
- Cyberbit SOC 3D
- CyberSponse Inc.
- Demisto
- DFLabs - IncMan
- Exabeam Security Intelligence Platform
- FireEye, Inc. – Security Orchestrator
- Gemini Atlas Platform
- Hexadite AIRS
- IBM Corporation - Resilient Incident Response Platform
- Intel – Open Security Controller
- Komand Security Orchestration & Automation Platform
- Phantom Cyber Corporation
- Resolve Systems
- Swimlane LLC
- ThreatNexus Orchestration Engine
- Tufin Orchestration Suite

When looking at these products you will need to recognize that half of them will no longer either be in business or operate as an independent company within the next two years. You should also note that this is an arms race with feature advantage changing sides often.

I have not mentioned the girth of log management and security incident and event management (SIEM) products that have just created white papers to convince us they are a security automation and orchestration solution.

# The Promise of Automation & Orchestration

The promise of automation and orchestration solutions lies in use cases. Depending on your solution, you can improve just about any SecOps function or process.

Below are some of the use cases best served by these solutions:

| USE CASE | RATIONAL |
|---|---|
| Alert Resolution | Reduce effort to aggregate, correlate, and resolve alerts from multiple sources. |
| Detect & Patch | Automate risk scoring of patch advisories, scan for missing patches and remediate in one continuous motion. |
| Incident Response | Execute incident response playbook in real-time. |
| Integrate Cybersecurity Countermeasures | Automate security technologies to work as a cohesive integrated workflow. |
| Metrics & Report Consolidation | Reduce time required to chase down metrics, consolidate results and produce reports. |
| Threat Intel Fusion | Reduce time and effort to source, analyze and report on threat intelligence from multiple sources. |

From what I can see from these products, your imagination is your only limitation on how deep you can automate SecOps.

## ALL THAT GLITTERS IS NOT GOLD

If you are waiting for the other shoe to drop, well listen – thud there it is.  Security automation and orchestration solutions are the next best thing to sliced bread, but they are not magic. You have to model your processes in advance before you can automate and orchestrate them. These solutions have no idea what you want to accomplish unless you tell them. Remember that old adage "garbage in, garbage out?"

Modeling a process is a 360-degree exercise. You will need to consider People, policies, procedures, processes, products and proof (metrics). It is only through the union of these domains does automation and orchestration occur.

I know what you are thinking, "I can get rid of all my SecOps staff through automation and orchestration. I will have a lights out SecOps." Wait what? Nice try but it does not work like that, you will still need people. Your goal is to root out the rote tasks of SecOps freeing your people up to focus on the strategic aspects of your cybersecurity program. Yes you may be able to stave off hiring more staff addressing the growing skills gap, but don't go into acquiring a security automation and orchestration solution thinking you're going to cut staff.

## SECRET SAUCE: PLAYBOOKS & PARTNERS

Sometimes the difference in being compromised or not is a matter of seconds. Security and automation software provides the ability to respond to attacks at machine speed. Designed to execute preset detection protocols, these solutions reduce the dependence on manual intervention. Some of the solutions already come with playbook templates.

Solutions that offer the broadest partner eco system and customizable library of playbooks should be at the top of you evaluation list. However, in order for them to acquire either, they will have had to log time in the seat. You will want a company, whose product has a reasonable size customer base (25+) and can provide evidence of automating and orchestrating dozens of security products within the same client.

# Eliminating Your MSSP

Security automation and orchestration has been the secret of Managed Security Service Providers (MSSP) for years. However, their solutions where mostly hybrids of service management tools or custom code written specifically for their SOCs. Having managed SOCs around the world, I know thing or two about what goes on behind the scenes. I can also say that some of you are perfect candidates for replacing your expensive MSSP contract through the introduction of an automation and orchestration solution.

Most organizations gravitate to an MSSP because they do not have the people to watch their network around the clock. In addition, when a critical event does happen, most companies still want a call in the middle of the night. What if you could eliminate all the white noise of SecOps, automate your incident response and receive a call only in times of emergency? It can happen when you implement security automation and orchestration solutions.

## DEVOPS

DevOps has produced one of the most profound changes in IT in the past five years. In many ways, it is a disruptive technology forever changing the landscape of application development and operations. Security automation and orchestration solutions are perfect for facilitating DevOps by supporting a playbook that integrates security-testing, validation and monitoring throughout the lifecycle of application development to deployment. Playbooks support the integration of security testing into the domain of application programmers rather than security personnel. Application development becomes their own gatekeeper and they no longer can blame deployment delays on the security department. Also, imagine the economies of scale of automating patching and hardening into release builds. In my mind, DevOps justifies moving toward a security and automation solution alone.

## A WORD OF CAUTION

I am a huge believer in taking stock of the past to ensure I do not repeat an incident as a future failure. I searched my disaster archives and found an extreme example of an automation blunder that serves as a cautionary tale. In June 2012, Royal Bank of Scotland's (RBS) NatWest and Ulster Bank subsidiaries descended into chaos following a glitch in their software workflow automation product.

The outage was so profound it got its own Wikipedia page. During the one-month outage, 1,200 branches had to remain open past normal hours, call center staff was doubled and millions of customers suffered. The CEO had to forego his bonus because of the fiasco's impact on roughly 20 million customers, and RBS canceled its presence at Wimbledon that year. Game, set, match.

# Conclusion

Orchestration and automation solutions are not new, but advances in technology has made their time finally come. As we try to maneuver around a critical shortage of IT personnel, manage an average of 60 security products, adapt to DevOps and strive to be more effective and efficient, few choices to accomplish all are left. As the CISO of your organization, you should be leading the charge toward SecOps automation.

## ABOUT THE AUTHOR

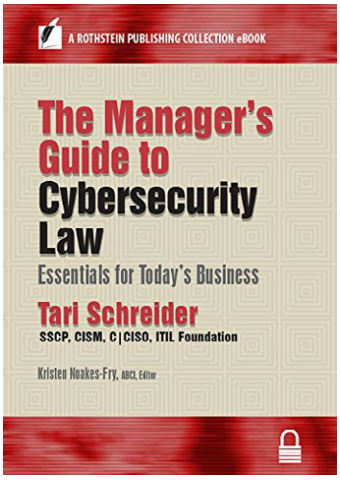
### TARI SCHREIDER

*C|CISO, CHS-III, CRISC, ITIL™ v3, MBCI, MCRP, SSCP*

Chief Cybersecurity Strategist & Author
Prescriptive Risk Solutions, LLC.
Atlanta, GA - Cheyenne, WY

www.prescriptiverisksolutions.com
tari@prescriptiverisksolutions.com

M: Atlanta – 678.595.2818
M: Cheyenne – 307.215.1330




The Manager's Guide to Cybersecurity Law

Qualifies for Five (5) EC-Council ECUs.