glassCanopy

Marketing Cybersecurity: **eBook Samples**

Our Philosophy

At glassCanopy – we love eBooks.

They make ideal "bait" when trolling for top-of-funnel leads and create a great first impression for your brand – they also provide valuable collateral for your sales force. What's more, eBooks can be easily chopped into SEO-optimized blog posts and provide the context needed to quickly create videos, datasheets, case studies, and other collateral.

However, to be effective, the research, writing, and overall quality of the eBooks must be top-notch. Nobody feels good about giving out their contact information in exchange for a thinly disguised sales brochure.

Many of our clients felt that no one outside their organization could write an ebook that wouldn't come off as just marketing fluff. That was **before** they started working with glassCanopy. Quarter after quarter, we produce in-depth eBooks on technical and complicated subjects that our clients (and *their* clients and customers) love.

Here's a taste of what we can do...

TABLE OF CONTENTS

API AND CLOUD INTEGRATION VULNERABILITIES

Standards-based APIs and similar technologies make the cloud an excellent environment for flexible, fast, and economical integrations. However, the very openness that makes all this connectivity possible also creates new risk exposure.

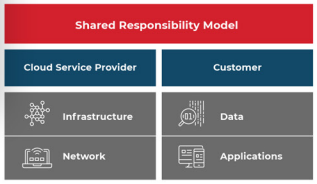
In addition to attacking APIs, hackers can target connection points like Azure's Event Hub or data integration services like Amazon Redshift data warehouse. These attacks can be particularly devastating since so much information flows through these access points. What's more, the information flow often doesn't look incongruous, so these attacks can go undetected for very long periods.

7

HE IMPACT OF THE SHARED RESPONSIBILITY SECURITY MODEL

ud customers work within the shared responsibility security model.

e CSP is responsible for securing its infrastructure and network. Their SecOps team onitors the compute, storage, and network hardware comprising the cloud platform. e customer, in turn, is responsible for their own data and application security, including e patching and access control issues that arise with working in the cloud.



This shared responsibility model makes a great deal of sense. The CSP cannot be expected to know which users are authorized to use the software installed in the customer's cloud. Nor is it realistic for the CSP to remember the specifics of how the customer wants to secure its data and applications.

However, the shared responsibility model leads to a lot of problems too. At a minimum, the cloud becomes yet *another* digital asset SecOps has to monitor by installing cloud-based versions of on-premise SIEM systems, Intrusion Detection Systems (IDSs), and other security tools.

8

ACCESS CONTROL ISSUES IN THE CLOUD

Who accessed what? That's one of the most critical questions facing SecOps teams as they analyze session logs and reports.

Deciphering the access control map becomes more complicated in the cloud. Users may get in using a "side door" by accessing digital assets remotely without having to pass through the corporate network. Cloud Access Security Brokers (CASBs) can help – as can identity access systems that have been set up for cloud use.

Using cloud deployments can inadvertently set up side-door access to critical data and systems.

ADDITIONAL COMPLEXITY AND GAPS CAUSED BY HYBRID AND MULTI-CLOUD ARCHITECTURES

Few organizations are one hundred percent in the public cloud. Many businesses have data across on-premise, public, *and* private cloud architectures. Others have applications and data that span AWS, Azure, and Google cloud. Such hybrid cloud architecture sets up a tricky security dynamic for SecOps to track by requiring many overlapping and repetitive systems for multiple cloud instances...further increasing the possibilities for human error and the need for automation.

11

NEXT-GEN MDR IN ACTION

A Next-Gen MDR platform should be able to provide the detection and response service timeline depicted in the "Left-of-Hack" and "Right-of-Hack" diagram in Figure 1. The figure offers a useful way to visualize the timing of threat detection and response actions. Each of the six steps within this workflow represents processes occurring along the timeline of an attack. The "Left-of-Hack" portion includes the proactive steps taken to detect threats before they occur. The earliest form of detection is threat anticipation, followed by threat hunting, which happens closer to the time of a hack, while security monitoring serves as the detection capability occurring up to the moment of a possible compromise.

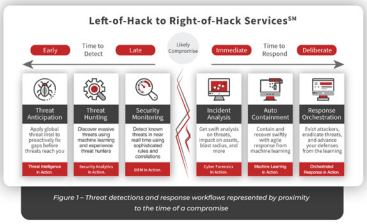
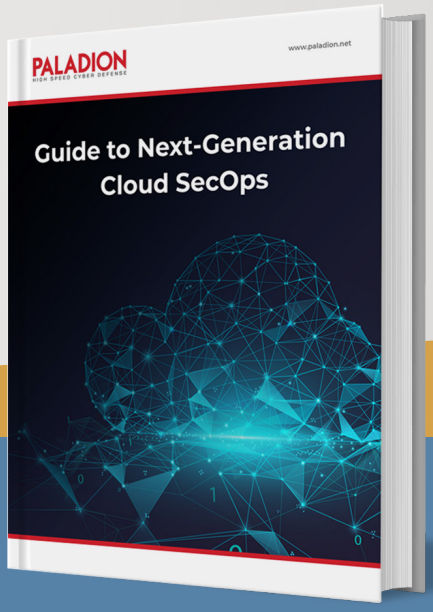


Figure 1 – Threat detections and response workflows represented by proximity to the time of a compromise

The "Right-of-Hack" includes the time-to-respond workflows, which follow a similar time-based pattern. The incident analysis takes place immediately after an attack, followed by auto-containment, and then response orchestration.

A robust MDR solution includes both pre- and post-attack activities.

16

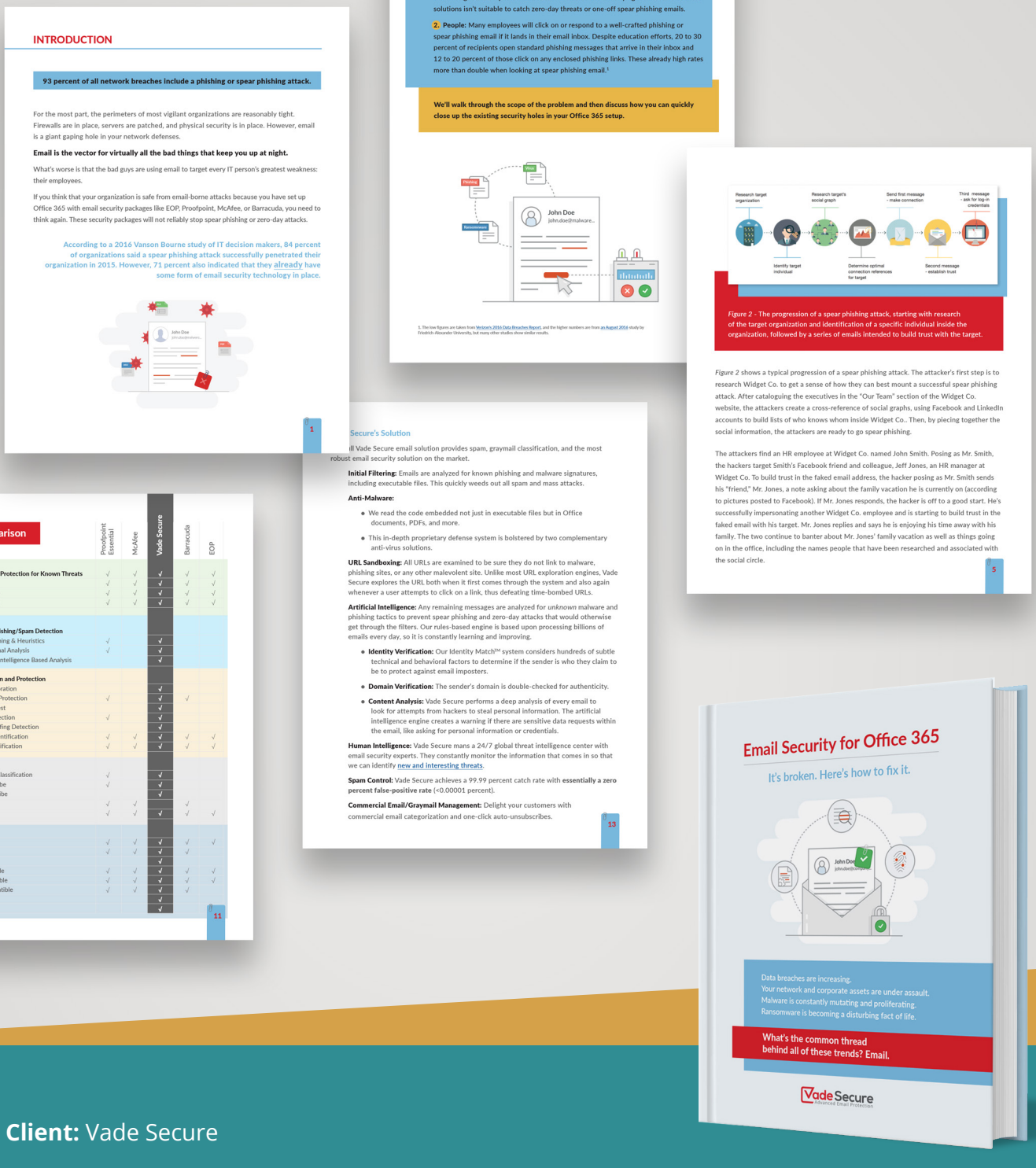


Client: Paladion

What they do: Next-gen managed detection and response (MDR)

Summary: A introduction to how next-generation managed detection and response (MDR) solutions allow cloud security operations to take a proactive approach to cybersecurity.

Want to read the entire 26-page eBook? CONTACT US



Client: Vade Secure

What they do: Predictive corporate email security

Summary: An introduction to the evolving email threat landscape and why you must implement advanced email security specifically for Office 365.

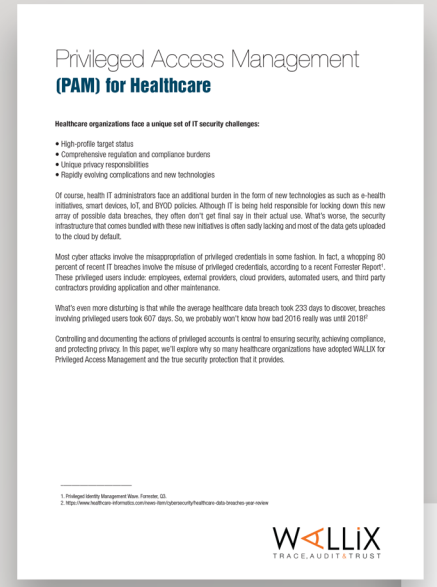
Want to read the entire 15-page eBook? CONTACT US

Client: Swimlane

What they do: Security Orchestration Automation and Response (SOAR) platform

Summary: An introduction on how using security orchestration to automate incident response improves security operations.

Want to see the entire 18-page eBook? CONTACT US



Privileged Access Management
(PAM) for Healthcare

Healthcare organizations face a unique set of IT security challenges:

- High-profile target status
- Comprehensive regulation and compliance burdens
- Unique privacy responsibilities
- Rapidly evolving complications and new technologies

Of course, health IT administrators face an additional burden in the form of new technologies as such as e-health initiatives, smart devices, IoT, and BYOD policies. Although IT is being held responsible for locking down this new array of possible data breaches, they often don't get final say in their actual use. What's worse, the security infrastructure that comes bundled with these new initiatives is often sadly lacking and most of the data gets uploaded to the cloud by default.

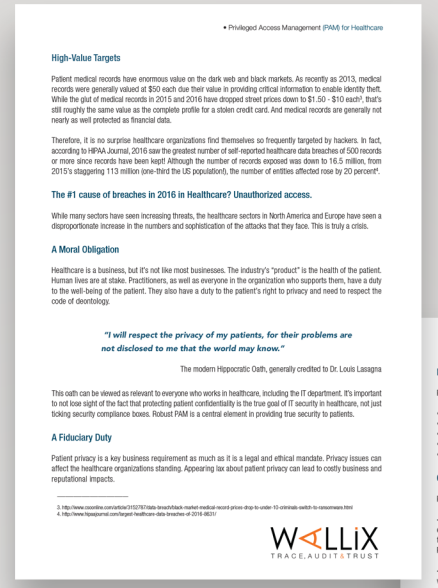
Most cyber attacks involve the misappropriation of privileged credentials in some fashion. In fact, a whopping 80 percent of recent IT breaches involve the misuse of privileged credentials, according to a recent Forrester Report[1]. These privileged users include: employees, external providers, cloud providers, automated users, and third party contractors providing application and other maintenance.

What's even more disturbing is that while the average healthcare data breach took 233 days to discover, breaches involving privileged users took 607 days. So, we probably won't know how bad 2016 really was until 2018![2]

Controlling and documenting the actions of privileged accounts is central to ensuring security, achieving compliance, and protecting privacy. In this paper, we'll explore why so many healthcare organizations have adopted WALLIX for Privileged Access Management and the true security protection that it provides.

1. Privileged Identity Management Wave. Forrester, Q3.
2. https://www.healthcare-informatics.com/news-item/cybersecurity/healthcare-data-breaches-year-review

WALLIX
TRACE.AUDIT&TRUST



High-Value Targets

Patient medical records have enormous value on the dark web and black markets. As recently as 2013, medical records were generally valued at $50 each due their value in providing critical information to enable identity theft. While the glut of medical records in 2015 and 2016 have dropped street prices down to $1.50 - $10 each[3], that's still roughly the same value as the complete profile for a stolen credit card. And medical records are generally not nearly as well protected as financial data.

Therefore, it is no surprise healthcare organizations find themselves so frequently targeted by hackers. In fact, according to HIPAA Journal, 2016 saw the greatest number of self-reported healthcare data breaches of 500 records or more since records have been kept! Although the number of records exposed was down to 16.5 million, from 2015's staggering 113 million (one-third the US population!), the number of entities affected rose by 20 percent[4].

The #1 cause of breaches in 2016 in Healthcare? Unauthorized access.

While many sectors have seen increasing threats, the healthcare sectors in North America and Europe have seen a disproportionate increase in the numbers and sophistication of the attacks that they face. This is truly a crisis.

A Moral Obligation

Healthcare is a business, but it's not like most businesses. The industry's "product" is the health of the patient. Human lives are at stake. Practitioners, as well as everyone in the organization who supports them, have a duty to the well-being of the patient. They also have a duty to the patient's right to privacy and need to respect the code of deontology.

"I will respect the privacy of my patients, for their problems are not disclosed to me that the world may know."

The modern Hippocratic Oath, generally credited to Dr. Louis Lasagna

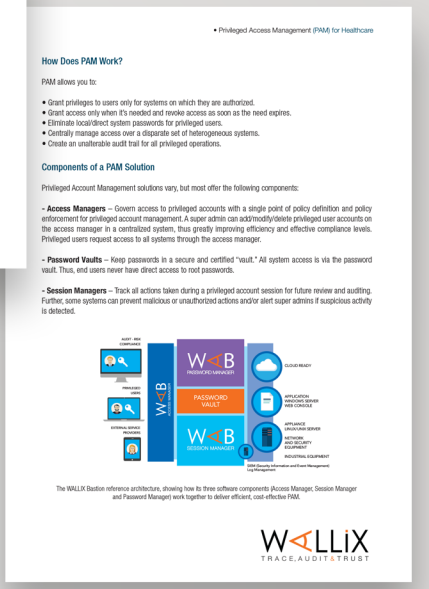
This oath can be viewed as relevant to everyone who works in healthcare, including the IT department. It's important to not lose sight of the fact that protecting patient confidentiality is the true goal of IT security in healthcare, not just ticking security compliance boxes. Robust PAM is a central element in providing true security to patients.

A Fiduciary Duty

Patient privacy is a key business requirement as much as it is a legal and ethical mandate. Privacy issues can affect the healthcare organizations standing. Appearing lax about patient privacy can lead to costly business and reputational impacts.

3. http://www.csoonline.com/article/3152787/data-breach/black-market-medical-record-prices-drop-to-under-10-criminals-switch-to-ransomware.html
4. http://www.hipaajournal.com/largest-healthcare-data-breaches-of-2016-8631/

WALLIX
TRACE.AUDIT&TRUST



How Does PAM Work?

PAM allows you to:

- Grant privileges to users only for systems on which they are authorized.
- Grant access only when it's needed and revoke access as soon as the need expires.
- Eliminate local/direct system passwords for privileged users.
- Centrally manage access over a disparate set of heterogeneous systems.
- Create an unalterable audit trail for all privileged operations.

Components of a PAM Solution

Privileged Account Management solutions vary, but most offer the following components:

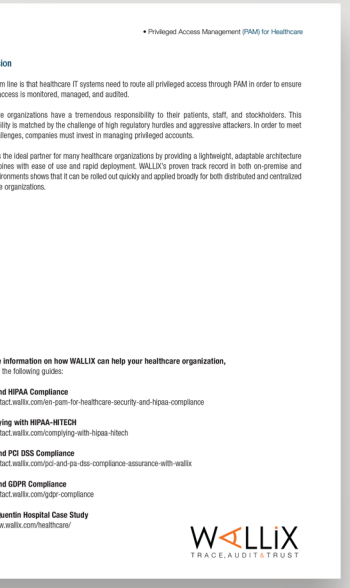
- **Access Managers** – Govern access to privileged accounts with a single point of policy definition and policy enforcement for privileged account management. A super admin can add/modify/delete privileged user accounts on the access manager in a centralized system, thus greatly improving efficiency and effective compliance levels. Privileged users request access to all systems through the access manager.

- **Password Vaults** – Keep passwords in a secure and certified "vault." All system access is via the password vault. Thus, end users never have direct access to root passwords.

- **Session Managers** – Track all actions taken during a privileged account session for future review and auditing. Further, some systems can prevent malicious or unauthorized actions and/or alert super admins if suspicious activity is detected.

The WALLIX Bastion reference architecture, showing how its three software components (Access Manager, Session Manager and Password Manager) work together to deliver efficient, cost-effective PAM.

WALLIX
TRACE.AUDIT&TRUST



Conclusion

The bottom line is that healthcare IT systems need to route all privileged access through PAM in order to ensure that this access is monitored, managed, and audited.

Healthcare organizations have a tremendous responsibility to their patients, staff, and stockholders. This responsibility is matched by the challenge of high regulatory hurdles and aggressive attackers. In order to meet these challenges, companies must invest in managing privileged accounts.

WALLIX is the ideal partner for many healthcare organizations by providing a lightweight, adaptable architecture that combines with ease of use and rapid deployment. WALLIX's proven track record in both on-premise and cloud environments shows that it can be rolled out quickly and applied broadly for both distributed and centralized healthcare organizations.

For more information on how WALLIX can help your healthcare organization,
download the following guides:

- **PAM and HIPAA Compliance**
  http://contact.wallix.com/en-pam-for-healthcare-security-and-hipaa-compliance
- **Complying with HIPAA-HITECH**
  http://contact.wallix.com/complying-with-hipaa-hitech
- **PAM and PCI DSS Compliance**
  http://contact.wallix.com/pci-and-pa-dss-compliance-assurance-with-wallix
- **PAM and GDPR Compliance**
  http://contact.wallix.com/gdpr-compliance
- **Saint Quentin Hospital Case Study**
  http://www.wallix.com/healthcare/

WALLIX
TRACE.AUDIT&TRUST

WALLIX
TRACE.AUDIT&TRUST

WALLIX Group is a cybersecurity software vendor dedicated to defending and fostering organizations' success and renown against the cyberthreats they are facing. For over a decade, WALLIX has strived to protect companies, public organizations, as well as service providers' most critical IT and strategic assets against data breaches, making it the European expert in Privileged Access Management.

As digitalization impacts companies' IT security and data integrity worldwide, it poses an even greater challenge if the data involved is highly sensitive. The recent regulatory changes in Europe (NIS/GDPR) and in the United States (NERC CIP/Cyber Security Directorate) urge companies belonging to sensitive sectors to place cybersecurity at the heart of their activity.

In response to these challenges, WALLIX created a bastion designed to secure organizations' core assets while adapting to their daily operational duties. WALLIX ADMINBASTION Suite. The WALLIX bastion accompanies more than 150 operators in sensitive sectors to conform with regulations and over 400 organizations in the protection of their critical assets, securing the access to more than 170,000 resources throughout Europe and the MEA region. It was also the first government-certified solution in the market.

WALLIX partners with a trained and certified network of over 90 resellers and distributors that help guarantee effective deployment and user adoption.

WALLIX is the first European cybersecurity software editor to be publicly traded and can be found on Euronext under the code ALLIX. As one of the leaders of the PAM market, major players trust WALLIX to secure access to their data: Danaqua, Dassault Aviation, Gulf Air, Marss Telecoms, McDonald's, and Michelin are among them.

WALLIX is the founding member of Hexatrust. The WALLIX bastion was elected "Best Buy" by SC Magazine and awarded at the 2016 Computing Security Awards, IBPI Excellence, and Pôle Systematic.

Twitter: @wallixcom
More information on: www.wallix.com

OFFICES &
LOCAL REPRESENTATIONS

WALLIX FRANCE (HQ)
http://www.wallix.com/fr
Email : sales@wallix.com
250 bis, rue du Faubourg Saint-Honoré
75017 Paris - FRANCE
Tel. : +33 (0)1 53 42 12 90
Fax : +33 (0)1 41 87 48 38

WALLIX UK
http://www.wallix.co.uk
Email : ukinfo@wallix.com
1 Farnham Rd, Guildford, Surrey,
GU2 4RG, UK
Office: +44 (0)1483 549 944

WALLIX DEUTSCHLAND
http://www.wallix.de
Email : dietrich@wallix.co
Leitelsteiger Str. 206
81241 München
Phone: +49 89 716771910

WALLIX USA (HQ)
http://www.wallix.com
Email: usinfo@wallix.com
World Financial District, 60 Broad Street
Suite 3502, New York, NY 10004 - USA
Phone: +1 781 569 6638

WALLIX RUSSIA & CIS
http://www.wallix.com/ru
Email: wallix@it-bastion.com
ООО «ИТ БАСТИОН»
107023, Россия, Москва,
ул. Большая Семеновская, 45
Тел.: +7 (495) 225-48-10

WALLIX ASIA PACIFIC
(Bluecoure Asia Pacific Pte Ltd)
Email : contact@bluecoure-soac.com
8 Ubi Road 2, Zervex 07-10
Singapore 408538
Tel: +65-6333 9077 - Fax: +65-6339 8836

WALLIX AFRICA
SYSCAS (Systems Cabling & Security)
Email: sales@wallix.com
Angré 7ème Tranche Cocody
06 BP 2577 Abidjan 06
CÔTE D'IVOIRE
Tel. : (+225) 22 5181 90

www.wallix.com

Client: WALLIX

What they do: Privileged Access Management (PAM) software

Summary: An overview of the unique cyber threats that face healthcare organizations and why implementing a priviledged access management solution is critical to protect healthcare IT systems.

Want to see the entire 10-page eBook? CONTACT US

Solution: How Swimlane Applets and Applications are up to the challenge

Security orchestration, automation and response

A security orchestration, automation and response (SOAR) solution like Swimlane automates manual and time-consuming security management tasks. Additionally, SOAR centralizes security operations by orchestrating incident response playbooks and workflows across multiple specialized security tools and related infrastructure. A security analyst empowered by SOAR can use a single console to monitor, investigate and respond to the outputs of SIEMs, EDRs, antimalware, sandboxing, threat intelligence and other security technologies.

SOAR enables SecOps teams to automate existing alert responses by modeling and orchestrating the workflow steps tied to virtually any use case. For example, an incident response process might call for a suspicious binary to be manually entered into a system such as VirusTotal for inspection. The SOAR solution handles the VirusTotal step on its own, automatically submitting the binary and collecting the results in a matter of seconds.

SOAR solutions allow SecOps teams to automate and orchestrate operational tasks and existing alert responses.

By automating and orchestrating time-consuming and repetitive tasks, such as opening and updating trouble tickets in systems including Jira or Remedy, creating reports, logging into multiple systems, entering incident information, and sending email alerts, SOAR significantly speeds up threat management and incident response processes.

SWIMLANE 3

Swimlane Applications

Applications within Swimlane are user-defined templates for collecting, storing and organizing your data. They can contain any combination of user-defined and out-of-the-box content, including both preconfigured and custom case management forms, workflow templates and relevant dashboards.

Swimlane Applets

Swimlane Applets are a preconfigured set of fields and layout specifications and can include playbook or workflow components that can be plugged into any Swimlane Application easily. By dropping them into to an existing Application, users can quickly and update and expand their existing Swimlane deployment to rapidly adapt to their unique security toolsets, incident response processes and personnel. Applets are essentially reusable building blocks that can be deployed in any combination to address virtually any use case with simple drag-and-drop deployment.

What's more, Swimlane's predictive orchestration mapping largely automates the process of integrating new tools so that adding new technologies into an environment is virtually seamless. Thus, combining these two features, new use case-specific Applications can be deployed rapidly to address an infinite number of incident response scenarios.

Modular by design

The modular nature of Applets is what makes them so versatile and valuable. SecOps teams can reuse previously built Applets easily, either on their own or as part of a collection. Users can mix and match Applets as needed to quickly build out customized Applications that rapidly map to unique configurations and processes. For example, with Applets, a team could quickly reconfigure an existing threat hunting SOAR application to incorporate an EDR's alarm data and its enforcement capabilities to facilitate automated responses to specific threats. Hundreds of Applets are available out-of-the-box to address specific threats and use cases.

SWIMLANE 4

Sharing without tipping off the bad guys

The availability of Applications and Applets helps resolve another challenge of collaboration between security teams: They may be reluctant to share detailed information about their responses for fear of inadvertently tipping off attackers about their security practices and architectures.

This lack of cooperation amongst security professionals is becoming increasingly problematic as the bad guys are increasingly sharing their own information and code on the dark web. The unprecedented level of organization and "professionalism" amongst cybercriminals and state actors, many of whom are working in loose concert, is an incredible challenge for even the largest organizations trying to adapt their defensive postures on their own quickly and effectively.

Swimlane helps address the core reasons behind this isolation in two key ways:

- The modular nature of Applets compartmentalizes sensitive information
- With AppHub, a trusted and open marketplace for Applets where all contributions are validated by Swimlane.

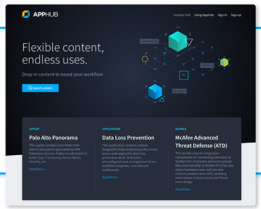


Figure 1: The Swimlane AppHub allows trusted organizations to securely share Applets, Applications and Bundles of integration components…

All validated by Swimlane.

SWIMLANE 5

Vendor-neutral community: SecOps Hub

Swimlane is also supporting **SecOps Hub**, a new vendor-neutral community for security operations professionals. This open community is aimed at helping security analysts and admins get better at what they do. It gives security professionals a place to share ideas about incident response processes, preferred security tools and specific threat management strategies. One could think of it as a hive mind for the SecOps community.

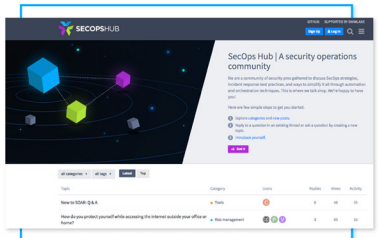


Figure 3: Join the vendor-neutral SecOps Hub to share SecOps tips and tricks with fellow professionals.

SWIMLANE 7

Conclusion

Security teams don't have time and resources to waste. With the ever-growing and evolving threat environment, duplicative and redundant SecOps environments can be costly and exhausting. Safe and effective collaboration in addition to automation and orchestration can solve these problems. Swimlane's approach to Applets and Applications harnesses the wisdom of the entire SecOps community and allows teams to build and share security response workflows that embody best practices that don't have to be constantly reinvented.

About Swimlane

Swimlane is a scalable and innovative leader in security orchestration, automation and response (SOAR). The flexible solution delivers powerful, consolidated analytics, real-time dashboards and reporting from across your security infrastructure, maximizing the incident response capabilities of over-burdened and understaffed security operations.

The scalable, innovative and flexible security solution offers a broad array of features aimed at helping organizations to address both simple and complex security activities, from prioritizing alerts to remediating threats and improving performance across the entire organization.

To arrange for a demo of Swimlane or to speak with one of our security architects to see if SOAR would be helpful to your organization, please contact us at 1.844.SWIMLANE or email us.

SWIMLANE 10

Client: Swimlane

What they do: Security Orchestration Automation and Response (SOAR) platform

Summary: An introduction to the benefits of modular security applications including the ability to create playbooks, modify workflows, and share optimized processes with peers.

Want to read the entire 10-page eBook? CONTACT US

About glassCanopy

You could probably write a fantastic eBook every quarter that would engage your prospects and customers... if you had the time. glassCanopy effectively creates that time by taking on all of the heavy lifting: conceptualization, research, writing, and final layout. All you have to do is provide feedback and revisions.

We then take those eBooks and integrate them into a lead generation machine that we run for you. We handle everything:

- Content creation
- Ad buy planning and execution
- Landing page and banner design
- Integrating with your CRM and marketing automation
- Lead nurture campaigns
- Closed-loop analytics, reporting, and optimization

Our core services cost between $10-25K per month plus media buys. We're best suited to companies with complex products/services with average deal sizes of $10K or more.

If you're interested in seeing what we can do for you:

Give us a call at (415) 663-7826

Send us an email at rich@glasscanopy.com

Get in touch

v5