E-Guide

Boosting Your Multi-cloud Security

March 2023

TechTarget

In this handbook:

Protecting one cloud environment is challenging enough. But, when you have a multi-cloud infrastructure to defend from evolving threats, the task becomes even more complex.

Fortunately, there are strategies that you can employ to boost your security, like multi-cloud threat hunting and SOCaaS.

This E-Guide not only delves into these topics, but it also ventures into the issue of securing industrial control systems.

Keep reading to unlock insights.

In this handbook:

How to get started with multi-cloud threat hunting

ED MOYLE, SYSTEMS AND SOFTWARE SECURITY DIRECTOR

Almost every organization is in the cloud. In fact, most organizations above a certain size are in more than one. As multi-cloud becomes more common, however, ensuring security among multiple providers becomes more challenging.

There are a few reasons why this is true, among them different security models and mechanisms between providers, lack of seamless visibility across environments and nonunified tool sets.

The good news is that being aware of these logistical challenges goes a long way toward planning around them. One of the best ways to do this is to deploy a comprehensive multi-cloud threat hunting strategy.

Let's look at some cloud-based threat hunting use cases and some of the logistical and other complexities multi-cloud threat hunting introduces into the mix, as well as how to maneuver around those challenges.

In this handbook:

WHY IS THREAT HUNTING IMPORTANT IN CLOUD ENVIRONMENTS?

Let's start by defining threat hunting and the value it provides in both single and multi-cloud deployments.

Threat hunting employs intelligence-driven analysis to determine if and where attackers have already gained access to your resources. While this description is a grand oversimplification, in a nutshell, threat hunting involves positing hypotheses -- based on known adversary tradecraft -- about how an attacker might have already surreptitiously gained access to your environment and then working out test conditions to prove or disprove those perceptions.

Threat hunting is important because sophisticated attackers can evade detection and bypass alarms. By staying vigilant for signs that attackers may have already notched a foothold in its network, an organization can increase its ability to detect those adversaries and, ideally, disrupt them before they can act on their intended objectives.

The same principles apply in a cloud context. The differences lie in how you obtain and analyze the information that goes into the process and the tools available to act in response.

In this handbook:

Cloud-based threat hunting rests on three fundamental precepts:

1. Just because your organization is in the cloud doesn't mean that attacker activity stops.
2. It is beneficial to your defense strategy to understand adversaries' objectives and the tradecraft they use to act on those objectives.
3. Visibility across all layers -- even those layers where operational management is on the cloud service provider's (CSP) side of the shared responsibility model -- help you better understand the adversary or their methods.

MULTI-CLOUD MAKES THINGS MORE COMPLEX

Logistically, the cloud makes threat hunting more complex. As Abbas Kudrati, Binil Pillai and Chris Peiris, authors of *Threat Hunting in the Cloud: Defending AWS, Azure and Other Cloud Platforms Against Cyberattacks,* wrote:

> As organizations migrate from a physical infrastructure/on-premise environment to a cloud environment, threat identification will be more challenging due to difficulties in compliance and configuration transparency, remote data sources and infrastructures, core security capabilities and the number of APIs. In a nutshell, as the attack surface is expanding, threat hunting requires more attention.

In this handbook:

The point the authors are making is that analysts need more information and training when threat hunting in the cloud. That's because hunters must understand and use the tool sets, security models, architectures, technology stacks and other elements deployed not only by their own organizations, but also by their CSPs, cloud suppliers and other providers.

Multi-cloud threat hunting further ups the ante. It means even more tools, more concepts, more APIs and more data sources. Cross-environment analysis and data correlation must also be factored in. Consider a three-way conversation among an on-premises user, an application front end in a PaaS and a back-end API in an IaaS VM, for example. Determining if a request made in that conversation was legitimate could involve various log repositories and different monitoring tools across each environment.

EXTENDING THREAT HUNTING TO MULTI-CLOUD

If your organization wants to roll out multi-cloud threat hunting, first, ask what practices you can establish to make that a reality. Ultimately, creating a strategy is unique to your company. It depends on your cloud usage, your threat hunting capability and approach, and your business needs. There's no one-size-fits-all approach, but there are some basic steps you can take to get started.

In this handbook:

First, normalize the data and event information that flows between your multiple environments, including CSPs and on premises. This is already a known bugbear of multi-cloud; for example, consider that the foundational pillars of cybersecurity mesh architecture include security analytics and intelligence, as well as consolidated dashboards.

Understanding events across environments is a core component of multi-cloud security management, operations, incident response and -- for our purposes here -- threat hunting. To do that, you must understand the cloud environments and services in use, know the security model(s) employed, and confirm you can and are collecting the right data from each location.

Second, address systematic threat modeling. Consider an application that spans multiple cloud environments. How do you know when a threat is a priority and how and where to apply resources to gather the information you need? Threat modeling can help. By taking an attacker's eye view of the application, you can start to develop hypotheses that gauge where and how adversaries might be more likely to attack. By extension, you can prioritize those areas for further exploration. This can help you know what data to collect from each environment and help you formulate the hypotheses you'll test to determine if an attacker is present in the environment.

Finally, there is education and actualization. Get educated about what you have fielded over different environments -- for example, building a reliable and systematic inventory -- and understand how components fit together, what native services are in use and how the services you use tie into the bigger, more sweeping narrative. This may sound basic, but it's the rare organization above a certain size that can do this reliably, accurately and completely.

Just like everything security-related, approach multi-cloud threat hunting through the lens of knowing your own usage, understanding your own security and business goals, and putting in the necessary thought and planning. Threat hunting can and should play the same role in your cloud security strategy -- multi-cloud or otherwise -- as it does for your on-premises environments.

▼ NEXT ARTICLE

Why your business needs SOC as a service

WARWICK ASHFORD, SENIOR ANALYST

Dismissed by some as a “marketing term”, security operations centre as a service (SOCaaS) is gaining traction and emerging as a discrete market because it addresses some key challenges facing most organisations, while also meeting other security and financial objectives.

WHAT IS SOCAAS?

Essentially, the term SOCaaS refers to a type of managed security service (MSS) that is cloud-based, built on a multi-tenant software-as-a-service (SaaS) platform, and goes beyond the managed security service (MSS) offerings of traditional managed security service providers (MSSPs).

Like MSS, SOCaaS includes all the monitoring and management of intrusion detection systems, firewalls, antivirus and antispam systems, virtual private networks (VPNs), endpoint protection (EPP), and endpoint detection and response (EDR). However, SOCaaS also provides:

In this handbook:

- Access to a team of analysts to resolve every alert, identify and analyse indicators of compromise (IoCs), and analyse and respond to attacks to minimise the impact of security incidents.
- Assistance in optimising an organisation's protection, detection and response capabilities through continual assessment and reporting, including guidance on security strategies and policies.

SOCaaS, therefore, includes services that typically make up managed detection and response (MDR) solutions and can be considered as an evolution of both MSS and MDR.
Although the term SOCaaS tends to be favoured by newer service providers, older organisations tend to offer services that meet the definition of SOCaaS as part of their MDR offerings. It is therefore important for user organisations to focus on the benefits of services that meet the SOCaaS definition rather than worry about whether those services are called SOCaaS or not.

Although the term SOCaaS tends to be favoured by newer service providers, older organisations tend to offer services that meet the definition of SOCaaS as part of their MDR offerings

With increasing demand for a comprehensive detection and response capability that is cloud-based and includes monitoring and analysis, the SOCaaS term is gaining currency in Europe and is likely to emerge as the dominant term to

TechTarget

Sponsored by:

OBRELA

distinguish these services from standard MDR and other more generic managed security services.

WHY IS SOCAAS NECESSARY?

The drive towards digital transformation and cloud services to improve efficiencies, increase agility and cut costs has rapidly and vastly expanded the attack surface of most organisations.

Cyber attackers have taken advantage of these trends as workforces become increasingly mobile and remote, accessing applications, systems, services and data both on-premise and in the cloud from outside the corporate network. The rapid increase in the number of people working from home through the Covid pandemic has accelerated this trend and compounded the risk.

In an effort to secure sensitive data to comply with a growing raft of data protection regulations around the world, and to protect intellectual property and other commercially sensitive information, most organisations have invested heavily in security monitoring tools on-premise and in the cloud.

For many organisations, however, this has resulted in an avalanche of security alerts being generated on a daily basis. For most of these organisations, especially small and medium-sized enterprises (SMEs), it is difficult or impossible to investigate and analyse every alert.

The emergence and adoption of SOCaaS has been driven by a combination of:

- The inability of most organisations to deal with security alert overload.
- The desire to get more value out of existing security investments.
- The need to expand security monitoring to include cloud, operational technology (OT) and internet of things (IoT) devices.
- The desire to achieve continual improvement by measuring the effectiveness of current security investments.

In addition, SOCaaS solutions provide the means of demonstrating to auditors a concerted effort to cover all cyber security risks and enable a comprehensive and standardised threat detection and response capability.

Another key driver has been the shortage of cyber security skills affecting organisations of all sizes. SOCaaS provides a way of tapping into the benefits of a security operations centre (SOC) or additional SOC resources without the challenge of finding and retaining people with the necessary skills. SOCaaS also provides a way of scaling up capacity quickly and at a much lower cost than maintaining additional capacity in-house.

WHAT ARE THE BENEFITS OF SOCAAS?

In the face of an increasingly challenging and rapidly changing business, IT and cyber threat environment, there is growing demand for SOCaaS as most organisations see the value of the benefits on offer, which include:

- Uninterrupted and comprehensive centralised monitoring and analysis of enterprise systems for suspicious activity at a fixed and predictable monthly or annual cost.
- Improved incident response times and practices.
- Faster detection of security events such as compromises and containment of threats.
- Resolution of all alerts to get maximum value out of existing systems.
- Reduced cost and business impact of security incidents.

TechTarget Sponsored by: OBRELA

In this handbook:

While MSSPs provide a wide range of services, they tend to generate too many alerts that need to be investigated. They also tend to lack advanced threat detection and remediation skills, require fixed and long-term contracts, and require a specific technology stack.

MDR providers, on the other hand, can provide round-the-clock monitoring and address the skills gap, but a narrow reliance on endpoint telemetry results in a high rate of false positives. MDR providers also typically require a specific technology stack, provide limited visibility and do not include remediation.

SOCaaS solutions provide the means of demonstrating to auditors a concerted effort to cover all cyber security risks and enable a comprehensive and standardised threat detection and response capability

For many organisations, especially SMEs, SOCaaS is the only way to:

- Consolidate all security threats, tools and systems into a single point of control to address and resolve all alerts.
- Monitor and respond to all indicators of potential compromise by analysing all security data.
- Evaluate the effectiveness of existing controls to identify how this can be improved.
- Get additional value from existing security investments.

In this handbook:

Taken together, these four factors are what distinguish the SOCaaS market from standard MSP or MSSP offerings, which typically:

- Do not all cover cloud environments.
- Are not all built on cloud-based SaaS platforms.
- Do not provide any analysis or guidance on developing a more effective security posture.

WHAT SIZE OF ORGANISATION BENEFITS FROM SOCAAS?

Although the requirements of user organisations vary widely according to size and industry sector, SOCaaS has something to offer all of them.

While micro and small businesses tend to need SOCaaS to fulfil all SOC functions, large enterprises tend to use SOCaaS analyst teams to supplement internal teams, while medium-sized organisations typically fall somewhere in between these extremes.

As a result, most SOCaaS providers typically specialise to focus on one or two of these sub-segments, with very few catering equally to all market segments. The trend of specialising to serve the needs of a particular market sub-segment is expected to continue.

SOCaaS suppliers focusing on SMEs will hone offerings to provide insights and guidance to enable organisations to co-manage their security with external SOC

TechTarget Sponsored by: OBRELA

In this handbook:

teams, for example, while suppliers focusing on medium, large and very large enterprises will expand their capabilities around risk, edge security, and OT and IoT security.

RECOMMENDATIONS

While SOCaaS has emerged as a discrete market, and no organisation can say it has no need for a centralised, coordinated view of its security posture and the ability to respond to threats and incidents, not all services provide all things to all organisations.

It is therefore important that each organisation:

- Recognises the importance and benefit of consolidating all security threats, tools and systems into a single point of control to address and resolve all alerts, to monitor and respond to all IoCs, and to evaluate the effectiveness of existing controls.
- Develops a thorough understanding of its current and future cyber security monitoring and response requirements from an MSSP.
- Recognises that some SOCaaS offerings are better suited to organisations of a particular size and industry sector, with some offering specialised support for regulated industries.
- Identifies which service providers best meet those needs, regardless of whether the service is called SOCaaS or not.

In this handbook:

SOCaaS offerings as defined above meet important challenges facing most organisations in the digital and post-Covid era. They provide benefits to organisations of all sizes and types, and therefore deserve consideration as part of any cyber security strategy.

▼ NEXT ARTICLE

In this handbook:

Industrial control system security needs ICS threat intelligence

MICHAEL COBB, CISSP-ISSAP

Industrial control systems were traditionally shielded from security threats due to their lack of external connectivity and the proprietary nature of their hardware and software. Today, however, ICSes, which oversee manufacturing processes and support key infrastructures, such as transportation systems and energy distribution networks, are isolated no longer.

Indeed, these systems now run on standards-based architectures and technologies and use the internet to connect with other ICS, IT and IoT systems. This interconnectivity has led to innovation and reduced costs as it enabled companies to remotely manage, monitor and control their ICSes.

But it has also dramatically increased ICSes' exposure to cyber attacks.

WHY ICS THREAT INTELLIGENCE IS KEY

Strong, effective ICS security is a must. Any compromise could result in loss of life and environmental disaster. The high availability requirements of ICSes mean security measures must not only be able to detect attacks, but, more importantly, they must prevent any attack from causing disruption.

In this handbook:

Threat intelligence, therefore, must be part of any ICS security strategy. This lets companies mitigate threats to operational continuity before they lead to downtime. Not surprisingly, one of the key metrics to evaluate the effectiveness of ICS threat intelligence is mean time to recovery -- the time between an attack's first operational disruption and the time when operations return to normal.

ICSes have a different threat landscape than traditional IT networks, and the consequences of a successful attack on an ICS can be much more severe. Generic threat intelligence, while useful, can't inherently help security teams improve their organizations' overall ICS security.

Strong, effective ICS security is a must. Any compromise could result in loss of life and environmental disaster.

Instead, organizations need ICS threat intelligence -- that is, threat intelligence specifically tailored to ICS equipment and processes. This enables organizations to gain an in-depth understanding of an attacker's motives and capabilities, past activities and the potential effects on their operations.

In this handbook:

TYPES OF THREAT INTELLIGENCE

Actionable information and insights into how adversaries compromise and disrupt systems can help predict and prepare for future attacks, stop active attacks and improve incident response plans. The three main types of threat intelligence are the following:

1. **Strategic threat intelligence.** This encompasses high-level, big-picture reports that detail the threat landscape, trends and potential effects. With this data, organizations can assess current and emerging risks and threats. Strategic intelligence is also valuable in making senior management aware of the overall threat environment, thus helping executives make more informed risk management decisions, security strategies and infrastructure changes aimed at strengthening the continuity and resilience of operations.
2. **Tactical threat intelligence.** This incorporates observed patterns, tactics, techniques and procedures associated with an attack lifecycle, the particular ICS technology being targeted, and the technical goals and consequences of the attack. This type of intelligence is used by SIEM systems and other analytical tools to link and analyze data points associated with a type of attack so security controls, such as firewalls and intrusion detection systems (IDSes), can be more effectively configured before an attack occurs.
3. **Operational and technical threat intelligence.** This entails detailed threat behavior and technical indicators, as well as signatures of emerging or active malicious activities, such as IP addresses and domains being used by suspicious endpoints, phishing email headers and hash checksums of malware. These

Sponsored by:

In this handbook:

indicators of compromise (IOCs) help organizations identify and stop incoming attacks and can be used to automatically block similar incidents in the future.

HOW TO GATHER ICS THREAT INTELLIGENCE

Threat intelligence can be acquired from both internal and external sources.

Internal ICS threat intelligence sources

Events and alerts logged by internal monitoring systems can be aggregated and analyzed in a SIEM system to turn unrelated and simple events into enterprise intelligence by comparing them to a baseline of typical activity to highlight unusual activity.

Analyzing suspicious activity can provide additional information that can be used to stop future attacks. For example, collecting IOCs and signatures of attack activity -- among them IP addresses and protocols used, file names and hashes, along with details of security control settings that failed to spot and stop the attack -- can all be used to better protect systems against similar attempts to compromise or disrupt operations.

TechTarget Sponsored by: OBRELA

External ICS threat intelligence sources

External sources of ICS threat intelligence can broaden the range and depth of information security teams base their decisions on. External sources include commercial and open source subscription services, security vendor reports and information shared within the industry and from government agencies, such as the Cybersecurity and Infrastructure Security Agency (CISA).

Look for quality third-party threat intelligence that is relevant, accurate and timely. It should describe the threat and explain its effect and the actions necessary to prevent or reduce the risk of the vulnerability affecting operations. Relevance is especially important as certain threats may only affect specific industries, verticals and geographic regions or particular technologies. Case in point: Spear phishing attacks target specific industries and individuals.

Avoid too much ICS threat intelligence

The main challenge with incorporating threat intelligence into a security program is information overload. To that end, it's important to be selective when choosing which sources of intelligence to use. Strategic intelligence should be collected only from evidence-based reports and white papers originating from well-respected security, industry and government agency leaders. Security teams should review these reports and present the results to stakeholders

In this handbook:

whenever an evolving threat is discovered or when significant changes to the threat landscape warrant a review of perceived risks and mitigation strategies.

USE ICS THREAT INTELLIGENCE TO MAKE IT TOUGHER FOR HACKERS

Tactical intelligence should be shared with security, operations and network teams so they can join forces to prioritize efforts to monitor and strengthen areas likely to come under attack. To extract important and usable intelligence in a timely manner, machine learning technology is required to filter and prioritize the quantity of information. This is also true of operational and technical threat data, which should be fed straight into active security controls, such as firewalls, IDSes and monitoring tools.

An important goal of any security initiative is to increase the cost and time it takes cybercriminals to mount a successful attack. ICS threat intelligence meets this objective by improving the effectiveness of real-time prevention and detection, which, in turn, makes security systems more proactive in combating a potential attack. At the same time, response and recovery efforts become more efficient, which lets enterprises withstand cyber incidents with minimal affect.

Incorporating threat intelligence into ICS security is not an easy task. It requires specialized workers to fully understand and react to the flow of information. Mission-critical systems and services are coming under increasing attack from

TechTarget
Sponsored by:
OBRELA

nation-states and other sophisticated bad actors. Having a better understanding of how, why and when attacks will occur can only help ICSes become more resilient.

To help others defend against infrastructure attacks, consider sharing internally collected threat intelligence, if possible, via initiatives such as CISA's Automated Indicator Sharing community and the Cyber Threat Alliance.

TechTarget Sponsored by: OBRELA

In this handbook:

Sponsor About Us

Obrela Security Industries is a global provider of cyber security services. Obrela provides security analytics and risk management services to identify, analyze, predict and prevent highly sophisticated security threats in real time. Founded in 2010 Obrela delivers Real Time Cyber Risk Management combining Threat Detection and Response (MDR) with the Managed Risk and Controls (MRC) services to resolve technology fragmentation and process disconnects, while aligning technology to business objectives leading to better decision-making.

Headquartered in London, UK OBRELA leverages a multi-tier operation model with Global Resilience Operations Centers and Regional Operations Centers to service the EMEA market combining international experience with local support. Obrela is recognized by Gartner Market Guide for its MDR and MSS services.

Our mission is to 'Keep Your Business in Business' at all times.

Website: https://www.obrela.com/