BROADBAND TESTING

Swimlane: Low Code Security Automation Report

A Broadband-Testing Report

First published February 2022 (V1.1)

Published by Broadband-Testing

E-mail : info@broadband-testing.co.uk
Internet: HTTP://www.broadband-testing.co.uk

TABLE OF CONTENTS

BROADBAND-TESTING

Broadband-Testing is an independent testing operation, based in Europe. Broadband-Testing interacts directly with the vendor, media, analyst, consultancy and investment communities equally and is therefore in a unique space within IT.

Testing covers all aspects of a product/service from business rationalisation in the first instance to every element – from speed of deployment and ease of use/management, through to performance and accuracy.

Testing itself takes many forms, from providing due diligence for potential investors through to public domain test reports.

Broadband-Testing is completely vendor neutral and independent. If a product does what it says on the tin, then we say so. If it doesn't, we don't tell the world it does what it cannot do… The testing is wholly complementary to analyst-related reports; think of it as analysts getting their hands dirty by actually testing what's on the latest hype curve to make sure it delivers on its claims and potential.

Broadband-Testing operates an **Approvals** scheme which prioritises products to be short-listed for purchase by end-users, based on their successful approval, and thereby short-cutting the evaluation process.

Output from the testing, including detailed research reports, articles and white papers on the latest IT technologies, are made available free of charge on our web site at HTTP://www.broadband-testing.co.uk

EXECUTIVE SUMMARY

- In all aspects of IT, automation has been on the agenda for decades, but regardless of the deployment scenario, it has largely failed to hit the mark. One of the problems has always been the complexity involved, regardless of the development of Artificial Intelligence (AI) and Machine-Learning (ML).

- In the context of security, automating and orchestrating a security strategy has to be absolutely comprehensive and watertight. Nothing is more dangerous within an IT infrastructure than a mis-configured and/or mis-managed security deployment.

- Swimlane, with its low code automation principles, is addressing both of these fundamental issues in one fell swoop. Moreover, it is a true platform, independent of 3rd party products and services. This means it really can be used to fully automate and orchestrate a company's security infrastructure, including operations beyond the SOC. In both simplifying and expanding the world of security automation it really is looking to be a game changer. Anyone familiar with classic workflow principles can set up even relatively complex processes with zero requirement for any development skills.

- In addition to the low-code concept, in day-to-day use, the product is very visual and visibility oriented; we're not talking screens of endless integration code and no supporting documentation. Equally, we are talking easy to read dashboards, classic drill-down approaches to extracting more detail and a wide range of report and alerting options. So, nothing in the platform is alien, even to a relatively new recruit to the world of IT and security admin. This approach is designed to enable fast and accurate integration, true continuity and the benefits, therefore, of speed and ease of problem resolution – basically the mantra of IT security operations.

- While the use cases for Swimlane deployments are effectively endless, within this report we are looking at three commonly observed requirements and seeing just how the Swimlane technology addresses these decades-old issues – a multi-triage scenario based around SIEM (Security Information and Event Management) alerts, resolving a classic phishing attack and threat intelligence feed analysis.

- In each use case, Swimlane massively reduces the time to remediation, compared with a manual, or even semi-automated approach. Moreover, it also removes the possibility of human error, so the results are watertight. Nothing is left to chance.

AUTOMATION FINALLY MADE EASY?

No one ever said automation was easy.

Here at Broadband-Testing we've been examining automation solutions across many different aspects of IT for over 25 years; there have been some worthy efforts, some less so, but all in all, even the best can be summed up by the classic phrase: "close, but no cigar." At one time, too, there was always an undertone with respect to automation of "is it going to put humans out of a job?" – yet we now live in a world where there are severe shortages of qualified technicians; there simply aren't enough security staff to cover off all the bases and fill in the holes. Meantime, developments beyond our control, such as the global pandemic we've all been suffering through, resulting in an ever-increasingly dispersed and weakened – from a security attack surface perspective - workforce, mean automation is more important than ever. But that "close but no cigar" level of automation is not the answer. Within the world of IT security, getting it 100% right is not a "nice to have" – it's a fundamental requirement. Moreover, that automation has to be flexible and almost infinitely expandable in order to address the threat landscape; it is ever-changing, increasingly complex, and increasingly smart. People talk about fighting fire with fire – in this case it's all about being able to match the intelligence levels of the threat guys. That's not a situation resolved by endless meetings and procrastination, but by having an automated system in place that attempts to stay one step ahead and serve as a system of record for all aspects of security operations.

It also means there has to be an end to the SecOps "panic attack" methodologies for resolving zero-day attacks, the dark web, and every other "unknown" in the world of cyber security attacks. Networks may well have been built over the decades in the form of a Picasso take on technological plumbing – add a bit here, a bit there… but they need to be secured in a totally structured fashion. Humans are not great at this approach – that's why we have computers in the first place. And then there's the security spend this scatter gun approach generates; the likes of Gartner report that most companies only actually deploy around 20% of their security solution real estate at any one time; that's a huge waste of money and resources. Moreover, it still doesn't solve the problem in the first place. It doesn't help that, each year, literally thousands of security start-ups tell you that their new gizmo is the latest "must have," even if it's far from clear – and it often is – what that product or service actually brings to proceedings. Sometimes you even wonder if the vendors themselves actually know!

So, how about a radical concept – making your existing security investment actually work as a solution, not a trail of endless bit parts? In other words, how can you have a secure threat defence if every aspect of your security strategy isn't tightly integrated – full of holes and easily breached? Here is where automation comes to the fore – humans cannot respond and develop solutions quickly enough – so fight technology with technology. The problem is that automation – to date - hasn't been sufficiently thought through and developed in a true end-to-end fashion, yet automating only part of the security real estate simply creates more potential problems and gaping holes in the security fabric. We saw this with first-generation SOAR (Security Orchestration, Automation and Response) products; they resolved part of the problem but not ALL of it. That is not the answer…

Swimlane appears to have grasped that security automation needs to be a dedicated, company-wide (and beyond) security real-estate deployment and, at the same time, one

that removes the "human error element" that is responsible for around 85% of security holes - one that can respond in real-time (or pro-actively) and comes future-proofed. It's answer to the security automation dilemma comes in the form of what Swimlane calls a "low-code" approach to automation, making it accessible at virtually any level of security skillsets, while being rapid to deploy and effectively self-managing.

So, what exactly is low-code security automation? For starters, it is very use case driven – not a solution looking for a problem – and can be as simple as a drag 'n' drop data entry deployment. It has been designed to maintain inherent simplicity, regardless of the actual complexity of the use case itself. Use cases build into comprehensive libraries of automation and - yes – it's cloud-based, so it's easy to access from anywhere. The idea is that every element of integration can be achieved, being workflow and technology agnostic, hence the "organisation-wide" aspect and using the same features and functionality – it is a true platform, not a toolkit with a few vital spanners missing... It also means that the IT teams become more efficient, rather than continuing down the lines of panic recruitment – and the inevitable high turnover of staff that approach leads to, along with the turmoil it creates.

In this report we will highlight three use case examples of how the Swimlane solution can be deployed, but first a brief overview of what the company is offering.

PRODUCT OVERVIEW

So, what exactly do you get from Swimlane?

First – yes, it's a product, and it's deployment-agnostic accommodating on-premises, air-gapped, virtual, and cloud environments. Swimlane Cloud can be deployed in days, but regardless of deployment model the platform is designed to orchestrate and automate to serve as the system of record for your entire security posture. From an analyst pigeon-holing perspective, it is a SOAR platform specifically, but – as we've noted – far more advanced than the first wave of such products. In other words, it's a security automation platform designed to execute incident response tasks through two-way integration with a broad range of 3rd party security platforms – the aim being faster mean time to resolution and easier focus on key threats. It is designed to be completely flexible and adaptable to every company's security infrastructure, bearing in mind no two deployments are ever exactly the same, which also ticks the "future-proofing" box.

A quick glance at the platform shows it to be very visual and visibility oriented; we're not talking screens of endless integration code and no support documentation. This approach can enable fast and accurate integration, true continuity and the benefits, therefore, of speed and ease of problem resolution. The aforementioned fundamental approach of low code automation ties in with this "speed and simplicity" approach, encompassing both automation and orchestration – so it automates the binding and management of the security deployment. Here, it's probably worth noting the difference between those two aspects, as often they seem to be cross-referenced:

Security Orchestration: The integration of disparate security tools and platforms to enable automated incident response.

Security Automation: The ability to execute a sequence of tasks related to a security workflow without human intervention.

Day-to-day use revolves around building out those low-code processes to identify all the possible security scenarios and automate the management of them. The latter comes from a classic combination of dashboards, alerts and – vitally – behind the scenes automation of what would otherwise be human-assignable tasks with the obvious delays and inevitable errors that approach has always generated. Within any element of IT, these are costly and undesirable, but within a security context they can be a business killer. And, as we've already noted, that "human element" is increasingly hard to find in the first place; an estimated 3.5m cyber security job openings were there to be filled in 2021, while an Ernst and Young report cited 53% of companies surveyed admitting they had a lack of skilled security resources.

Importantly, Swimlane is also flexible in terms of having many different methods of bringing data into the platform; again, no two companies are the same in this respect. Once that data is stored, the basic approach is to build out a series of workflows that dictate all the possible scenarios – kind of a latter-day take on a classic "if-then-else" dev approach. Here is where interaction with 3rd party security tools is fundamental to the Swimlane approach – typically via a plug-in or integration. Here is also where the level of automation can be defined, from basically full automation to primarily manual (the latter might still be required for legal and conformance reasons in some cases – or simply company practise). Multiple dashboard options manage that data interaction, from basic overviews to detailed drill-down capabilities, with a wide range of reporting options available at the end of the chain.

So much for this overview - the best way to understand Swimlane is to add some context to the product definition, so here are three common use cases we worked through, showing the product in action, first in terms of an SIEM-related alert triage, secondly in the event of a phishing attack, and finally in the case of threat intelligence analysis.

SWIMLANE: USE CASES

SIEM Alert Triage

We've already mentioned the importance of 3rd party integration within the Swimlane platform.

This use case demonstrates the automated triage of data provided from a range of tools, including Elastic Security, with automated actions via McAfee ePO, Tufin, Recorded Future and Palo Alto Networks Firewall integrations. Our use case starts with the condition that an alert has been received from Elastic Security and is automatically entered into a Swimlane record. When the alert is received, Swimlane carries out a first set of actions to begin the triage of the alert, opening up the respective parts of the form that apply to this incident. This means admin personnel reviewing the data will automatically be able to see the corresponding fields and their content. By querying Elastic Security, Swimlane pulls in the underlying logs that triggered the alert.

This initial data is supplemented by retrieving all of the related host details from McAfee ePO and Tufin, so the picture begins to become both clearer and more detailed. Rulesets related to the IP addresses in the alert are gathered and added to the record, as is a network topology diagram that can provide additional context to anyone reviewing or analysing the record. Finally, in this series of actions, Swimlane searches Recorded Future for information on the indicators present to determine whether or not the incident is actually malicious.

Figure 1 – KPIs & Metrics Dashboard showing ROI, MTTR etc based on Swimlane's actions

The defined workflow then automatically branches to a new set of conditions to analyse the results of the data gathered.

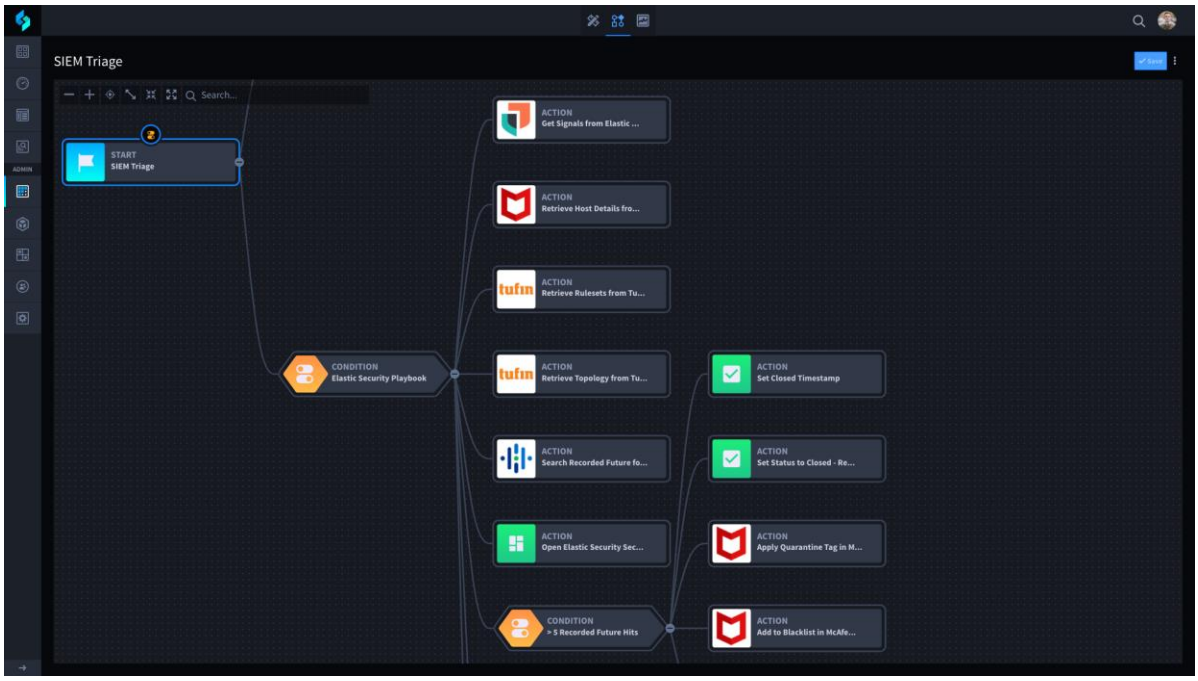

Figure 2 – Swimlane Workflow For SIEM Alert Threat Analysis

In this instance, if there are more than five Recorded Future hits, Swimlane will consider the event malicious and begin executing relevant remediation actions, timestamping the record. It quarantines the host using McAfee ePO, adds all the associated URLs to a blacklist in the McAfee Web Gateway, blocks the related IP addresses in a Palo Alto Networks firewall and then marks the record as closed. Note – all of this is done automatically, with no human interaction required. Think of the timed saved, as well as the accuracy of the analysis. If, however, the automated analysis indicates the event is not malicious, Swimlane simply closes the event and record by setting a closed timestamp and changing the status to closed.

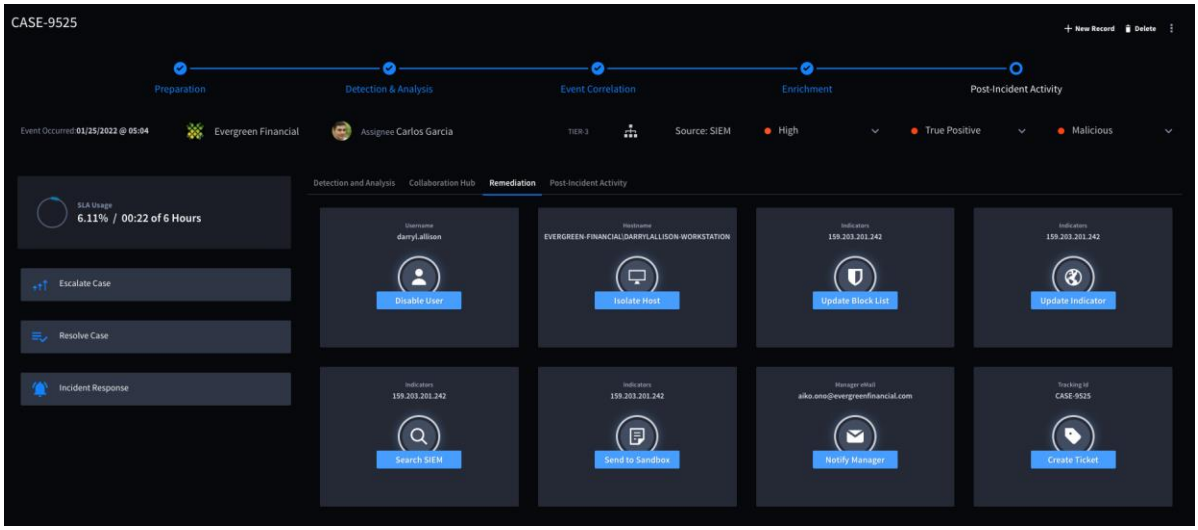

Figure 3 – Swimlane Remediation Tab Options For SIEM Use Case

The third possibility here is that the analysis does not clearly determine the event to be either malicious or safe, in which case the record will be left open for an analyst to review, the case is automatically escalated to Tier II and the status is changed to open investigation. The assigned analyst is notified of the case and is fed the appropriate dashboard information – all available from a single viewpoint, and with all the automated actions and detailing (enrichment) already done. So, the analyst simply has to review the information via a series of onscreen tabs and determine the outcome. In this instance, the relevant log data from Elastic Security is parsed out and presented onscreen in the relevant fields.

The enrichment tab is used to display the data integrated from Tufin - rulesets related to the IP addresses in the alert and a topology diagram is automatically downloaded to give a visual representation of how any blocking activities might affect the rest of the network. The next tab displays the information Swimlane received from the Recorded Future IP report, such as the risk score and criticality for that suspicious IP address. The ePO host details are provided on a third tab, where Swimlane has automatically obtained all of the information about that endpoint. In the event of the analyst declaring the alert to be malicious they can then use the remediation tab to carry out the same steps as the automated example. The analyst can then close this investigation. Note, all of this information is also gathered at a macro level and used to display various performance metrics in a customised dashboard interface.

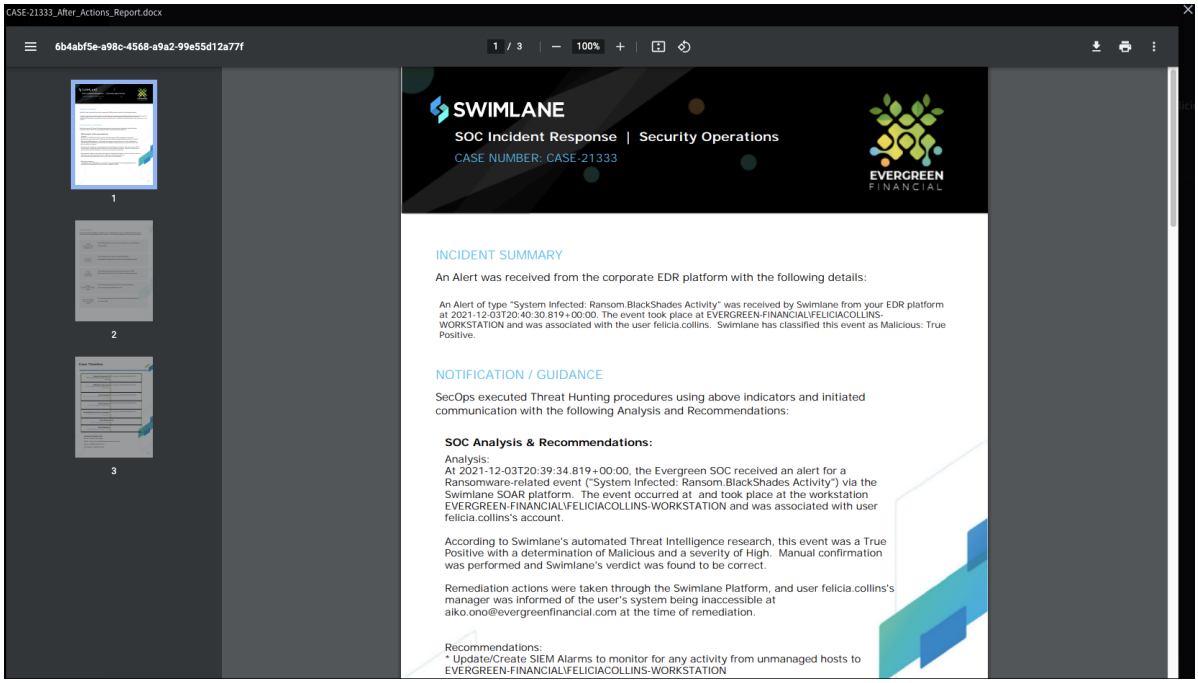

Figure 4 – Swimlane SOC Incident Report

Phishing Alert

Our second example is a common phishing alert. Again, it involves integrations with a number of 3rd party tools – in this case McAfee ATD, Lastline and VMware Carbon Black.

Our use case begins with a suspicious email received in a monitored mailbox, which triggers a series of actions from Swimlane, parsing the suspicious email and automatically filling in applicable fields with content from the email, such as email addresses, headers, attachments and URLs. Our workflow in this instance has a basic condition: Is there an attachment? If there is, Swimlane submits the attachment data to Lastline and McAfee ATD. Both of these are sandbox environments where the attachment will be detonated and automatically analysed, to determine whether or not it is malicious. Again, no human intervention is required here.

This sandbox analysis is used to determine which path to take through the defined workflow. So, if the results indicate a malicious attachment, Swimlane automatically executes a series of remediation actions, using the VMware Carbon Black integration to isolate the host and block the corresponding hashes found. Importantly, VMware Carbon Black will also be used to search out those hashes to see if they are found on any other hosts in the environment. Nothing is left to chance. If other hosts are found with those hashes, Swimlane uses VMware Carbon Black to automatically isolate the additional hosts. At this point, the incident is closed by removing the email from the mailbox, and changing the record status and time-stamping it. Should, however, the sandbox analysis determine that the attachment was safe, the user is automatically notified that the submitted email is safe and the status changes to closed, defined as a false positive, again with a closed time-stamp.

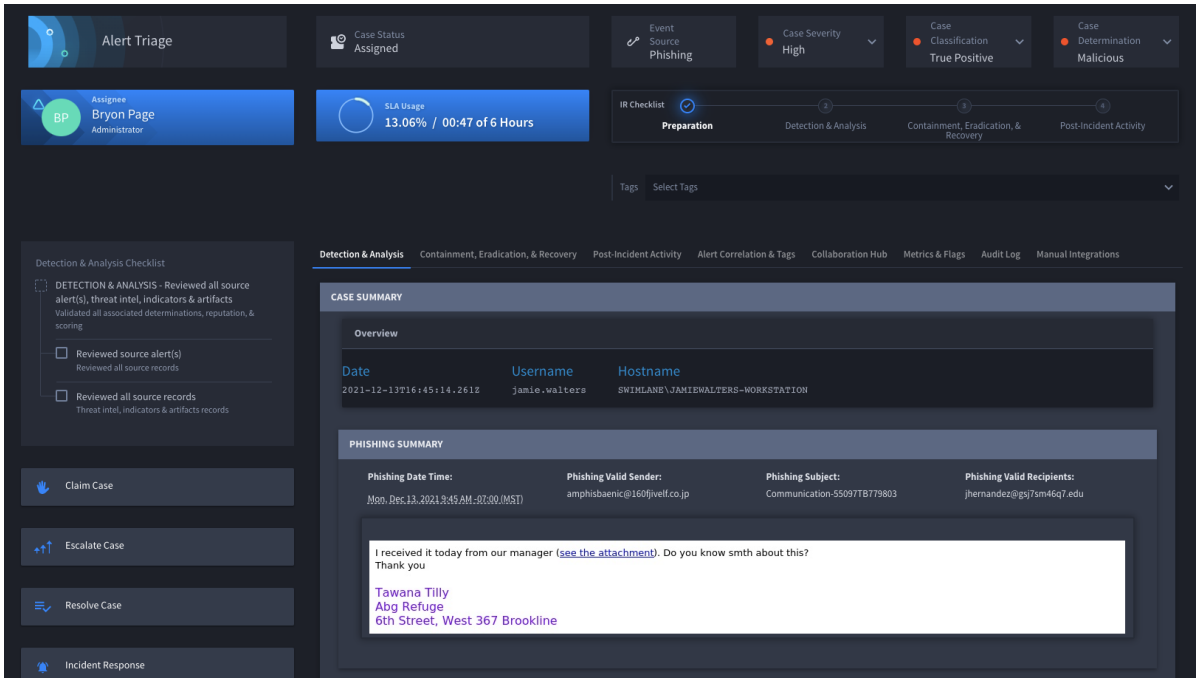

Figure 5 – Swimlane Detection And Analysis Tab: Widgets Of Status And Progress

Again, in either instance, the remediation was fully automated. But if the sandbox analysis proves inconclusive, the incident is partially automated and left open for an analyst to review. On this path, VMware Carbon Black is still automatically called up to scan the network and see if any other hosts contain the hashes found during the sandbox evaluation. This speeds up manual evaluation by ensuring the analyst has all the additional information readily available as they open the record. The record is automatically escalated to Tier II and the status is set to Open Investigation and the assigned analyst is notified they have a record to review.

In this instance, all the automated actions and enrichment have already been done and the analyst simply needs to review the information and make a decision. Swimlane, as before, displays all the submitted email information including a safe view of the HTML body, URLs and domains found in the email, attachments, and hashes of the attachments. The latter are evaluated using McAfee ATD and Lastline and VMware Carbon Black is once more employed to see if the hashes are found on any other host. In this use case, any host count confirms there are additional hosts in the environment that contain the suspicious hashes. The analyst can now determine whether this is malicious or not and use the remediation integrations to protect the environment.

If malicious, the analyst can use a simple two-button process to have Swimlane use VMware Carbon Black automatically isolate the hosts where the hashes were identified, and block the hashes. The analyst can then close the record. Again, all the information is gathered to display various performance metrics at the management dashboard, which is completely customisable.

Threat Intelligence Analysis

Our final use case revolves around the common procedure of using threat intelligence reports, such as tactics, techniques, and procedures – TTPs - and indicators of compromise – IOCs - to detect and mitigate threats proactively.

If done manually, this can be an incredibly time-consuming process, especially when it involves several steps across multiple disparate systems. Instead, Swimlane integrates the toolset and auto executes research queries and other threat hunting techniques at machine speed. Not only does this massively accelerate the process but it enables the analyst to immediately see all relevant threat data and execute the correct response, drastically reducing resolution time, not simply the research time. The Swimlane workflow methodology allows you to automate as many evaluation decisions as you want, meaning an analyst can quickly focus on the highest priority threats.

In order to appreciate the benefits of using Swimlane, the easiest method here is to compare the classic "without" then "with" Swimlane in situ. Starting with the manual process, an analyst typically kicks off the analysis by using common tools such as an RSS reader, threat intelligence feeds, and research blogs – to manually collect IOCs and look for any new TTPs being employed. As a result, the analyst might notice – for example - that an MD5 hash has emerged as a second stage indicator of a trojan infection. To verify that the IOC is a valid threat to hunt, the analyst would open additional browser tabs and perform a series of further research queries, based on the severity rating found in some of those queries, and then hunts for the MD5 hash. This means logging into a SIEM and other tools and – in each case – running a series of queries for the suspect MD5 hash. In our use case, the analyst finds seven matches. In turn, they will document the matches and prepare an incident report, typically by copying and pasting the host details and other relevant information into those reports – both time-consuming and repetitive. Once complete, those incidents will be submitted for approval and, post-approval, the impacted parties are notified and the case is closed – a process that could easily take several hours.

Enter Swimlane – the analyst logs in and is immediately presented with the indicators that Swimlane has auto-ingested from the RSS, threat intelligence feeds and relevant research blogs. This means they can focus on the intelligence that has been verified to be malicious, meaning they instantly see that a specific MD5 hash has been identified as a second stage indicator of a trojan infection, having been automatically verified by Swimlane using a Recorded Future API query. At this point, the analyst doesn't really need to perform additional research on this indicator, given how high – in this case - the Recorded Future risk score and risk criticality is. Should they wish to gather further intelligence, they can simply perform a one-click search on a number of research links provided, such as Google, Recorded Future, Bing or ThreatMiner – these are Swimlane pre-filled searches customised for these resources. What was that old line about "information at your fingertips!?

Should the analyst decide to perform a threat hunt and determine if this indicator has been identified in their environment, they simply click on the threat hunting tab, verify that no threat hunts exist yet and click [Go Hunting]. This generates a new threat hunting record in Swimlane. The new threat hunt record will contain a query that has been designed for the appropriate platform – in this case for VMware Carbon Black.

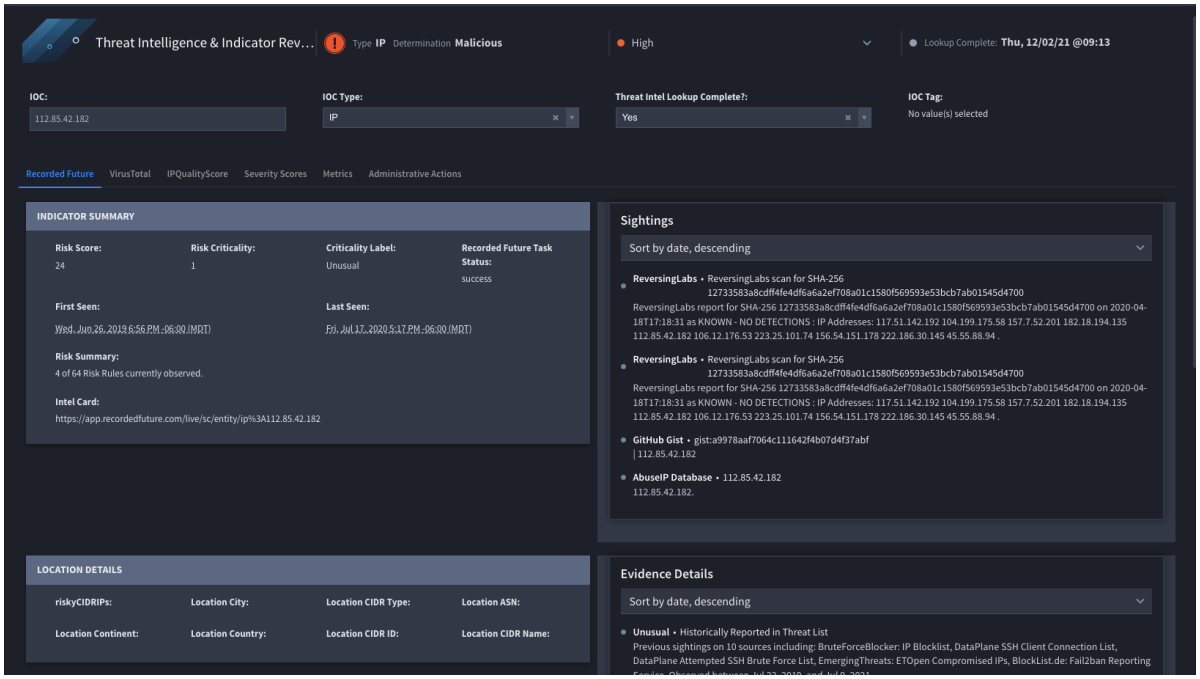

Figure 6 – Threat Intelligence Indicator Record

The custom query looks for this specific hash in the previous 14 days of records to identify whether or not this indicator has been seen in the environment during that period. Returning the query results in our example, Swimlane informs the analyst that there are seven hits for the query. At this point, they can view the raw results by clicking for more details, or simply click [Generate Report] to create the appropriate report. Again, all the information is gathered automatically, such as the query itself, the date scanned, the event ID, affected hosts, affected users, file names, PIDs, execution times, matching processes and hashes, and used to populate the report.

In this use case, the severity is determined by the number of individual hosts affected, with Swimlane showing the first and last positive hits and the subject matter of the searches, as well as detailed information on the individual hits. At this point, the analyst simply needs to review the report, make any modifications they deem necessary, and then click [Submit Incident Report]. The incident report is submitted to a supervisor and the case is closed. More importantly, what would otherwise have taken several hours of manual effort is completed in a matter of minutes and accuracy is guaranteed. That is what automation and orchestration is all about in practice.

IN CONCLUSION

IT security strategies have never been harder or more complex to deploy and manage.

The threat rate increases daily, as does the intelligence factor of those threats. It means that "old school" manual methodologies for securing a company's network, data and applications – whatever the topology - are simply no longer applicable; the human element alone is insufficient, and increasingly harder to find in the first place.

With its independent, platform-based approach to automating and orchestrating the security infrastructure, Swimlane really has hit the proverbial nail on the head. It's low-code automation principles mean that no new science is required in order to make the security infrastructure water-tight and human error-free. It also means that the vital time to resolution is massively reduced. And, as the threat landscape expands and changes, so the Swimlane platform, with its open integration approach, is able to match that shape-changing and ever-increasing level of intelligence.

In relative terms, in might still be early days for Swimlane, but it really has the principles of automation absolutely right, and in that sense, it is a game-changer. Long live automation…

.