OPEN ALLIANCE for CLOUD ADOPTION

Topic: SIEM in the Cloud

Contributors:

Krishna Jadhav – TechMahindra
Mark Williams – RigD
Matt Estes—The Walt Disney Company
Ryan Skipp—T-Systems
Shamir Charania – Keep Secure
Tom Scott—The Walt Disney Company
William Dupley — Liam Associates Inc

Contents

LEGAL NOTICE

1. Executive Summary

It is no secret that Security Incident and Event Management (SIEM) systems are a core part of the security controls for any enterprise. Most SIEM organizations focus on detection and response activities such as gathering logs, predictive threat identification, sometimes providing the tooling, and querying across multiple sources of data during investigations and normal operations. In recent years, SIEM tools have evolved to incorporate concepts such as machine learning and IT automation, which allow SIEM solutions to not only detect issues, but automate a response when appropriate.

Despite the advances in technology, the underlying problem with SIEM effectiveness has remained the same. What combination of endpoint telemetry, log capture/storage capabilities, processing power, and alerting will deliver the right alert to the right team at the right time with the right amount of detail needed to take decisive action to mitigate the threat?

In many ways, the introduction of cloud services changes some of the problems SIEMs have traditionally had, making some better and some worse. Taking telemetry as an example, cloud services are generally better at having telemetry out of the box than native applications. This is contrasted with the fact that there are now greater quantities of those logs to deal with, and those logs are still not security focused.

Enterprises therefore have to figure out how to deal with SIEM “at arm’s length” from the cloud perspective. Security teams will have to use creative techniques to gather all the inputs they require from cloud providers to build effective SIEM strategies. They will have to do this at cloud-speed, and, increasingly, thinking about systems and business processes in a distributed fashion. All of this on the backdrop of the division of responsibility between provider and enterprise, the shared responsibility for industry-specific regulation, and the broader business-to-business nature of SIEM processes and operations in a Hybrid IT environment.

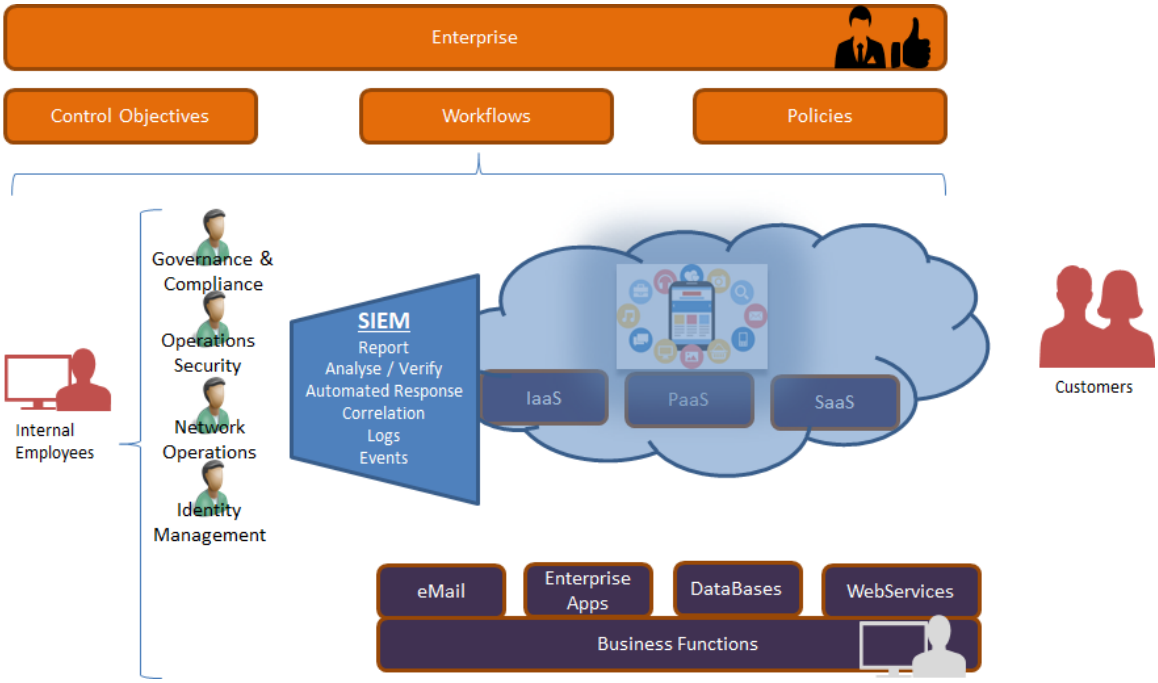
This document shares some of the problems, experiences, and learnings that companies have gone through in this regard.

2. Introduction

SIEM is about dealing with incidents and events in a Hybrid platform environment (Private and Public cloud), based on security controls defined as necessary for that enterprise.

While SIEM exists within the framework of security controls, it is not about the controls themselves. Rather, it's about how incidents and events are detected in hybrid cloud environments and how they are then managed per the compliance requirements, security control definitions, rules, and policies in the organization.

One may consider SIEM as a key pillar of governance, and this pillar now has to be extended to include the externally leveraged Cloud services. This can be illustrated by means of a graphic:



This is best understood by defining some problem statements for SIEM in a Hybrid World.

This paper is targeted at Leadership and Security Managers in order to help drive awareness of the changes necessary in skills, technology, and processes relating to SIEM that need to be considered, when moving into a Hybrid Cloud Platform environment.

3. Problem Statement

A whole host of new challenges and opportunities arise as the Security organization faces a Hybrid Platform environment.

Increased security threat sophistication: Security attacks have evolved from fame-seeking deniers of service to mercantile exchange's offering digital armies to deploy brute force attacks, exploit zero-day vulnerabilities, and hold data hostage with ransomware.

Business unit managers ignoring security policy: It is not uncommon for business unit managers to feel that security practices are an impediment to their business. They often complain that their company must move much faster than IT enables them and as a result cannot afford the time wasted by the security demands.

Inadequate and inconsistent information technology patch management: The majority of IT breaches occur because hackers have exploited a known weakness in the operating system of the technologies in an IT architecture. There are many reasons why software is not consistently patched. Since storage, server, PC, and servers are all managed by different organizations, it is very common for these organizations to not consistently patch or renew the hardware and software maintenance since each has their own process, schedule, and technology. In many cases, patch management is still done manually which leads to inconsistency of implementation of the patches as well.

Employees compromising security: A major source of security breaches is caused by employees. Employees are generally unaware of the risk their decisions pose to themselves and to the enterprise. Some are under a false belief that their IT organization or their Internet carrier is protecting them from security threats.

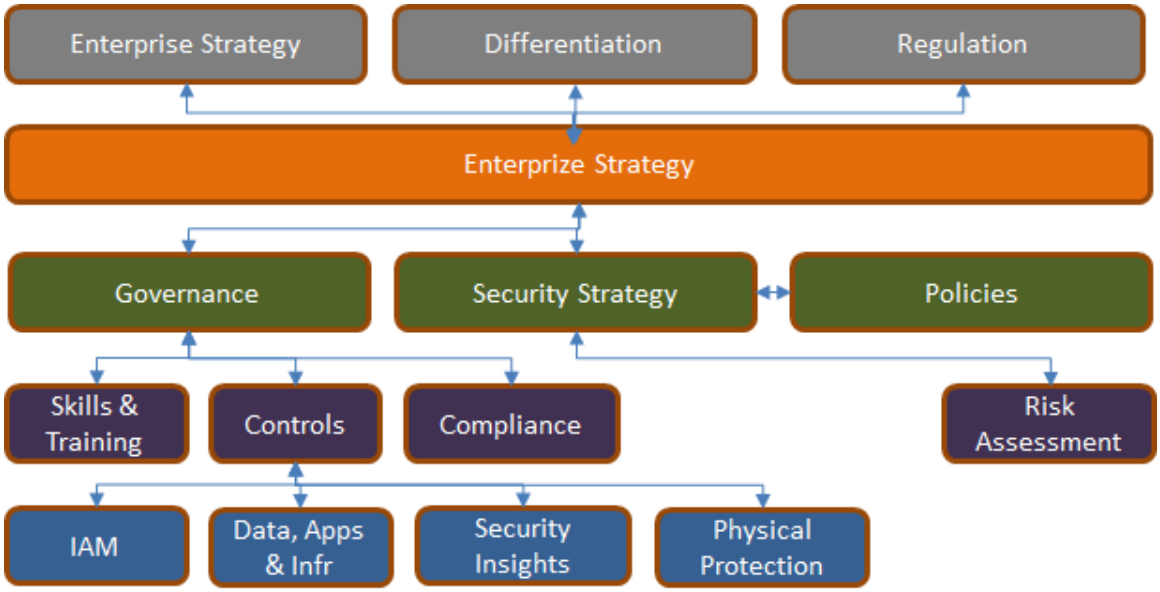
Security vs Development: There is often tension between security teams and developers due to conflicting goals. Developers want their software in production as quickly as possible. Security teams stand in the way of that with requiring developers to go back to the drawing board in order to fix flaws. Often Security keeps changing the demands, or the demands may be inconsistent, depending on which Security entity/person the developers are working with…so they avoid each other, and problems or gaps arise.

Skill Opportunities: Budgets should account for training of developers in security and Operations in big data analytics, so as to avoid overwhelming the SIEM team or searching for / retaining scarce resources.

Automation Opportunities: Leverage Automation technologies so as to lighten and focus the human teams on exceptions that the automated responses can't deal with.

Illustratively, 58% Of All Healthcare Breaches Are Initiated by Insiders, as reported by Forbes 2018 [ix]

It can be seen from these challenge areas, that updates may be needed in a number of areas. Some of these areas that need enhancement to accommodate Hybrid IT are illustrated below as per the Cloud Security Alliance models:



Specific examples to address these problems are discussed next, under the banners of Organization and Roles, Process and Governance, and Technology.

4. Organization and Roles

a) Skills

A number of entities in the organization will need to develop new skills to deal with SIEM in Hybrid Clouds and Cloud Native Application environments. These entities include:

- Security teams
- Users
- Developers
- Management
- Networking teams

I. Security Team Skill Updates

Start by identifying relevant training to bring the current SIEM team into the cloud world – give them a strong base of new cloud knowledge to work from. Consider what they need to know regarding:

a. Cloud Technology (Cloud Native, Micro-services, Containers, Security provisioning in a Cloud Native App)
b. Extended corporate perimeter and new threats, entry points to manage
c. DevOps and where they fit into it
d. New vectors of attack

Many corporations are addressing the skills shortage reality by bringing on specialized managed services organizations to do their security threat identification and analysis.

According to a recent report[i] there are significant talent shortages in the security realm. Currently some of the top five security positions going unfilled are:

1. IT security administration (34.3%)
2. Security architect (28.2%)
3. Security analyst/incident responder (27.6%)
4. Application security tester (22%)
5. Compliance auditor (21.6%)

One of the primary reasons that these positions are unfilled is that in many countries, security personnel are not paid that well. As a result, it is not attracting resources. Cybercrime organizations pay very well. An important recommendation is to review the salaries of security resources to ensure that you attract and retain the staff you need.

Security could be trained to be a consulting organization within the enterprise, to the Business, and to the Developer (DevOps) teams, amongst others.

The security team will need to learn about cloud native applications and related threats, and how to better secure apps in a DevOps process and environment. Those learnings include creating a capability to develop and write code and scripts, as well as working with APIs (including how to develop Security as Code!) A key to integrating security processes into DevOps is learning about and then implementing security as code [ii].

II. User Skill Updates

A large percentage of security breaches arise with employees who are either generally unaware of the risks of their actions to themselves and to the enterprise, or deliberately violate the policies for various reasons. Some are under a false belief that the IT organization or their Internet carrier protects them from security vulnerabilities. For example, very little stops an employee from accidentally or deliberately finding a way around controls and clicking on an illicit email link or turning off virus scanning technology or safe website detection software because it's perceived to slow down the service. Some even believe that because they have a Mac they don't have any problems because security issues are only on PCs. The solution to this behavior is education. Users must continually be trained on how to detect security threats and how to avoid compromising the security of the enterprise.

The IT security organization must take responsibility for all security training and certification. A policy is recommended that enforces the consistent certification of employees on security threat detection and prevention methods. It is often recommended that users who do not recertify annually have their access to the enterprise network revoked.

III. Developer Skill Updates

There is often tension between security teams and developers due to conflicting goals. Developers are driven to get their software into production as quickly as possible. As discussed in the Organization and Roles section, security teams slow them down with extensive testing and demands, resulting that developers often first have to go back to the drawing board to fix flaws. A culture of respect between the two groups has to be developed recognizing each other's benefits and imperatives, and that must then be supported by a culture of collaboration.

In some organizations (depending on the prevailing culture and leadership), companies are even hiring developers and teaching them about security, as this can sometimes be easier than taking traditional security people with experience and trying to push them into new ways of working!

Developers usually hold most of the keys to supporting integration of security into DevOps. The No. 1 priority for developers involved in a secure DevOps transformation should be self-education about security (and hiring more security-knowledgeable developers). In general, DevOps can make applications more secure by baking security into the Software Development Lifecycle, right from the earliest stages of that cycle, if they know what to do and what the threats are that they must defend against. In mature security organizations where application

security was already an integral part of development, it is usually more easily prioritized as a critical DevOps process component, but where a secure SDLC was not part of a disciplined practice previously, it can get left behind in the rush to DevOps.

Security (or the DevSecOps role for it) also has to constantly evaluate the developed code (usually leveraging tooling) to ensure that no malicious openings have been created either deliberately or accidentally by the developers.

Once SIEM is done properly, the organization is in a far better position to deal with ongoing detection and management of security related incidents and events during the operational phase of the product.

IV. Management Skill Updates

It is common for business unit managers to feel that security practices are excessive and an impediment to their business, and that their company must move much faster than IT enables them, in order to be competitive in their marketplace. As a result, they claim they cannot afford the time "wasted" by the security demands. This has become very common with the rapid expansion of cloud services.

These managers need to be trained regarding the criticality of security with respect to data and product protection, Customer protection, and the protection of the company brand. They also need to understand the compliance requirements of the industry sector they are part of and what that really means in the IT space.

It is often more expedient for a business unit manager to just buy a cloud service than to develop their own service, especially since an internally developed service must follow the corporate security policies. The managers need to learn what to look for, from the cloud provider, regarding security and compliance.

Most business unit managers choose to ignore security IT policies because IT delivery is just too slow – therefore IT must commit to business management to identify/provide secure, supported cloud services or providers with the same speed of delivery as a commercial cloud provider.

V. Networking Team Skill Updates

Leveraging Hybrid platforms means that a business function often ends up with more networking connectivity between its elements, and the elements may be located separately on appropriate platforms. The network team needs to understand the criticality and impact of the network on the business transactions, how the security of cloud applications work, and then enable the application or function. For example, if the data is located in a data lake on the private cloud, and the customer interface is located on a public cloud, and parts of the application leverage SaaS services from other providers, then they need to learn about QoS, application and data access, and authentication mechanisms, and the sensitivities of the cloud

app to the network. From a SIEM perspective though, their tools need to support detection of illicit activity and traffic profiles – and the team needs to learn what these are and how to deal with this dimension.

Often the network team will attempt to apply their standard policies to networks supporting cloud applications. By introducing them to the architecture and concepts of Cloud Application Design, and including representatives from Networking in the DevOps team, required updates to policies and other issues can be identified early on. The network team is in a better position to design and prepare their monitoring and control systems to automatically enable and apply the necessary controls that help the applications to work according to the business requirements, safely and securely.

b) Organizational Changes

Organizations are designed to facilitate the efficient execution of the work of a company. When considering changes to an organization due to new security threats, we need consider some of the most significant security issues facing enterprises today.

"Security threat sophistication" is increasing exponentially and is taking advantage of the lack of security understanding of many people using cloud services. Corporations need to significantly change their attitude toward how security is viewed. No longer is it a disruptive necessity but rather should be seen as "part of the team" needed to move things forward.

VI. Reporting Line

Many companies have well established "reporting lines" that can, in the modern and agile environments of businesses today, become barriers to needs of the business to be responsive and nimble. The solution to this problem is not really an organizational one but a governance one. IT security policies need to be developed by a corporate security group who is responsible to write all security policies. These policies should include controls on physical assets, people assets, intellectual property, and information technology. The policy must be enforced on all levels of Corporation, and no manager, VP, President, or CEO can override these policies. This will ensure that if a business unit manager decides to compromise an IT security policy then they are committing a violation of the business conduct standards and could face dismissal.

This policy will provide the protection a company needs, but it is not an excuse for an IT organization not to transform its operational model to ensure a rapid supply of approved IT cloud services.

VII. Product Owners

Another key to any successful SIEM capability is to assign a formal Product Owner to every product of the organization, and to sensitize them to SIEM so that they are able to ensure that the SIEM requirements are catered for at the necessary level, at all times.

VIII. DevSecOps

An important step is to align the DevOps group and the Security group, with SIEM processes integrated throughout the Dev process, as part of the team. This enables the team to create rules and policies together and to develop monitoring points built into their products. The resulting Secure DevOps groups are often also referred to as DevSecOps [iii], or Rugged DevOps by practitioners.

By integrating the teams up front, one begins to avoid putting security reviews at the end of a production cycle, which is not effective because that often causes security problems and release delays that could have been caught if security expertise had been involved from the design phase forward.

Sometimes though, teams are still reluctant to collaborate, fearing that the larger integrated group will just slow the development process down to a crawl and make them unable to meet business demand for DevOps-level speed. Security teams are often also hesitant about trying to match pace with DevOps practices, since that would involve using more automation—and their security tooling hasn't always been up to the task. DevOps security teams must adjust to the required speed!

Operations teams need to take inventory of their environments and put every piece—especially network configurations—through automatic and manual security checks that security teams and operations build together.

Developers and operations will need to help facilitate this change by understanding more about what security teams do.

IX. Team Sizing

Successful Dev(Sec)Ops teams tend to be smaller and more focused on specific components of a product, meaning there are more of them. Without a fully automated tool chain, security can slow down the DevOps process by hours or days. Placing a security capability in each DevOps team up front (maybe a Developer assigned to represent security as a shared responsibility), can help to prevent gaps right up front, which could prevent gaps and inevitable slowdowns right up front. A common set of security requirements, threat definitions and sharing of updates provided through shared learning, structured knowledge management and standups across DevOps teams can also help prevent issues arising that would have otherwise led to slow downs.

X. Team Optimization through use of Automation

If an organization's security tools are friendly to DevOps, most security tasks/actions can be performed automatically in the same pipeline as the one used for producing the app. Only the security issues that require human intervention are then flagged for individual attention.

Basically, the statements above illustrate that instead of Security erecting quality gates that code has to pass through before moving to production, they need to erect guardrails that enable developers to develop securely, make some mistakes, but prevent them from creating disasters.

XI. Culture Updates

Here's how the DevSecOps Manifesto [iv] describes the underlying principles for culture changes which will strongly enable secure cloud application development and SIEM:

Cultural Aspect	From	To Be
Leaning in, **over Always Saying "No"**	Judging from the side	Actively finding solutions, as part of the team
Data & Security Science **over Fear, Uncertainty and Doubt**	Making generic statements	Specific problem listing – specific solution identification
Open Contribution & Collaboration **over Security-Only Requirements**	Only focus is security	Understand the groups' imperatives, and support them
Consumable Security Services with APIs **over Mandated Security Controls & Paperwork**	Paper checklists and quality gates from Security	API driven configurations and tests which include automated Security testing
Business Driven Security Scores **over Rubber Stamp Security**	Quality Gate manual approvals	Automated security testing (may include accepting certain risks at business level, in collaboration with Security, or leveraging acceptable mitigations or workarounds)
Red & Blue Team Exploit Testing Over-Relying on Scans & Theoretical Vulnerabilities	Reactive scheduled tests quarterly	Active inter-team testing continually for each stage of development (attack / contain or defend)

24x7 Proactive Security Monitoring Overreacting after being Informed of an Incident	Log analysis daily and reporting / escalating	Traffic monitoring and anomaly detection in real time
Shared threat intelligence / information hoarding info to ourselves	Private security group list of threats and risks	Open sharing of current risks and threats with developers
Compliance Operations **over Clipboards & Checklists**	Auditor style scheduled reviews	DevSecOps team participation throughout development

There are a few key steps that successful security teams engage in:

a. Identify automation opportunities for security testing and application of rules, policies, and configurations,
b. Automate software testing from a security perspective,
c. Integrate the security dimension early in development, to fail quickly, and find fixes for the failures,
d. Avoid generating false alarms,
e. Appoint security champions within teams,
f. Maintain operational visibility at all times.

A Culture of transparency should ultimately exist so that no one can hide when they circumvent rules and policies, but it must also be positive and constructive and the reasons for it must be well understood and transparent as well!

c) Tactical / Strategic approaches

Several solutions are possible to ensure that SIEM is capable, no matter what the organization size or current stage of cloud adoption:

a. When buying Cloud services, include the provider's SIEM capabilities for those services, from the provider, including reporting and compliance.
b. Constrain the scope of SIEM in each scenario and allocate that to a specialist organization – e.g. IOT, Websites, Network.
c. Break up SIEM into specialist sub-elements and buy it as a service from specialist providers.
d. Small and mid-size companies are often already forced into outsourcing SIEM as they have low resource capacity to try and keep up.

e. Even large organizations contract specialist SIEM services for specialist areas today

d) Summary of Organization and Roles

Security is everyone's responsibility. Not just the security organization. Professional policing has never been enough to ensure a community is safe. Most cities also implement neighborhood watch programs because everyone needs to be involved in recognizing security threats in a community. The same principles are valid in the enterprise. IT security organizations must be responsible for communicating and facilitating this reality to their organizations and rallying all employees to become part of a strong security enforcement team. There's no bigger relief than catching what might have been a serious security hole in the design or development phase of a new feature. That's what DevSecOps training and structure provide.

5. Process & Governance

Governance oversees a number of processes, and SIEM can help illuminate gaps and blockages that may exist. SIEM is a methodology in which an organization's information security governance strengths and weaknesses can be revealed. This revelation can provide insight into an organization's use of policies and governance as metric to measure its effectiveness across the organization. Governance, the decision an organization makes on how to enforce policies and compliance, can leverage SIEM as a way to gain understanding of how events are being managed, policies are being enforced, and whether or not compliance is being adhered to. Governance can then use this information to develop and enforce clear lines of responsibility and accountability, enhancing the security of information systems across the organization.

When IT existed exclusively on-prem, one of the ways it was defined was by process ownership. If the network experienced a disruption, the application owner would know about it but was helpless to address it, having to depend on the network team to identify and resolve the issue. However, in the Hybrid IT world, that process has a much more generic degree of ownership, and the lines that define it are becoming more blurred. Therefore, when moving to the cloud, end-to-end accountability must be understood and appropriately assigned. From the application/service owner to the service provider and even to third party suppliers all must be made accountable down to the component level. Ultimately, application/service owners must take ownership of how their services are meeting the needs of the business and understanding how to utilize SIEM in the Hybrid IT world will go a long way in achieving this.

a) Governance and Accountability

Governance specifies the accountability framework and provides oversight to ensure that risks are adequately mitigated, while management, ensures that controls are implemented to mitigate risks. SIEM is core to that accountability in providing both the needed information for

the development of security controls and the processes needed for a company to protect its assets. SIEM, if not implemented with governance, especially in the Hybrid environment, can lack direction and can be misaligned with the strategic needs of the company. A strategic plan to manage information security needs to be in place, and SIEM needs to be part of that plan.

The company's strategic teams must take into consideration not only key stakeholders from the security operations team, but also from the various "other" IT teams such as, risk management, compliance, audit and business operations, as well as, teams outside of IT, for example finance and procurement. Security use cases (as discussed in the Problem Statement earlier in this document) also need to be developed in order to drive the adoption of policy and provide inputs for the overall security strategy. These use cases can drive the development of security policies, and SIEM can help ensure they have been captured and are being adhered to.

b) SIEM's Effectiveness

SIEM's effectiveness should be driven by organizational management of corresponding policies and practices. As stated at the beginning of this section, SIEM needs to be in place in order to maximize the efficiency and effectiveness of governance. Both IT teams and stakeholders need to be able to see the alignment with policies and compliance as well as how events are being managed and responded to. This "visibility" is best achieved via reports and dashboards which can provide to stakeholders the actionable data they need to optimize strategy. This will help to drive the governance process, and for IT teams the insight needed to identify anomalies and act proactively on predictive analytics. Use cases also can help develop policy, policy can help drive compliance, and compliance can help ensure systems are protected and less vulnerable to attack.

Leveraging SIEM, especially in Hybrid IT, can help provide the insight needed to determine the effectiveness of the level of governance being applied. For example, in the case where default configurations are being used often, depending on the service being consumed, Basic Authentication will be the default authentication being offered. If not changed for external services, this level of authentication, when being used over a non-SSL connection, exposes the password in clear text every time it is called by a requesting service. Without policies in place to prevent this kind of use it could lead to exploitation of a service and allow access that could potentially lead to other vulnerabilities exposing the entire environment to attack. Another way to detect where policies may be falling short is to measure changes against defined Key Performance Indicators, (KPI's). When used to measure performance KPI's can be a useful tool in determining effectiveness, ownership and accountability. For example, if a large number of Denial of Service (DoS) attacks are occurring a KPI could be used to determine the target of those attacks and therefore the owner of that target could be held accountable.

c) Keeping up with Change

How we look at our environments has changed as much as the environments themselves – we now hardly think about off-prem as being outside the company's secure perimeter. As the Hybrid IT landscape evolves, so must the way we implement governance and policies on these environments. These changes can be large and impactful as well as subtle and, in appearance, insignificant. For example, when deploying in a public cloud provider environment accepting "default" configurations can not only lead to a breach in policy but create vulnerabilities that are not even in scope under current compliance rules. New policies and compliance rules must be in place before deploying in a provider/hosted on-demand environment. None of this works without the ability to ensure that policies are being adhered to and compliance is being enforced. However, carefully determining and assigning the appropriate accountability, in context of the business function and policies, will enhance business agility when they adopt Hybrid IT and improve performance, while also verifying the security posture's effectiveness against threats and cyberattacks across the organization.

d) SIEM and Patch management

The majority of IT breaches occur because hackers have exploited known weakness in the operating system of the technologies in an IT architecture. One example of this is the exploitation of "abandoned" virtual machines (VM), known as zombies. A zombie can be any VM that continues to run in the background but is not carrying any significant workloads and is therefore often forgotten and consequently left unpatched. This condition can spread and multiply over time causing what is called VM Sprawl, making it even more challenging to identify this as it is happening. Even with a SIEM solution in place, these and other patching challenges could still happen.

Here are a few reasons why software is not consistently patched:

1. There is a support cost that needs to be paid to ensure that equipment is kept up-to-date, and no one wants to pay the support cost.
2. The technology is old and is working fine and is no longer supported. No one wants to incur the capital expenditure to replace it.
3. Some of the old equipment has never had good security practices built-in, for example, old card key door scanners never implemented encryption. So, it's quite easy just to read the data that comes from one of these scanners and obtain the passcode. Again, the root cause of the problem is no one wants to pay for the capital expenditure to replace the old equipment.
4. The false belief that the bad guys are on the outside of the firewall [viii] and the good guys are on the inside. This is not true. Any retailer will tell you that 2% of their annual shrinkage is directly related to employee theft. IT theft by employees is much higher. Particularly in the area of intellectual property.

5. Closely related number four is not encrypting customer data or company private data at rest, in transit, or at destination. One large corporation recently disclosed that many of their customers' passwords were stored in plaintext on their internal server. They assumed it was safe because only their employees could see it.

The solutions to these problems start with a commitment from the CIO and the financial controller that all old equipment and equipment that presents a security threat is replaced, that support contracts are purchased, and that the required patches are made available to the IT organization to implement. Second is the implementation of a modern SIEM solution where data is collected in real-time, event driven automated remediation, policy engines that are kept up to date and aligned with the needs of the business to be agile and responsive to technology changes/opportunities.

e) Keeping it Safe

The next change deals with customer data. Technology must be implemented that ensures that all "customer data" and company "private information" is encrypted at rest, in transit, and at the destination. You will need a solution that can validate if encryption is indeed being used as intended. SIEM is the methodology needed to ensure that assets are working compliantly and in alignment with corporate policies. In the Hybrid IT ecosystem this can be especially challenging due to the mix of roles and responsibilities across various cloud models as they change from on-pre to off-prem environments. Utilizing SIEM to collect and preserve a "chain-of-custody" as evidence of an attack, or to store and annotate relevant events wherever the workload went, is paramount to securing the Hybrid IT workload.

Also consider inventory, if you don't know about it, you can't fix it. Maintaining an accurate inventory is paramount in addressing patch management. Automate monitoring to help identify and track VM's as they spin up and down enabling greater accuracy in identifying gaps in your patch management strategy.

Lastly, consider that SIEM security audits need to be conducted on cloud environments where the involved employees may now be located in distributed geopolitical areas and across boundaries, particularly when considering the transfer of personal and intellectual property data outside of the company. This can help reduce loss and potential legal battles.

f) Consistent Patch Management

While applications, infrastructure, storage, servers and PC's are all managed by different organizations, it is very common for these organizations to not consistently patch the hardware and software since each has their own process, schedule, and technology. In many cases, patch management is still done manually which leads to inconsistency of implementation of the patches as well. Create a view of the patch levels of the whole chain, and any anomalies.

Now that your systems are “in the cloud” you need to consider how SIEM can help to implement an integrated patch management process feeding automation tools and helping to ensure that all patches to all devices in the enterprise, whether on-pre or off-prem, are consistently updated. Whether this patch management process and toolset should belong to security, is open for discussion. There are many reasons why specific patches need to be done at certain times. Generally, only the equipment owners know when that is. We recommend that a common patch management tool is implemented across all technology environments so that all organizations using it can be audited equally by security, to ensure that consistent patch management is facilitated. It is also recommended that security take a very active role in scheduling patches and ensuring that they are consistently implemented on all technology platforms across all organizations.

SIEM is made up of many processes ranging from data aggregation to compliance verification and analytics. These, and other SIEM processes can change when implemented across the Hybrid IT model.

Some key areas to consider which must change:

1. Security Information Management
    a. Must develop the ability to pro-actively respond to trend analytics.
    b. Must be extended to the Hybrid environment.
    c. Enable patch management through AI enablement of the tools.
2. Security Event Management
    a. Must pro-actively respond to events with no/minimal human intervention.
    b. Must manage events throughout the Hybrid environment.
    c. Enablement of AI tools is needed to manage events across workloads.
3. Security Operation
    a. Monitoring of network and host events.
    b. Timely and accurate detection and alerting of critical issues.
    c. Enabling defensive measures and rapid/pre-active incident response.
4. Authorized Providers
    a. Must go through a “vetting process” to determine which services can be used.
    b. Provider services must be adapted to deal with Hybrid IT SIEM reporting.
5. Controls prevent certain events from impacting the integrity of processing or data.
    a. Examples are computer operations, physical and logical security, program changes, systems development and business continuity.
    b. Application controls include policies and procedures designed and implemented in the business areas by the respective owners of the applications and data.
6. Compliance helps avoid conflicts and improves process by detecting breaches and adherence to regulatory mandates.

7. Hybrid Inventory is both organic and ethereal, elasticity and on-demand services make managing inventory challenging and elusive.
    a. Assets that are deployed to on-prem hardware can be just as challenging as off-prem. Virtualized environments, even on-prem, can still experience organic growth that is difficult to track and reconcile.
    b. Look at inventory holistically and consider the workload which transcends on and off prem environments.
8. Visibility is key to security, if you can't see it you probably can't secure it.
    a. Know who's accessing what, and for what reason.
    b. There is a myriad of actors in the environment and you will not be able to control them all.
        i. Consider managed access using federated identity and role-based access control.
    c. East-West traffic is where most of the connections are happening yet has the least safeguards in place to restrict and control access between systems.
        i. Consider isolation techniques such as dynamic and micro-segmentation.

SIEM is a great way to collect data on your Hybrid environment and enable actionable response to changes and anomalies. Use SIEM data analysis from across the technology landscape to identify needed changes in how applications are built and developed. This can enhance and drive agile methodologies while delivering on data driven policy enforcement.

6. Technology

From a technology perspective, the fundamental building blocks of SIEM have not changed significantly in the last few years, even with the uptake in cloud/SaaS usage. From a capability perspective, SIEM tooling still needs to perform the following tasks:

- Data collection/storage/processing,
- Event Detection,
- Investigation Support
- Response support

The resulting goal for SIEM technology in a Hybrid IT environment**: The SIEM technology must acquire and generate data to drive changes in how applications are built and deployed more securely.**

a) Data Concerns

The value of any implementation of SIEM has always been tied to the amount of data sources the SIEM can consume and process (and as an extension, the value of the data provided by those data sources). Current day SIEMs are expected to not only be data sinks (think traditional

syslog forwarding from many small endpoints), they are also expected to understand the APIs of various cloud/SaaS providers and to periodically fetch data for ingestion.

Moving from the traditional SIEM use cases, SIEMs can, and should, consume telemetry arising from DevSecOps outputs in a well-built application. In a cloud native application which is located on a Hybrid IT platform, it assumes that good practices have been applied throughout the development phase, and all key components have measurement/monitoring points built in, and appropriate tooling is integrated to trap and collect events and classify them. In ideal scenarios, SIEM specific application SDKs should be used to provide a deeper connection between the running application and the SIEM. This allows for richer logs with more context to help enforce security rules and make security related decisions.

The increase in the amount of data sources required for full investigations has caused a problem in how logs are ingested and stored. Modern day SIEMs should leverage cloud-constructs such as blob storage, data lakes, and auto-tiering to allow for maximum retention of required logs while minimizing overall storage costs. Other data techniques, such as lambda functions over data, should be employed to maximize the speed of querying the stored data.

The increase in data has also caused an issue with processing time of any given log. While this was always an issue before, the ideal of logs being processed “in-real-time” is vague at best.

Take an example. An event occurs at your cloud provider. It may take seconds or minutes for that event to be surfaced in an activity log on their management plane. The management plane may have the capability of forwarding that event to your SIEM, which also incurs a latency overhead. Once it gets to your SIEM, there is a storage latency and a processing latency before an alert is actually generated and sent to an administrator. Minutes or hours may elapse.

In the cloud world, security professionals need to become (more) comfortable with the idea of eventual consistency. Events may be generated from source systems, and it is expected that there will be a delay before that event is converted to an incident and alerted upon. Hence the need for event prediction based on the leading pattern analysis!

b) Event Detection Concerns

From an event detection standpoint, SIEM technology has taken many steps to get to present day capabilities. What started out as simple if/then rules grew up to become correlation rules written and maintained by SIEM companies.

Self-described “Third Gen” SIEM solutions make use of AI and ML tooling to augment existing detection capabilities. User/Entity Behavior Analytics (UEBA) is the next logical step in SIEM tooling. Making use of ML and behavior baselines, UEBA promises to help address issues of malicious/compromised insiders, incident/alert prioritization, and data loss prevention.

Taking the concepts of UEBA one step further, SIEM solutions are starting to make use of graph databases. The unique way of building/storing relationships in these database types assist with activities such as kill chain detection and pivoting in investigations between relevant data sources.

While UEBA is a core component of modern day (cloud focused) SIEM technology, these SIEMs need to continue to use traditional techniques for event detection, most notably integration with third-party threat intelligence feeds (both commercial and open).

In the cloud, SIEM solutions must strike a hard balance from a feature set perspective, continuing to focus on core metrics such as mean-time-to-detection, and false-positive rates.

c) Investigation Support

In true cloud applications, the amount of telemetry data from this monitoring increases exponentially, and teams must carefully decide what telemetry data to collect and process in each application or business function, else they can quickly become overwhelmed! This is where AI technology can help extensively, and even enable them to sense problems in advance, and apply automatic corrections or fixes before an incident occurs.

In a modern architecture, monolithic applications have been broken down in to smaller, purpose specific services. The problem that this presents for modern-day SIEM is twofold. The first is that there is an exponential increase in the amount of event volume that needs to be handled (discussed elsewhere). The second is that these smaller services are now one (or more) steps removed from the context of a given request. Because of this, it is harder to understand the nature (or intent) of a particular request, and thus, harder to understand the security impact. Modern day SIEMs must employ strategies around distributed tracing, allowing security personnel to examine sets of event data in terms of higher-level constructs such as user flows, or request journeys. [x]

The architecture for the SIEM function needs to be updated to consider and manage the overhead that would be incurred through a lift n' shift of the SIEM management systems to Hybrid IT – this could drive exponential license cost increases (license sprawl), and an updated SIEM architecture should consider this dimension, along with adjusted SIEM management processes.

It is important to actively monitor for events and items of concern in *near real-time* in the logs, rather than collecting the logs once a day and analyzing them to see if anything outside of standards has occurred. The idea is to become aware of a problem as it is happening - e.g. see multiple-failed-logon attempts, then pro-actively check if a brute-force attack is about to bring the user interface down, and proactively block the source causing it. In addition, reactive analysis of logs further enables patterns of activity to be identified, and then for proactive planned steps to be designed to counter reoccurrence of the threat.

SIEM tools are generally still in early versions and not yet ready for Cloud landscapes. (Typically, we consider Gen 1 tooling typically performing traditional reactive log analysis, vs Gen 2 which often considers SNMP alerts and events, and Gen 3 moves towards behavioral profiling and leveraging AI - predictive). In addition, Cloud Native SIEM solutions are typically also in v1 level, because the vendors themselves are carefully considering rapidly evolving new architectures for cloud native applications and business functions, which heavily leverage SaaS and PaaS models with their own SIEM capabilities built in.

Cloud providers generally do a good job of logging their services, but the cost of leveraging this data in the organization's central SIEM tools can be prohibitive. Using data analysis tools selectively as part of a SIEM solution can make prediction of problems easier and be a more cost-effective approach, rather than just updating to a full Gen 3 SIEM tool for all environments. IMPORTANT: Take a selective approach in this regard – determine what, why, and how exactly is needed for each application landscape, for what business protection purpose, and don't try to do the same level of monitoring, analysis and actions for all business applications or functions.

Rather than trying to import all of the data from various elements of the landscape, leave it at the endpoint (as a small data sink), and leverage API's to query specifics from that data that are known indicators of a problem. For example, *query the logs via API for known issues, rather than collecting and storing them centrally.*

Leverage automation as far as possible – once patterns of undesired activity have been identified through use of log pattern analysis and AI, automate the corrective actions, else actual administrators will be constantly dealing with new alarms and be swamped in prioritizing and attending to each.

Create a defined library of flagged events and counteractions for Hybrid IT landscapes, which enable the SIEM team to be able to focus more on updating this library with new pre-classified patterns of threats for cloud native apps, rather than actually having to tend to the events themselves. It may be useful to add AI and capabilities like security graphs for cloud application monitoring points for linking data points together, to create clear records of causes and associated effects in the library.

In summary, from a technology perspective, there should be a larger focus on User/Entity Behavior Analytics (UEBA) and Security Orchestration/Automation/Response (SOAR).

Some good recommendations that many enterprises and cloud providers such as Microsoft [v] and AWS identify regarding what should change specifically in the SIEM-supporting technology are as follows:

- Templates for Security Architecture - create a template defining the target state for security capability which reaches from internal environments, to the whole Hybrid IT estate

- List your current tool capabilities, and what is missing, then make sure the existing and required capabilities are leveraged across the Hybrid environment consistently.
- Adjust the paradigm for analyzing security events – consider all IT elements from a perspective of trustworthiness and integrity, rather than some of the more traditional groupings/classifications (e.g. previously network / firewall, server, now becomes customer interface, data transport, transaction or business function)
- Re-order the Security Operations Checklists to align more appropriately to actual Hybrid IT environments
- Move from batch driven data collection and analysis to event driven triggering (preferably then feeding automated systems for responses, with humans only becoming involved with exceptions)
- Synchronize or integrate information protection and threat protection with identity and access control systems in the various parts of the Hybrid systems in use (such as Multi-Factor Authentication), to ensure that authentication is being provided by secure and compliant sources!
- Discover and register your data in SaaS environments, and define its protection requirements, policies, and mechanisms. (e.g. on prem vs off-prem specifics for the handling of data and what may be located where and in what format, and with what protection)
- Update your data loss prevention (DLP) tooling and integrate it with SIEM to leverage the DLP engines, with automation.

By considering some of the above items in your technology landscape, one would be well on the way to reaching a more proactive state for dealing with SIEM in Hybrid IT environments.

7. Conclusion

Security is everybody's problem. Hybrid IT opens new threat paradigms and attack vectors, which must be considered by IT, DevOps, Business, and all other business functions (e.g. Procurement who contracts the partnerships), and this has to start from Executive level. The "operating model" of IT must be updated, and an education/sensitizing initiative must address all layers of the company about security, and the impact of security breaches. It is extremely easy for any business user to start up a service in the cloud, and IT may never find out about it and know of its existence!

As organizations begin to include Hybrid IT platforms in their production environment it becomes crucial to update their structures, processes, and technologies relating to SIEM, to accommodate and oversee these environments. Strategic updates and enhancement to their Security controls will enable them to more easily recognize the benefits that they expect cloud services to deliver for the organization, safely, and with minimized risk. One cannot just expect external cloud providers to meet the organization's expectations either – these need to be aligned and selected carefully, and if done well, can bring great enhancement and benefit to business functions.

An example is always useful to lead management, and it helps to see how others have brought the data together and figured out how to represent SIEM data across different sources. One can consider the examples of some of the companies using one illustrative technology stack here [xi]

Authority and mandate must be issued from the executive levels, to make this work – and not be seen as a pocketful of cloud fanatics trying to update the organization "from the side". Failure to do this effectively may lead to brand damage, and blaming of cloud and Hybrid IT, together with wasted money resulting from difficult or costly recoveries if a breach occurs. The Gartner SOAR strategy (Security Orchestration, Automation and Response) [xii] also ties the elements discussed in this document together very nicely and logically.

And the responsibility in the end, for both success or failure in this regard, will rest on the Executives' shoulders!

8. References

a) Web References

i. 5 IT security roles business are most desperate to fill: https://www.techrepublic.com/article/5-it-security-roles-businesses-are-most-desperate-to-fill/

ii. Security as Code: Why a mental Shift is Necessary for Secure DevOps: https://simpleprogrammer.com/security-code-secure-devops/

iii. Secure DevOps: What's in it for dev, sec and ops?: https://techbeacon.com/app-dev-testing/secure-devops-whats-it-dev-sec-ops

iv. DevSecOps Manifesto: https://www.devsecops.org/

v. Cybersecurity Reference Architecture: Security for a Hybrid Enterprise: https://www.microsoft.com/security/blog/2018/06/06/cybersecurity-reference-architecture-security-for-a-hybrid-enterprise/

vi. An Evaluators Guide to NextGen SIEM: https://www.sans.org/reading-room/whitepapers/analyst/evaluator-039-s-guide-nextgen-siem-38720

vii. A SIEM Security Primer: Evolution and Next-Gen Capabilities: https://www.exabeam.com/siem/a-siem-security-primer-evolution-and-next-gen-capabilities/

viii. Anomaly Detection in Log Data using Graph Databases and Machine Learning to Defend Advanced Persistent Threats: https://arxiv.org/pdf/1802.00259.pdf

ix. 58% of all Healthcare Breaches Are Initiated By Insiders: https://www.forbes.com/sites/louiscolumbus/2018/08/31/58-of-all-healthcare-breaches-are-initiated-by-insiders/

x. Towards Turnkey Distributed Tracing: https://medium.com/opentracing/towards-turnkey-distributed-tracing-5f4297d1736 and https://opentracing.io/docs/overview/what-is-tracing/

xi. Introducing Elastic SIEM: https://www.elastic.co/blog/introducing-elastic-siem

xii. Prepare Your Security Operations for Orchestration and Automation Tools: https://www.gartner.com/en/webinars/3866777/prepare-your-security-operations-for-orchestration-and-automatio