White Paper

HardenStance

Next Steps in Playbook Driven Cyber Security

By Patrick Donegan, Principal Analyst, HardenStance

Sponsored by:

September 2019

Executive Summary

- Cyber security must become more playbook-driven to reduce the time to respond to threats. Priority should be given to leveraging and adapting generic playbooks.
- The model to aspire to is the airline industry model of physical security operations which is highly orchestrated and automated, as well as reviewed and rehearsed.
- User organizations need to commit to defining, documenting and maintaining their security playbooks. Without that, there can be no effective security automation.
- Automating basic Defensive playbooks is a lot easier than automating Incident Response (IR) playbooks.
- More standardized security operations enable playbooks to run to completion faster.
- Most enterprises can't manage security playbooks very well. Providers of managed security services should prioritize investing in managed playbook services.

In Cyber Security Operations, Time is Money

Despite increasing cyber security spending, the costs of a data breach are still growing:

- The Ponemon Institute's "Cost of a Data Breach 2019" survey shows that the global average total cost increased to $3.92 million in FY 2019, up 1.5% on FY 2018.
- Using a different methodology, Accenture's annual "Cost of Cyber Crime 2019" report yields an average cost of $13 million for 2018, up 12% on $11.7 million 2017.

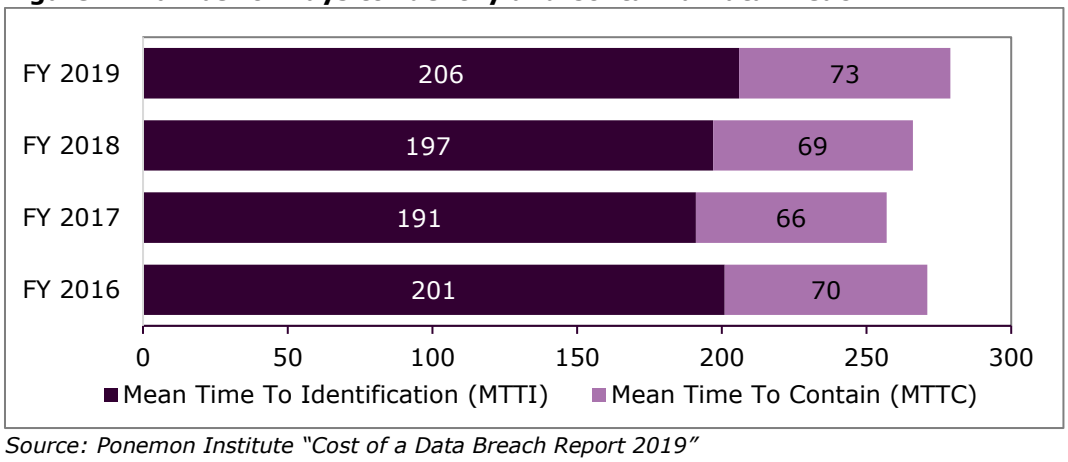
Alarmingly, the average time it takes an organization to identify and contain security incidents is actually getting longer.

As shown in **Figure 1,** a key reason that the average cost continues to climb is that, alarmingly, the average time it takes organizations to identify and contain security incidents is actually getting longer. If you can contain an incident within a few minutes, usually not too much harm will come of it. If an attacker is able to move laterally and dwell within the environment for days, weeks or months, the damage increases. The Ponemon Institute even puts a number on this. A breach with a lifecycle longer than two hundred days costs an organization 37% more than one with a lifecycle shorter than two hundred days ($4.56 million vs. $3.34 million) according to the Ponemon survey.

This White Paper looks at the role that cyber security playbooks (or runbooks) play in reducing the time security analysts spend on known threats; the number of threats that become full-blown incidents; and the time taken to contain incidents when they occur. It focuses on the following two key requirements for playbook-driven cyber security:

- a commitment to creating, implementing and maintaining cyber security playbooks as a foundational component of cyber security strategy.
- the automation of as many steps as possible in those security playbooks.

Figure 1: Number of Days to Identify and Contain a Data Breach



Source: Ponemon Institute "Cost of a Data Breach Report 2019"

Definition of a Playbook

The Collins English Dictionary defines a 'playbook' as "a range of possible set plays" and "a notional range of possible tactics". Adversaries have been using and sharing highly automated attack playbooks for many years. This reduces their costs, increases their reach and effectiveness, and maximises their ROI.

The MITRE Adversarial Tactics Techniques and Common Knowledge (ATT&CK) Framework, shown in **Figure 2,** was developed in 2018 by the Mitre Corporation, a US not-for-profit organization that manages federally funded R&D centres supporting several government agencies. It is one of a number of examples of efforts by the cyber security community to match what attackers are doing by sharing open access to well-known attack playbooks.

ATT&CK is already widely used by many user organizations as well as by many of the world's leading cyber security vendors.

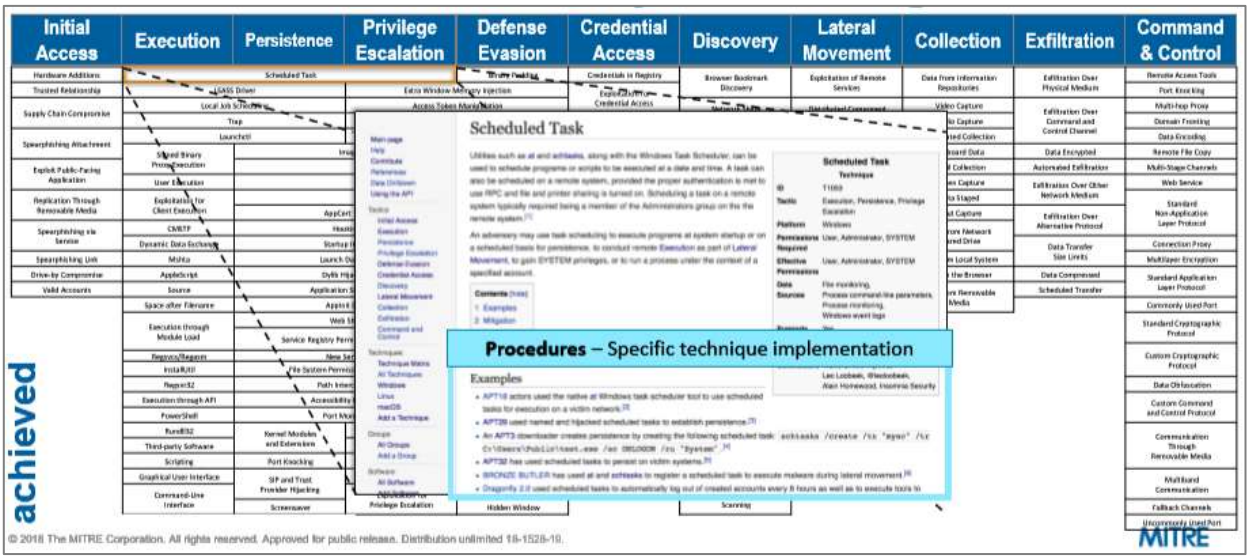
The Mitre ATT&CK Framework is Proving Increasingly Popular

ATT&CK details threat group behaviour in terms of the step by step tactics, techniques and types of software they use, as well as the key geographies in which each adversary is active. In the year since its release, ATT&CK has become very popular. It is already used by a number of leading user organizations as well as by many of the world's leading cyber security vendors spanning many of the most important cyber security product categories. These users and vendors, together with the Cyber Threat Alliance, value the common language that ATT&CK provides for describing the behaviour of adversaries.

Defenders are using ATT&CK as a key threat intelligence tool that helps them allocate limited security budgets efficiently. It helps them create security playbooks that are customized to the highest risk attacks that they are most likely to face in their specific industry sector, and in the context of their unique organization and IT environment. For users that are already leveraging it, ATT&CK is becoming key to updating and executing security playbooks quickly in multi-vendor environments, including through automation.

Security playbooks need to be central to any organization's cyber security posture and preparations for suffering a data breach. Rather than creating them from scratch themselves, users should leverage security playbook resources that are already widely and freely available. These are available from a range of sources including vendors, managed security providers and organizations like the National Institute of Science and Technology (NIST) in the US and the SANS Institute. According to the 80/20 rule, users can take 80% of the content in a generic security playbook and either customize the rest themselves or get a managed security partner to do it for them.

Figure 2: The Mitre ATT&CK Framework



Source: The MITRE Corporation

Throughout this paper, reference is made to both Defensive Playbooks and Incident Response (IR) playbooks. Even many of the smallest organizations should be embracing Defensive Playbooks. A policy that requires employees to call an outsourced IT helpdesk if they think their laptop has been infected is the simplest form of Defensive playbook. So too is an embedded decision rule for responding to alerts that correspond to well-known threats and a mandate that routine tasks like patching or checking on the status of specific ports should be carried out at specified times or intervals. Security playbooks like these run within the confines of the IT domain today, although organizations should be planning for how to incorporate the OT domain into them over time too.

Incident Response (IR) playbooks, also known as IR plans, kick in once an organization has determined that an incident has taken place, resulting in a live potential threat to the organization's data or other assets. These tend to be a lot more complex, incorporating as many as several dozens of steps. These lead first to threat containment, then eviction and recovery. **Figure 3** shows how Defensive and IR Playbooks form part of a library with an organization's master security playbook. Distinguishing between the two types of playbook is useful in terms of identifying their different roles in preventing an incident from occurring and then responding to an incident that has - or appears to have – occurred. However, a core goal of playbook-driven security should also be to ensure that hand-offs between Defensive and IR playbooks are as seamless as possible.

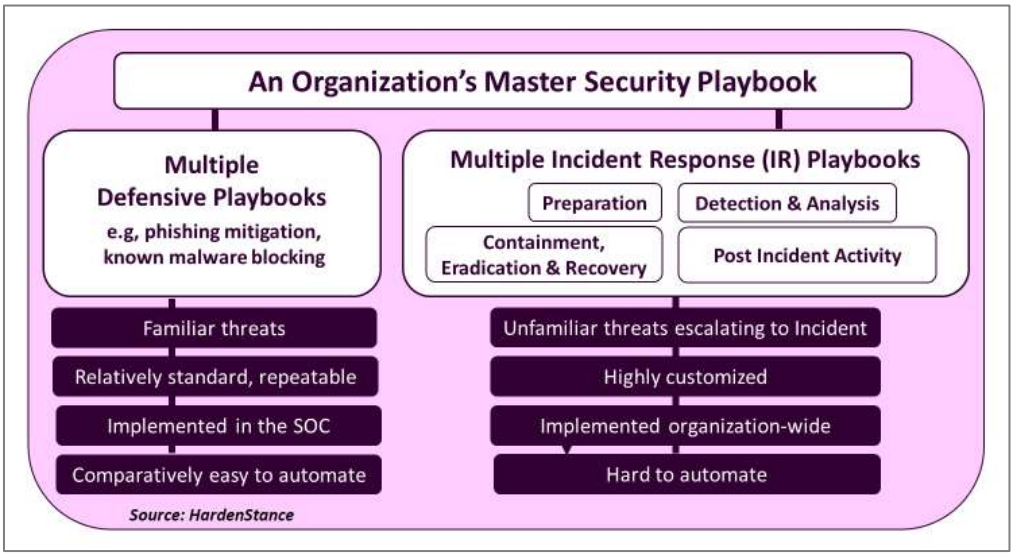
Incident Response Playbooks tend to be a lot more complex than Defensive Playbooks, incorporating as many as several dozens of steps.

Barriers to Adopting Cyber Security Playbooks

As is clear from the dictionary definition, incident playbooks are neither new nor specific to cyber security. Many organizations have detailed playbooks as part of their overall preparedness efforts to protect employees and assets that are exposed to significant physical risk – such as in areas prone to political turbulence or natural disaster. Similarly, in most countries, all organizations of a certain size have to carry out regular fire drills.

These playbooks can be similar from one organization to the next, albeit with variations across and within industry sectors, regions, and size of organization. Specific departments and individuals are assigned set roles within a sequence of steps to mitigate a specific risk. Those responsibilities are captured in the organization's response or business continuity plan. The plan document is then required to be regularly reviewed, rehearsed and updated. In the case of cyber security risk, variations in how the IT estate is architected tend to be significant, leading in turn to greater variation in cyber security playbooks between organizations compared with other types of risk-related playbooks.

Figure 3: Master Playbooks, Defensive Playbooks and IR Playbooks



Most organizations don't rely heavily on cyber security playbooks

The reality of day-to-day cyber security operations around the world is that only a minority of leading organizations in critical industries, such as the banking, energy, healthcare and telecom sectors, have committed to a playbook-driven security model. Few beyond this present-day elite are even familiar with tools like ATT&CK. Today, most organizations don't rely heavily on cyber security playbooks. Among those that do, most only use simple Defensive Playbooks that are operated either internally or outsourced to a third party managed security provider.

Most organizations don't have their own Incident Response Playbooks that extend beyond the IT departments. Neither do they outsource the creation and management of them to a third party. In its 4th annual study on "The Cyber Resilient Organization", the 2019 Ponemon Institute recently found that out of 3,665 IT and IT security professionals surveyed from around the world, only 22% said their company had an IR plan applied consistently across the entire enterprise. Many organizations just hope they won't suffer a major breach. Then, once a breach is discovered, they turn to an IR provider in desperation, typically paying much more than if that same IR provider had been on a retainer as a managed service partner.

Documenting, maintaining and rehearsing internal processes is typically perceived as boring.

Playbook-Driven Security requires a long term commitment

The same inertia that leads many organizations to be complacent about cyber security risk in general can make them unwilling to commit to a playbook-driven security model. Embracing a playbook-driven approach requires a long term strategic commitment. This can be challenging for many security organizations that are under so much pressure that they don't know how to make time for anything other than fighting the next fire.

There are grounds for believing that new data protection laws like the EU's General Data Protection Regulation (GDPR) are having a positive effect in terms of creating extra incentives for organizations to be more strategic in their approach. But other human factors that can prevent organizations moving in this direction still need to be addressed:

- **Documenting, maintaining and rehearsing internal processes is typically perceived as boring**. This legacy mentality has to be unlearnt. Like it or not, this is the foundation of playbook-driven security, hence of security automation. Moreover, there is more to this than creating an initial baseline of playbooks against attacks that may or may not occur in the future. For example, creating new playbooks in real time as a response to emerging situations can be one of the most fulfilling roles in security operations.
- **Some infosec chiefs want to protect their tribal knowledge.** Being 'the one that knows' a company's approach to routine security operations, or has extensive experience in different Incident Response scenarios within an organization's unique environment, can be empowering for security professionals. Some therefore view a requirement to commit to documenting those processes in a playbook – for everyone else to use and learn from – as undermining their own status and value to the organization.
- **Incomplete understanding of automation.** At a high level, C-Level management and information security teams see greater automation as key to improving cyber security. They are right to do so but only up to a point. As discussed in the next section, what many don't fully grasp is that to be effective, security automation relies heavily on a strong foundation of process documentation – i.e. playbooks.
- **There is currently no standardized format for the way that openly available generic playbooks are written and presented**. Without a consistent baseline of common structures, elements and features, it can be hard for users to compare generic playbooks and understand which offer the best models to leverage in their environment and customize them accordingly.

Management needs to be made aware of how playbook-driven security can improve a company's security posture. It needs the will to commit to setting the right goals to achieve it. And it needs know-how in gaining internal support for the strategy.

Realistic Expectations of Playbook Automation

As shown in **Figure 4**, IT and IT security professionals quite rightly consider that greater automation of responses to alerts and incidents is a critical part of the answer to today's cyber security challenges. The more the responses to growing volumes of familiar alerts can be automated, the more analysts can be liberated from chasing around after them and freed up to focus on higher risk threats and proactive threat hunting. Likewise, the fewer steps in complex playbooks that require human intervention, the faster organizations can get to containment and remediation. Ultimately, the model to aspire to is the airline industry model of physical security operations which is highly orchestrated and automated, as well as reviewed and rehearsed.

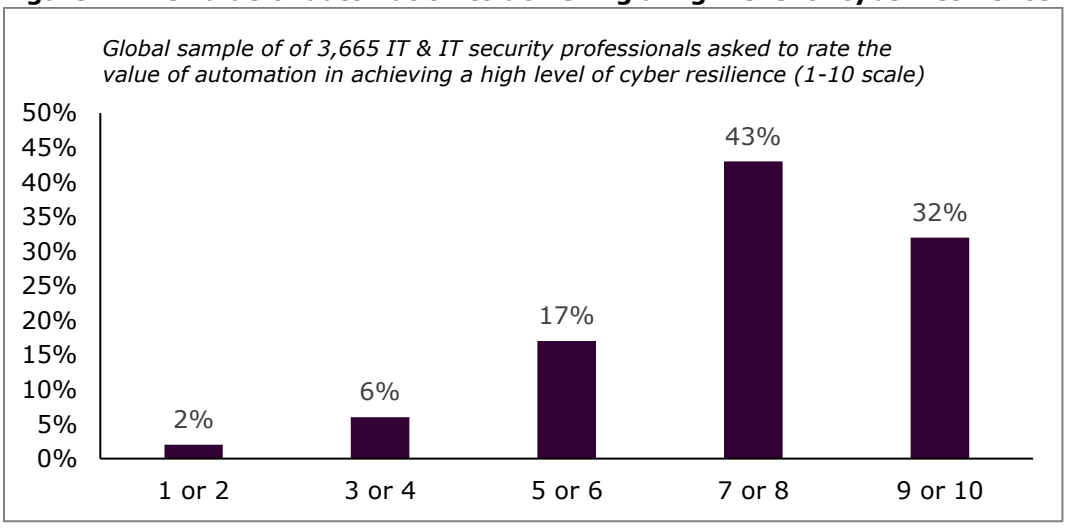
Even some of the most automated playbooks have to comprise a mix of manual and automated steps.

Peoples' expectations aren't always realistic

Peoples' expectations of how much automation is achievable aren't always realistic, though. The reality is that even some of the most automated playbooks have to compromise a mix of manual and automated steps. There are aspects of playbook automation at the abstract or logical level of creating and updating them that are often misunderstood. One of the value propositions of many security automation tools is that they enable the creation and updating of playbooks at an abstract level to be automated via software. For example, a Security Orchestration Automation and Response (SOAR) platform can serve up a nice GUI so that a security analyst can indeed observe a deviation in a known attack playbook and update their own security playbook in minutes.

What isn't well enough understood about this example, though, is that a playbook that is put to work by an organization in software in a SOAR or other platform didn't get there without a lot of painstaking process documentation work to ensure that it maps exactly to the organization's own environment. In some cases, that playbook may have started its life being input into Word, Excel or another format as a written playbook months or years earlier, perhaps before automation was even an option. To make it into operational software that playbook may have had to be translated from its original text-based format and ingested into a vendor's platform to make it capable of supporting automated changes. It's only at a fairly mature stage of playbook-driven security that new playbooks can be spun up and deployed though software in minutes.

Figure 4: The value of automation to achieving a high level of cyber resilience



Source: The Ponemon Institute, 4th Annual Study on The Cyber Resilience Organization 2019

Some organizations have therefore misunderstood what playbook automation at this logical or abstract level actually means in practice. Some have assumed that the time-consuming process of figuring out what their specific security playbooks need to look like could be magically automated or even bypassed altogether. This is not the case.

The learning here is that mature organizations that already have documented playbooks of some kind can see a rapid ROI by investing in security automation tools. For organizations that don't, the main value of SOAR platforms in the first instance is often helping them realize that they need to invest time in determining the basics of which playbooks they need and what they should look like - and that there can be no effective security automation without initial process documentation. Building from a foundation of playbooks can also be very helpful in helping organizations review and optimize their end to end security architecture as a whole, as well as some of the individual vendor components within it.

There can be no effective security automation without initial process documentation.

Automation of Defensive and IR Playbooks is a very different thing.

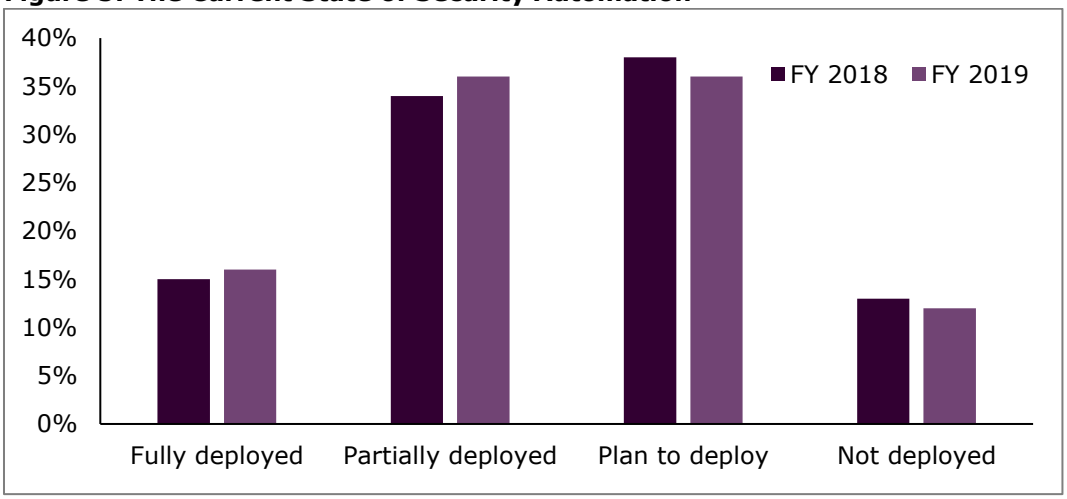
The second way in which the reality of playbook automation can be obscured is by failing to distinguish correctly between the scope for automation in the case of different types of playbook. To put it simply, automating what this paper has defined as Defensive playbooks is a lot easier than automating IR playbooks.

This is because automated steps in Defensive playbooks are characterized by responses to known threats or carrying out routine procedures solely within the IT security domain in which machines are interacting with one another and with security analysts. Nailing down in a playbook which routines should be run and when and automating the execution of certain actions by machines at a given point in a response – often in a complex multi-vendor environment – is where significant time-saving gains can be made through Defensive playbook automation.

Automating steps in IR playbooks is a lot more challenging. In the first place, an 'incident' is typically defined as something that isn't yet understood, which immediately reduces the scope for automating responses. Many IR playbooks also reach beyond the confines of the SOC or other IT security environment to introduce people into the workflow from across different departments in an organization like finance, marketing, HR and legal.

This is because critical decisions that contribute to containing or remediating an incident have to be taken with regard to requirements like reporting the incident to regulators; notifying law enforcement; and providing status updates or guidance to different stakeholders ranging from customers to investors, employees and the media.

Figure 5: The Current State of Security Automation



Source: Ponemon Institute "Cost of a Data Breach Report 2019"

An IR playbook tends to focus more on pre-defining the procedural protocol for how an organization responds. How quickly and effectively IR playbooks can run to completion tends to be more dependent on the quality of playbook training given to the human beings that are the designated decision-makers. The quality of contextual information served up to them at points where a decision is required of them also tends to be more relevant to response efficacy than the potential for a machine taking an automated decision in that person's place.

Many stakeholders in IR playbooks aren't security professionals

Moreover, whereas the choice of whether or not to automate in a Defensive Playbook context is fundamentally a choice between assigning decision-making responsibility to a security tool or a trained security analyst, many of the individuals assigned roles in IR playbooks are not security professionals. There is certainly scope for automation of individual steps in IR playbooks. An example is the automated triggering of calendarized conference calls for nominated decision-makers at a given point in the playbook, taking into account each individual's relative importance to the decision and their availability. However, the scope is clearly a lot less and will remain so, for at least the medium term.

Complexity is a major barrier to effective playbook driven security with a high level of automation.

Whilst an IR playbook to remediate the exact same threat may have common components from one organization to the next, some level of customization is invariably needed to reflect differences in organizational structure across industry sectors, or even within the same sector. Another aspect of distinguishing between what can reasonably be expected by way of automation of different types of playbook is understanding the hand-off between one and the other. The precise circumstances in which a day-to-day Defensive Playbook should not execute because of ambiguity and should therefore hand off to an IR playbook need to be very clearly defined.

Technology Barriers to Playbook Automation

Building on a foundation of a strong commitment to process documentation, identifying and operationalizing those specific steps in each of its playbooks that can be automated with confidence falls to the user organization. How well each one does it depends on how effectively it exploits available security automation and orchestration tools, as well as inputs it takes from professional services and managed services partners.

The technology core for enabling security playbooks to be automated is driven by the mature Security Incident and Event Management (SIEM), the emerging Security Orchestration Automation and Response (SOAR) and related product spaces. The SIEM essentially aggregates available alerts, handling the response to only a very small subset of the most basic ones.

The SOAR pulls information and orchestrates automated responses across diverse, multi-vendor infrastructures. As such, it allows playbooks to be extensible across multiple vendor tools by providing abstract functions for enabling access to each of them, querying them, and allowing information to be analysed across them. This enables different manual or automated steps in the playbook to be orchestrated.

Complexity - a major barrier to Playbook Automation

This paper has already identified the human constraints on organizations adopting a more playbook-driven approach which, in turn, serve to hold organizations back from automating security operations. The next section considers some of the technology constraints that stakeholders should be addressing to make it easier to automate security playbooks. This matters because complexity is a major barrier to effective playbook-driven security with a high level of automation.

The following are candidate ideas for what can be done to simplify complex multi-vendor environments and make it easier for security playbooks to run to completion faster.

1. A standard data model for describing security playbooks.

The statement was made earlier that no common natural language exists for describing cyber security playbooks. There isn't a data model for this either. Today, if two vendors want to share a playbook that plots defensive moves they have to re-write them in their own code. Widely used common specifications exist for attack playbooks in the ATT&CK Framework. They exist for threat intelligence sharing in the form of Structured Threat Information eXpression (STIX) and Trusted Automated exchange of Indicator Information (TAXII). The equivalent for security playbooks is needed too.

2. Orchestration workflow standards for better playbook portability

The way that a playbook defines a workflow today is proprietary. This creates friction whenever cyber security stakeholders want to port a playbook from one environment to another. This can be alleviated via the adoption of a workflow orchestration standard for security playbooks. Business Process Model and Notation (BPMN) is widely used outside the security world and is also used by a number of leading security vendors, including in the key SOAR space. It seems like an obvious candidate.

In August this year, the OpenC2 Forum approved the first specifications of the Open C2 standard.

3. Better incentives to augment threat intel and automate sharing

The faster that security playbooks can be updated with new threat intelligence, the faster they can run to completion to block, contain or eradicate threats. A barrier to this is that many user organizations fear that enriching shared threat intelligence or automating the sharing of it risks sensitive information about their own organizations being disclosed. This is because it can often be hard to determine whether all the features of an attack that they have been subjected to are necessarily the exact same as those that other victims have been subjected to. Many users therefore err on the side of sharing too little information rather than too much. In the process they can fail to share information that might help accelerate playbook execution in other environments. There are three areas to look to for improvements. The first is better tool accuracy. The second is further work and communication around the anonymization features of STIX and TAXII. The third is via Information Sharing and Analysis Centres (ISACs). Examples are T-ISAC which serves the telecom sector and FS-ISAC which serves the financial services industry.

4. More and deeper integrations between large vendors

The large-scale integration partnerships announced in the last couple of years by IBM Security and Cisco as well as by Fortinet and Symantec have potential to accelerate the operational efficacy of playbook automation. Multi-vendor security environments are extraordinarily dynamic in terms of the volume of updates of different vendor products that are underway almost constantly. Deeper, portfolio-wide, integrations between the largest vendors can reduce the risk of a single missed update or unforeseen configuration change delaying a security playbook's progress through to completion.

5. A standard Command & Control interface for security operations

To effect an orchestrated response to a security incident the security team typically needs to know the syntax of each different product that's involved in the response; go to a web based application; and use an API or connect remotely to input commands. In August this year, the Open C2 Forum – part of OASIS – approved the first specifications of the OpenC2 standard. By commoditizing the command and control interface, Open C2 is designed to empower security teams to automate security playbooks more reliably and faster. For now, OpenC2 is a user-driven standard, pushed primarily by Bank of America, AT&T and the US National Security Agency (NSA). The outlook for large scale commercial adoption of OpenC2 is unclear at this time. With large scale adoption, it has potential to improve time-to-completion of cyber security playbooks.

Managed Playbooks As A Service

It ought be clear from this White Paper that while adoption of cyber security playbooks is becoming more popular, at this point in time those that use them still represent a minority elite among the world's cyber security professionals. That begs the question of how to accelerate adoption across the majority of organizations that don't use them.

The recent emergence of a new service category of Managed Detection and Response (MDR) services provides a seque into the answer. A core part of many of these companies' business models is the creation, operation and maintenance of security playbooks, especially in real time and in response to emerging situations.

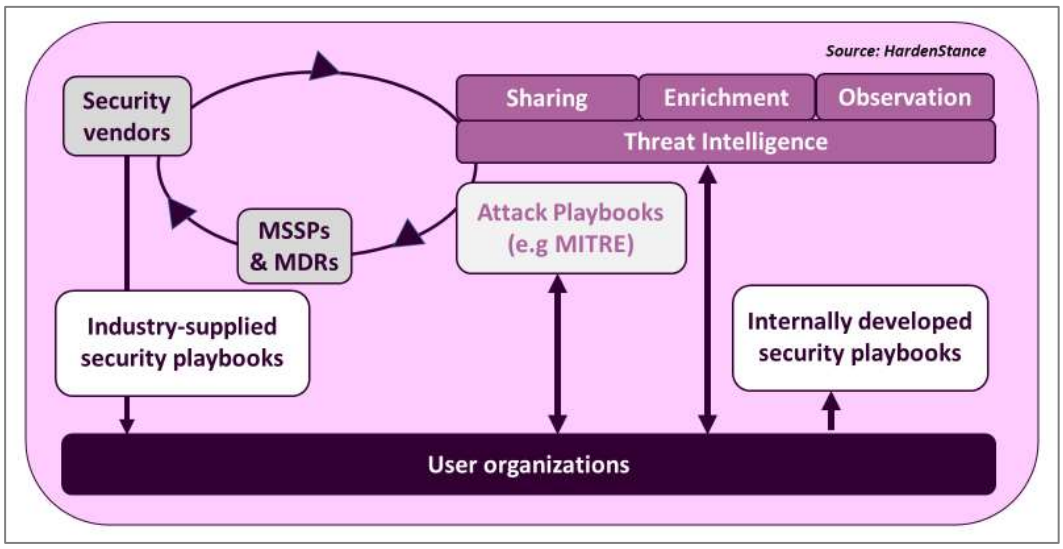
There is clearly a large opportunity here for Managed Security Service Providers (MSSPs); management consultancies like the 'Big Four' accounting firms; as well as pure-play MDR providers to grow substantial revenues in managed playbook services. In its most simple form, security-focused management consulting has a substantial role to play in helping businesses navigate the foundational cultural and organziational challenges involved in making the initial commitment to playbook-driven security and the setting of related initial goals. The opportunity for MDR providers is at the operational end while, depending on their business model, MSSPs can potentially target a managed playbook offering across the value chain.

Playbook management services should be an increasingly important area for providers of managed security services.

Linking playbook adoption to the Capability Maturity Model

One can even see how the level of playbook adoption can be extended to the well-established Security Capability Maturity Model. This provides organizations with a means of benchmarking the maturity of their cyber security posture against five levels of process maturity. This spans a basic level , in which cyber security posture is ad hoc and undocumented, all the way to an advanced Level 5. At Level 5, an organization's security posture is optimized and subject to continuous improvement with a high level of automation. It's inevitable that somewhere along the industry adoption curve – more likely sooner than later – many user organizations that buy into the case for a more playbook-driven approach will come up against the limitations of their own organization in being able to operationalize it.

Figure 6: Sourcing of Security Playbooks



At the outset of identifying the right playbooks to create, it's true that there is a rich variety of generic ones to build from. The necessary skills for companies to leverage these as well as customize them to their own environment are in short supply, though. This is especially true when it comes to closing the loop to maintain and update an organization's playbooks with the latest threat intelligence once the playbooks are in operation, according to the MDR model. Although openly available resources like ATT&CK do democratize access to adversary playbooks, most organizations will still struggle to compete with managed providers when it comes to creating, managing and implementing a security playbook response.

Managed providers don't just have the advantage of specialization and scalability. They also have the advantage of implementing playbook operations across multiple customers, including in some cases many customers in the same sector. This is yielding experience and capabilities that individual organizations will struggle to match. For at least as long as the human and technology barriers to playbook-driven security raised in this paper remain in place, managed providers will tend to be very much better equipped to navigate them than most organizations acting on their own. ■

About The Sponsors

About IBM Security

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, provides security solutions to help organizations stop threats, prove compliance, and grow securely. IBM operates one of the broadest and deepest security research, development and delivery organizations. It monitors more than two trillion events per month in more than 130 countries and holds over 3,000 security patents. To learn more, visit www.ibm.com/security

About KPN

KPN is the leading telecommunications and information & communications technology (ICT) service provider in the Netherlands. KPN offers a broad portfolio of services to the business (SoHo, SME, large & corporate enterprise), consumer and wholesale market, varying from fixed and mobile telephony, fixed and mobile internet, and TV to a wide range of ICT services, such as cloud, workspace, internet of things and security. KPN is passionate about offering secure, reliable and future-proof networks and services, enabling people to be connected anytime, anywhere, whilst at the same time creating a prosperous and more sustainable world. To learn more visit www.kpn.com

About Nokia

We create the technology to connect the world. We develop and deliver the industry's only end-to-end portfolio of network equipment, software, services and licensing that is available globally. Our customers include communications service providers whose combined networks support 6.1 billion subscriptions, as well as enterprises in the private and public sector that use our network portfolio to increase productivity and enrich lives.

Through our research teams, including the world-renowned Nokia Bell Labs, we are leading the world to adopt end-to-end 5G networks that are faster, more secure and capable of revolutionizing lives, economies and societies. Nokia adheres to the highest ethical business standards as we create technology with social purpose, quality and integrity. To learn more visit www.nokia.com

(see also next page)

About Cyber Threat Alliance

The Cyber Threat Alliance (CTA) is a not-for-profit, U.S. based organization that improves the cybersecurity of the global digital ecosystem by enabling near real-time, high-quality cyber threat information sharing among companies and organizations in the cybersecurity field. With over 20 members based in 8 different countries and with global reach, we seek to protect end-users, disrupt malicious actors, and elevate overall security for everyone.

Members use our automated platform to share, validate, and deploy actionable threat intelligence to their customers in near-real time. They share research findings and priorities with each other at human speed as well. Based on our shared intelligence, CTA and its members create outputs, collaborate on actions, and respond to cyber incidents to reduce the overall effectiveness of malicious actors' tools and infrastructure. Finally, CTA shares content, establishes partnerships, and promotes policies that enhance the overall security and resilience of the digital ecosystem. To learn more visit www.cyberthreatalliance.org

About HardenStance

HardenStance provides trusted research, analysis and insight in IT and telecom security. HardenStance is a well-known voice in telecom and enterprise security, a leader in custom cyber security research, and a leading publisher of cyber security reports and White Papers. HardenStance is also a strong advocate of industry collaboration in cyber security. HardenStance openly supports the work of key industry associations, organizations and SDOs including NetSecOPEN, AMTSO, The Cyber Threat Alliance, The GSM Association, ETSI and TM Forum. To learn more visit www.hardenstance.com