IDC ANALYZE THE FUTURE

IDC TECHNOLOGY SPOTLIGHT

Sponsored by: IBM

Unified threat management is about people, processes, and technology — all these areas count. Any improvement in software makes the security analyst better, and streamlined processes improve accuracy. Connecting teams beyond the security operations center (SOC) improves outcomes even more.

Making Molehills from Mountains: Using a Platform Approach to Simplify Security Management and Operations

October 2020

Written by: Christopher Kissel, Research Director, Security and Trust Products

AT A GLANCE

KEY STAT

72% of all midmarket companies (with 2,500 or fewer employees) spend at least 50 man-hours per week chasing down alerts.

WHAT'S IMPORTANT

Data, cloud, and networks are critical control planes. Security operations centers (SOCs) must have visibility and continuous monitoring capabilities in each control plane.

Introduction

A quick snapshot of the global condition helps frame the challenges in cybersecurity. Naturally, the first communal problem is the global reaction to the coronavirus. Corporations, governments, and individuals now use social distancing. Working from home, which was once limited to people of certain vocations — has become a much broader phenomenon: Roughly 20% of companies have one-quarter or more of their workforce working from home or expecting to work from home. This trend has created three rifts in cybersecurity:

- The first weakness is that end users often must work through a virtual private network (VPN), and even when a VPN is either impractical or simply not used, devices still needed proper protection.
- The second problem is that the camaraderie among workers in the security operations center (SOC) has changed. New emphasis has been placed on workflow because teams are no longer housed under one roof.
- The third consideration is that data protection has become a bigger concern. Many companies have had to expedite moving on-premises assets and data stores onto the public cloud. The control plane for data in the cloud is different from the control plane for data on premises, and the data itself often has various levels of importance.

The onset of COVID-19 has accelerated emerging trends in IT and cybersecurity, with the following cybersecurity trends among the most compelling:

- **Digital transformation.** The digital transformation that has happened over the past several years has focused on the speed of business more than detailed cybersecurity postures or processes. Companies consider cybersecurity adversaries an important threat to their long-term well-being, but far more dangerous is the idea that their business models will become obsolete. The transformation already includes Uber's disruption of the taxi industry, travel agencies as online entities, and ecommerce companies pushing aside brick-and-mortar businesses. (Sadly, COVID-19 is wreaking havoc with retail businesses that are running on thin margins.)
- **Data gravity.** An essential part of digital transformation is gaining insights from data. However, to take advantage of cloud computing and storage, companies sometimes store critical data and metadata in public clouds. Data types such as personally identifiable information (PII) require additional attention.
- **Multitiered networks.** The definition of networks now includes private and public clouds, mobile devices, container software, straight-to-user applications, open source applications, and conventional assets behind a stateful firewall. This leaves the SOC team no alternative other than to continuously monitor L3–L7 network layers and to have a proper response if an incident occurs. According to IDC's December 2019 *Data Security Survey*, which was conducted in North America and EMEA, the average corporation has assets in eight different datacenters and protects 2,675 endpoints.
- **Talented adversaries.** Wherever the organization and its development team may be, an adversary can be there too. The adversary can initiate an attack anywhere, from the BIOS of a machine, to malware and phishing, to cookies and web applications, as well as from the network exfiltrating data. Unfortunately, the adversary picks the battlefield.
- **Noisy cybersecurity tools.** However amazing best-of-breed cybersecurity tools may be, several problems still exist. Each tool has its own type of temperance. An alert can be anything from a benign user interaction (e.g., a mistyped password) to a latency, a rule violation, or a full exploit. Regrettably, a network is never a settled thing — updates to an application or an operating system, power failures, or any number of alternative events can alter the network from its last known good state.

  With each security tool, there is a new set of alerts, widgets, and workflows for analysts to learn — and a dashboard for each feature. At some point, there is a "paralysis of analysis." Worse yet, alerts often come without sufficient context to create a plan for incident response. An analyst may need to piece together three or four alerts and throw out false positives before he or she can begin remediation.
- **Scarce cybersecurity analysts.** Assembling a strong SOC team is problematic to begin with; keeping analysts together may be tougher. The relationship between businesses and cybersecurity analysts is frayed on both ends. Security analysts often have too much work to do. Without proper tools, the formal triage of alerts that may or may not lead to the root cause analysis of a security problem is tedious and burnout becomes a factor. On the other hand, if the cybersecurity stack is not automated, the skills of given analysts are not easily replicated, meaning that the SOC analyst becomes a prized commodity. Equilibrium between businesses and analysts is hard to achieve.
- **Agility within the SOC.** Cybersecurity is a maze of dashboards. Even the best analysts are looking up identities on LDAP, isolating user groups, and performing manual research about domains, malware types, and threat actors.

We have posited the problem, and now it is time to consider resolutions. A mathematical expression of incident response would be to optimize:

- Incident = Time to detect + Root cause analysis + Lateral movement
- Response = Protection of most sensitive assets + Fortifying ingress/egress/access

Let's first consider the "incident" side of the equation. The sum of this is linear; an improvement to any discrete aspect of incident improves the net efficacy of the process. For example, improved monitoring to an initial detection improves the time to execute the whole cycle. As we intimated, detection is often noisy, so the ability to streamline the events to a more accurate narrative and perform root cause analysis is crucial for success. Finding out where the adversary has entered the network and where he or she has gone or is going becomes imperative for remediation.

Now let's pivot to the "response" part of incident response. The art of remediation is not just to throw patches at everything — it is also determining which assets must be protected first and which paths to and from the network are the most exposed. Risk, too, includes the following components:

- Internet-facing devices are much more at risk than on-premises machines and assets. Understanding a web server is more important than protecting a print server.
- Exposure matters. A file type that can be manipulated, destroyed, or altered is more tenuous than a file that can simply be observed by an adversary (admittedly, this is not a great outcome either).
- If files are leaving the network, the SOC team must prevent the leakage.
- A platform should be able to determine if given users have access to specific data.

The network itself is changing. Perhaps a decade ago, security teams could stash critical assets behind an on-premises firewall and the network architecture was flat. This is no longer the case. The network consists of private and public clouds (often more than one public cloud), ephemeral workloads in containers, mobile users, and Internet of Things (IoT) devices. The complexity of networks is changing, but what cybersecurity analysts must achieve is still straightforward.

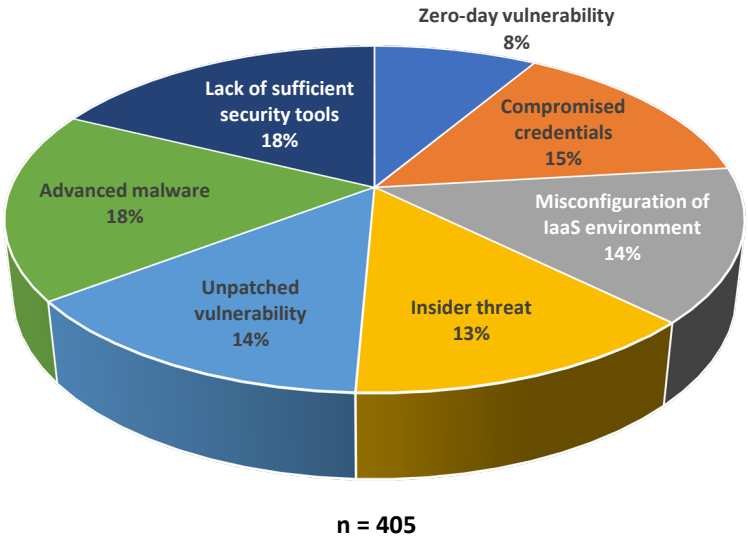
Imagining the Best Possible Platform Approach to Cybersecurity

The first consideration for a state-of-the-art cybersecurity platform is that it must be cloud native but not confined to software as a service (SaaS) — that is, the platform should provide flexibility to deploy where an organization chooses: on premises, in a public or private cloud, or as a hybrid architecture. A cloud allows for cloud compute, multitenancy, remote storage, a central vantage point for search, better north-south ingress/egress, and the possibility of using public cloud infrastructure as a service (IaaS) as a connective tissue for multiple appliances. A flexible architecture also supports organizations with hybrid environments, including multiple clouds and on-premises solutions.

Digital transformation and — now — work from home are accelerating trends. Visibility of IaaS is not so much a suggested good practice as it is a requisite cost of doing business. IDC's December 2019 *North America Cloud Security Survey* asked respondents to identify the source of the most recent breach in their IaaS environments. Figure 1 illustrates their responses.

FIGURE 1: ***Causes of the Most Recent Breach in an IaaS Environment***

Q *For your most recent breach of an IaaS environment, what was the predominant factor that resulted in the breach?*



n = 405

Source: IDC's North America Cloud Security Survey, December 2019

Of course, on-premises servers can be protected by a stateful firewall and air-gapping machines or by simply configuring servers and routers without internet access as on-premises security measures. It's also worth noting that companies may not wish to relinquish on-premises security because different applications and compute were designed for legacy architectures and would be (or are proving to be) difficult to replicate in cloud environments.

The platform has to be vendor agnostic. This seems like it would be a tough pill to swallow for any security product vendor. However, cybersecurity vendors must seek the best outcomes for their clients. End users cannot be cowed into vendor lock, and a key feature for any tool or platform is that the business not be required to "rip and replace" existing security tools.

The platform should also include data loss analytics and file integrity management (FIM). To be fair, several tools are involved in defending data from improper access or obfuscation. However, the ability to see whether data is leaving a network should be a line item.

The quality of alerts should be managed and vetted within the platform even before the analyst considers an investigation. A smart platform should be the central nervous system of information coming to and from security information and event management (SIEM) tools, endpoints, firewalls, and threat intelligence tools, as well as any other adjacent IT-related software. However, cybersecurity tools are temperamental.

The tools often see anomalies that are based on changing network conditions (e.g., new configurations, operating system and software upgrades). Ultimately, a platform needs to weed out weak signals and correlate stronger alerts.

Cybersecurity teams need to match the speed and agility of their attackers. Intelligent automation is the long game.

Further, the process of incident investigation is inextricably tied to workflow. For example, when an analyst researches a specific malware family, the dashboard should prompt what is known about the malware type — this information should not require additional mouse clicks. Playbooks are immensely helpful to analysts, too, prompting what to do next in investigations and where to initiate remediation. Every efficiency counts.

Considering IBM Cloud Pak for Security

IBM Cloud Pak for Security is a cloud-native, automated, and unified security platform that uses the following technical underpinnings found in other IBM technologies:

- **IBM Security QRadar and QRadar on Cloud.** The on-premises QRadar is like an enhanced SIEM tool with device vulnerability management, multiple user behavior analytics (UBA) algorithms, network detection and response (NDR), and IBM X-Force Threat Intelligence embedded on the same platform.
- **IBM Security Resilient.** IBM's purchase of this software in 2016 has enhanced capabilities in security orchestration, automation, and response (SOAR). SOAR is more than automation. With IBM Cloud Pak for Security, automation and orchestration are the gateway between discrete appliance and external threat intelligence from IBM X-Force. Without this ubiquitous recording platform, measuring mean time to detect and mean time to respond is impossible. The SOAR platform is also extensible, and new playbooks can be accessed through IBM Security App Exchange.
- **IBM Security Guardium.** This holistic set of smarter data security offerings affords clients the visibility, automation, and scalability they need while complying with regulatory mandates. IBM Cloud Pak for Security now includes frameworks for over 180 regulators.
- **The artificial intelligence (AI) engine Watson.** AI by Watson is now integrated into cybersecurity operations. One of the first security use cases for Watson was pulling together threat intelligence reports to the SOC. Watson is on the back end working to refine alerts and direct the analyst through the investigation process.

IBM Cloud Pak for Security incorporates these linchpin technologies onto a hybrid multicloud platform. Through pre-integration with Red Hat OpenShift, IBM Cloud Pak for Security can be deployed on premises, in a private cloud, or in a public cloud. It will soon be offered through a SaaS delivery model. Importantly, IBM offers the product on a "seat license" basis, meaning the solutions that are part of Cloud Pak for Security are priced for how many servers they protect, not by the volume ingested. It is also simple to add additional solutions using this pricing model. Key features of Cloud Pak for Security include:

- **Simplified install.** Cloud Pak for Security offers a unified deployment experience across private cloud and the various public cloud environments. Built-in automated processes simplify the deployment to as few as two clicks and less than 15 minutes of setup time.
- **Seamless analyst workflow.** Cloud Pak for Security provides an intuitive, modern user experience that brings together visibility, detection, investigation, and response in one console — no more switching between different tabs and screens. SOC analysts can view SIEM alerts from QRadar, gain prioritized threat intelligence, run federated searches across their IBM and third-party data sources, and orchestrate and automate tasks with seamless workflows.
- **Embedded SOAR.** Not only is there a directed workflow, but SOC teams can dynamically change the way they track assets. Query capabilities allow analysts to view all artifacts, and the security team can tag and classify artifacts for further investigation. Dynamic playbooks also help guide the analyst through the response process, ensuring consistency of execution. Furthermore, integrations are simple due to a guided installation process, with configuration of each application through auto-generated and editable settings. In other words, Cloud Pak for Security provides protection from application installation to investigation remediation.
- **Dashboards.** Preconfigured and customizable dashboards provide quick visibility into threat intelligence, insider threat analytics, case management analytics, risk metrics, and SIEM monitoring, giving high-level overviews for security leaders and drill-down, detailed information for SOC analysts and incident responders.
- **Full case management.** The case management includes ticketing, task lists, and the ability to pass along cases to other analysts with notes on the progress made in the incident investigation. With visual design that leverages process techniques utilized in lean manufacturing, it's easy to manage and coordinate security responses.
- **Unified data insights.** Cloud Pak for Security can connect to multiple data sources, such as SIEM, endpoint detection and response (EDR), and data lakes from IBM and other vendors, to provide unified data insights without requiring any data migration. SOC analysts can search these data sources from one place and view standardized results for further analysis. In addition, because the platform is built on open source technology, any organization can build its own data source connector to the platform.
- **Data security.** IBM Security Guardium Insights for IBM Cloud Pak for Security connects data security insights to the broader security framework. This integration enables otherwise disjointed teams to take advantage of consistent case management and orchestration and improve their approach to data security by sharing context across other security tools.
- **Extensibility.** Cloud Pak for Security allows security teams to add new infrastructure using the pre-configurations from other frameworks. Additionally, because Cloud Pak for Security is a cloud-native appliance, IBM can enhance the platform with new threat intelligence, better interfaces, and road map items such as insider threat, data lake consumption, and AI-assisted investigation.

Challenges

IBM Cloud Pak for Security integrates several elements into a unified management platform. The idea of a unified management platform is not new, and several companies are developing similar architectures. Yet, in fairness, the IBM Cloud Pak for Security framework is accepting of open source and competitive cybersecurity tools, while competitors are creating automation for their own platforms.

Cloud security is still in nascent days. Cloud Pak for Security may find itself competing with tools that offer container security, configuration tools, network intelligence and threat analytics tools, and other automation and orchestration tools. But the near-term outlook for Cloud Pak for Security is positive, with continued enhancements planned for workflow, along with deeper integration with QRadar, new connectors, and a dashboard with a risk-centric approach.

Conclusion

Unified threat management should be more than just the work of analysts mining disparate information systems. At some point, insights should lead to conclusions and exposures should be remediated. The learnings of case investigation should populate new use cases. IBM Cloud Pak for Security is designed to be an effective approach for SOC teams as the solution offers both a single pane of glass and a unified workflow.

Cloud Pak for Security is a one-to-many platform that integrates external threat intelligence with the input data from multiple security point product tools. The emphasis on data and compliance is more than ornamental; risk and compliance are dual considerations, with vulnerability and incident detection helping establish the proper security posture. Cloud Pak for Security is intended to be a good fit for IBM customers because it is designed to work with existing security platforms and open source tools, and the product should further strengthen IBM's presence with IT/SOC teams.

About the Analyst

Christopher Kissel, *Research Director, Security and Trust Products*

Chris Kissel is a Research Director in IDC's Security and Trust Products group, responsible for cybersecurity technology analysis, emerging trends, and market share reporting. Mr. Kissel's primary research area is cybersecurity analytics, intelligence, response, and orchestration (AIRO). The major technology groups within this practice are SIEM, device and application vulnerability management, threat analytics, and automation and orchestration platforms.

MESSAGE FROM THE SPONSOR

Explore IBM Cloud Pak for Security Through an Interactive Experience

Whether you lead a security team or dig deep into investigations as an analyst, Cloud Pak for Security can help connect your teams and streamline workflows through a unified platform. This interactive digital experience demonstrates how Cloud Pak for Security can bring value to your role within a security team.

» ***Explore Cloud Pak for Security***

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.

5 Speen Street
Framingham, MA 01701, USA

T 508.872.8200

F 508.935.4015

Twitter @IDC

idc-insights-community.com

www.idc.com