SAVIYNT

2023 AND BEYOND

Identity & Security Trends & Predictions

INTRODUCTION

“The arrogance of success is to think that what you did yesterday will be sufficient for tomorrow.”

The axiom, while cliché, captures the cybersecurity dilemma. From shifting regulation and workforce dynamics to intensifying board scrutiny, extortion-based threats and sprawling IoT landscapes, security leaders daily contend with new challenges.

At times, long-term planning feels like a lost cause. However, by considering industry trends and their implications, practitioners can weigh their own responsiveness, resilience, and agility–critical characteristics no matter what eventually comes.

In this eBook, we consider research and gather insights from cybersecurity leaders, consulting and systems integration experts, and technology providers. Further, we suggest actionable steps surrounding each trend to fortify your security posture.

From our research, here are eight trends we’re following.

TREND NO. 01

The New CISO Leadership Mandate

↓ HOW TO RESPOND

> "If all you got were other leaders to nod their heads, **expect your plans to fall apart when resistance hits.** You have to facilitate belief and buy-in, not just tell people what to do."
>
> **Jim Routh**
> *Former CSO & CISO*
> *MassMutual, American Express, DTCC & Aetna*

INTRODUCTION

Enterprises tend to view cybersecurity and business issues as distinct. In particular, non-security executives see cybersecurity as a "technical concern"– detached from the broader business.

Regrettably, CISOs often fuel this with leadership styles ill-suited for C-level effectiveness. Not surprisingly, disconnects emerge that affect the critical flow of resources and information. To maximize impact, CISOs must evolve their communication style to bridge gaps, improve performance, and even limit professional liability.

"Organizations, CEOs, and boards intuitively understand revenue," guides Gopal Padinjaruveetil, Chief Information Security Officer of the Auto Club Group. "In some cases, we ought to eliminate the term 'cyber risk' from our vocabulary, because every risk is a business risk."

With respect to role reframing, Anurag Rai, Principal, KPMG LLP, points out that CISOs must dispel the view of information security as the department of 'no.'

"Once CISOs understand business strategy, they must do all they can to enable it while also meeting security obligations. If a leader wants to be transformational, this is the way."

Rai notes how the CISO upleveling mimics the historical arc of the CFO or COO roles. "These executives were once seen as purely operational. Today, they are considered by boards as strategic, visionary offices."

David Mapgaonkar, Principal & Identity Practice Lead at Deloitte & Touche LLP, also reinforces how CISOs need to demonstrate how cyber helps achieve organizational initiatives. According to Mapgaonkar, “leaders must better articulate impact with respect to priorities including modernization, customer experience, workforce experience, and supply chain transformation.”

To enable this, Padinjaruveetil suggests that CISOs grow their story-telling ability, linking technical discussions to business inhibitors or growth opportunities that resonate with a specific audience. As responsibilities elevate, security officers must craft narratives to ensure that metrics, ideas, and proposals are grounded in stakeholder-centered language and outcomes.

“A CISO’s professional background unconsciously becomes an inhibitor in effective communication,” notes Padinjaruveetil. “For example, security leaders who came up through the infrastructure and technology services worlds habitually use overly technical language. People respond to stories – there’s power in connecting information security narratives to business implications.”

Beyond communicative shifts, CISOs must also reengineer their leadership. “When we have a seat in the C-Suite, we’re no longer just subject matter experts, we’re leaders,” emphasizes Jim Routh, former CISO for MassMutual, American Express, DTCC, and Aetna.

Routh points out a critical difference for effective CISOs, “As a subject matter expert, you just tell others what the enterprise cybersecurity priorities are. The problem is, when financial resources dry up, the board pushes back, or competing priorities crop up, the support you thought existed from the stakeholders dissolves.” Effective CISOs have to facilitate consensus on the allocation of scarce enterprise resources to the highest risks. Facilitators have to demonstrate an unbiased perspective (neutrality) to facilitate consensus.

Beyond boosting performance, cultivating this leadership may reduce personal and professional liability. While corporate law entitles company officers to indemnification, by facilitating broader executive participation in decision-making, CISOs show a clearer case of having acted in the best interests of their respective corporations.

As recession looms and cybersecurity risks grow, we expect that outperforming enterprises will be the ones that cost-effectively improve security postures. This hinges on CISO and C-suite togetherness.

HOW TO RESPOND TO THIS TREND:

- Link cybersecurity discussions to broader organization outcomes. Too few security leaders dedicate sufficient time to truly understanding how a business works and cannot prepare leaders, minimize disruptions, or become the “connective tissue” to mitigate risks or capture opportunities.

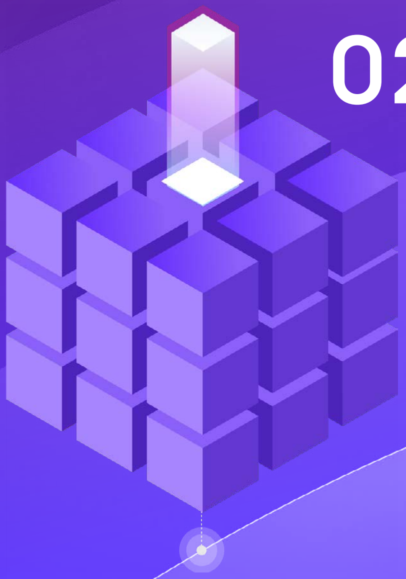
- Stop the information dump. “CISOs keep generating detailed charts, dump them into 50-page slide decks and throw them at other executives,” says Sam Olyaei, VP Team Manager, Gartner.

- Communicate the need to elevate the CISO role, and fight against the tendency for non-information security tasks including IT mismanagement, business continuity, or privacy to end up under this leader’s purview.

TREND NO. 02

Rapid Uptake of Cyber Insurance

HOW TO RESPOND



> In 2023 and beyond, we expect pronounced supply and demand tension within this space. C-suites with meaningful technology exposure will build cyber insurance plans into their risk management practices.

INTRODUCTION

Spurred by the pace and scale of cyberattacks and a growing need for risk transfer, RBC Capital Markets calls cyber insurance the most “rapidly evolving sector in the insurance industry in the last decade."

Cyber insurers **provide coverage** for cost and other liabilities stemming from intrusions and extortion threats, data breaches, network or security wrongful acts, denials of service, and network outage situations.

For some, cyber insurance is a critical means of transferring operational risk. Policies are sought with provisions that may also cover issues like:

- Ransom payments to restore data access
- Customer and employee lawsuits due to privacy breaches
- Lost income from network outages
- Regulatory fines
- Public relations and reputation restoration costs

Alarmingly, the growing volume of cyber threats now **pressures insurance** availability.

> **“While more attacks could stimulate demand, they also create a supply problem, making insurers wary of providing coverage and reinsurers (who provide insurance for insurance providers) less interested in backing cyber liabilities.”**
>
> **Harvard Business Review**

In 2023 and beyond, we expect pronounced supply and demand tension within this space. C-suites with meaningful technology exposure will build cyber insurance plans into their risk management practices. However, we may see insurance companies pull back commitments, raise premiums, or tighten coverage thresholds before providing coverage.

Because the most significant cost factor in insurance coverage is policyholder risk profile, identity security leaders need to execute access management diligently. Before underwriting coverage, for instance, AIG produces **comprehensive reports and grades** around an enterprise’s risk controls including, data protection, controlled use of administrative privileges, secure software configuration.

Cyber insurance is an important risk lever, but insurers are in the driver’s seat – dictating coverage based on perceived levels of exposure and maturity of cybersecurity and privacy controls. We expect a growing desire for insurance, but potential limitations given weak security postures and policy availability issues.

HOW TO RESPOND TO THIS TREND:

- Maximize your “insurability” by investing in robust defensive cyber policies, controls, monitoring, and employee training.
- To reduce accessibility concerns, consider partnering with a cloud services provider that uses data-powered underwriting policies and has direct bid connections to preferred insurers.

TREND NO. 03

Machine Identities and an All-Out Assault on APIs

↓ HOW TO RESPOND

INTRODUCTION

"Since most organizations have not extended governance over who controls an API, our expectation is that solutions for continuous API risk monitoring and granular, policy-driven access management will be in demand."

Last year, we highlighted the explosive growth of non-human user identities. A typical enterprise now has 250,000 machine identities. Predictably, cyber criminals have exploited the expansion: cyber attacks that misuse machine identities increased by 1,600% over the last five years.

Within the machine identity landscape, API prominence is growing. APIs enable machine to machine communication and act as nexus points for information and secure data transfers. These interface points allow data and applications to connect with internal or external systems.

Now, notable API insecurities at Optus, John Deere, Coinbase, and others have thrust this attack vector into the mainstream.

Given the role APIs play in digital transformation (as well as growing use of cloud native applications built on microservices spawning APIs and machine identities) we expect intense scrutiny of API security in 2023.

According to one **report**, APIs remain "the most exposed component of a network, are predisposed to DoS attacks, and easy to reverse-engineer and exploit." Insecure APIs present easy access points for otherwise secure hardware, applications, or networks – and they are notoriously difficult to track and control, particularly in multi-cloud environments.

More than ever, enterprises are asking these types of questions to security partners and vendors:

- What application or business is using the API and associated machine ID?
- Who is the responsible owner?
- What access level (including privilege) is currently assigned?
- How wide is the scope of data being pulled by the identity?

Since most organizations have not extended governance over who controls an API, our expectation is that solutions for continuous API risk monitoring and granular, policy-driven access management will be in demand.

Likewise, as enterprises harden APIs, adjacent machine identity insecurities (like around robotic process automation [RPA] bots and service accounts) will shift into the security purview.

In general, machine identity use exposes cracks in manual management effectiveness. Our view is that enterprises will start evaluating tools for automated discovery, removal of embedded credentials, and self-adjusting authentication.

Ultimately, the most secure organizations will embrace a Zero Trust ethos and remove implicit trust from **all facets** of computing infrastructure.

HOW TO RESPOND TO THIS TREND:

First, focus on discovery and machine identity inventorying efforts. Enterprises cannot manage what is invisible to them.

Next, classify risk based on identity type and prioritize governance through a risk-lens. "Enterprises must establish risk classification because not every machine identity usage has the same risk exposure level," guides KPMG LLP's Rai. "For instance, sending sensitive data to the cloud via APIs is likely riskier than internal data translation using RPA bots."

TREND NO. 04

Filling Identity Security Gaps with IDR

↓ HOW TO RESPOND

> "By incorporating identity-based risk signals, enterprises **boost the effectiveness of their threat detection** and response capabilities and maximize their internal cybersecurity talent."
>
> **Jeff Margolies**
> *CSO at Saviynt*

INTRODUCTION

From Solar Winds to Uber, an unfortunate series of high-profile attacks using privileged access proves the claim: "identity is the new security perimeter." Underscoring this is growing interest in identity detection and response (IDR), a security method designed to confront credential and entitlement vulnerabilities in real-time.

As CyberRisk Alliance **shares**, most identity security practices are primarily preventative. For instance, enterprises may safeguard privileged credentials in PAM solutions or secure authentication processes with MFA and IAM tools.

Alongside this, Laxman Tathireddy, Advisory Principal at Deloitte & Touche LLP, highlights limited focus on identity within many enterprises' detective controls and capabilities: "Too often, identity centricity has been focused on supplying identity context for individual incidents. The ability to understand advanced identity threat detection use cases such as privilege escalation is limited, particularly with popular point solutions."

From issues like these, when an identity-based breach occurs, companies may lack reactive response capabilities.

IDR advances identity defense by automatically surfacing unmanaged, misconfigured or other exploitable identity risks. This can include **detecting** entitlement exposures, credential misuse, and privilege escalations that suggest a breach. Once potentially malicious behavior occurs on a corporate network, security leaders can restrict or terminate the identities exhibiting questionable behavior.

Presumably, IDR fills the security gap when cyber attackers have accessed a target, but before they destructively span networks and consummate attacks using lateral movement.

As IDR solutions emerge, we expect basic remediation functionality at first. To maximize the data and intelligence that IDR brings – particularly within the broader extended detection and response (XDR) function – practitioners need reskilling.

“Forward-thinking enterprises will invest in data science capabilities to effectively extract knowledge and offer predictive insights. This may require retraining or reassessing hiring profiles, especially as threat sophistication grows,” offers Routh.

While even early IDR applications add usefulness, to achieve solution potential, Charlie Jacco, Principal, KPMG LLP, suggests that tools must do more than just simplify analysts’ workflows.

“The fear is that IDR becomes another ingredient in a muddled ‘DR-soup.’ There’s not enough triage analysts on the planet right now who understand identity security. The silver bullet will be deep connections between identities and network information leading to an orchestrated, automated, identity-related security response.”

HOW TO RESPOND TO THIS TREND:

- **Resist the idea that preventative security measures are enough. “Breaches are inevitable. Although IDR solutions are still nascent, the insights they deliver will build your detect-and-respond capabilities. Enterprises must divert some resources from ‘protect’-only thinking,” shares Jacco.**

- **During deployment, maximize IDR potential by integrating with authorization systems native to your applications, cloud resources, infrastructure, and OT.**

TREND NO. 05

Advancing Permission Management with Policy-Based Access Controls

↓ HOW TO RESPOND

"Many organizations have non-comprehensive or fragmented authorization management practices and technical controls, which can **increase both the complexity and cost** associated with mitigating, managing, and governing access risk."

Rajesh Radhakrishnan
Managing Director
Deloitte & Touche LLP

INTRODUCTION

In early 2022, we predicted operationalizing of long-discussed Zero Trust initiatives. As these unfolded last year, ineffective access controls proved a hindrance for many.

Krishna Dasari, Managing Director, Digital Identity at Accenture Security notes how enterprises still often 'safeguard' themselves with complex, perimeter-based security controls. According to Dasari, these fail given dynamic infrastructure environments and also crimp productivity for dispersed workforces. “The key security gap today is the use of static controls or rules engines–modern enterprises need more dynamic policies, including real time creation, deployment, and attestation.”

To support Zero Trust progress, many security leaders feel pressure to swap static entitlement management processes with more dynamic ones. Rajesh Radhakrishnan, Managing Director at Deloitte & Touche LLP, regards this as important with respect to efficiently and affordably pursuing least privileged access:

> **“Many organizations have non-comprehensive or fragmented authorization management practices and technical controls, which can increase both the complexity and cost associated with mitigating, managing, and governing access risk.”**
>
> **Rajesh Radhakrishnan, Managing Director at Deloitte & Touche LLP**

Alongside Radhakrishnan and others, we foresee growing interest in more contextual, smarter policy-based access controls (PBAC).

KuppingerCole **acknowledges** how PBAC environments boast 'built-in' agility and improve security postures for companies operating with varied IT environments – including on-premises services (legacy line-of-business applications), IaaS, cloud-based apps, and multi-cloud deployments.

Ostensibly, the shift improves management with centralized rules and policy creation and management. However, Saviynt's Yash Prakash shares how security leaders will confront how these policies actually cascade into their various security tools.

> **"While simplifying governance and enforcing consistent entitlements is admirable, enterprises must still deal with how policy-based access controls interact at actual enforcement points.**
>
> **Companies desire centralized management capabilities, but implementation remains siloed. Security leaders still must dig to see how a centralized policy is applied across the IT tools a user has access to."**
>
> **Yash Prakash, Chief Strategy & Marketing Officer at Saviynt**

In 2023, we expect new marketplace solutions as well as more creation and adoption of open source standards to support policy-based controls throughout the security stack.

The Secure Production Identity Framework for Everyone (SPIFFE), for instance, **defines a** standard to secure workloads individually without tying them to a specific host or environment. According to CIO Magazine, SPIFFE and similar **open source software** help organizations "go beyond a mere superficial approach to Zero Trust," by creating a "platform agnostic way to define, grant, and destroy identities for workloads at scale."

The recently published Identity Query Language (IDQL) Standard **simplifies CloudOps** across multiple clouds with an abstraction layer for identity and access control policies. The standard connects to cloud systems, determines the resources and policies that exist, translates them to IDQL, and then, upon orchestration, publishes translated policies into the target environment.

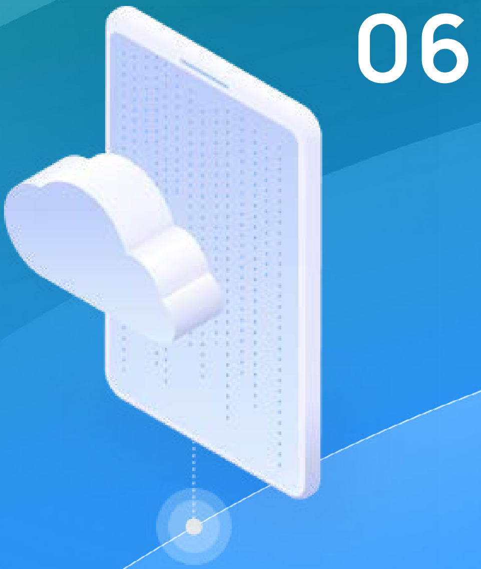
As enterprise IT architecture complexity grows, more policy layers will add insecurity. Conversely, smartly orchestrated policies could increase flexibility, improve security, and decrease spend. Time will tell to what degree these can be implemented.

HOW TO RESPOND TO THIS TREND:

- Evaluate a modern control authorization and entitlement platform (in particular, when migrating to the cloud). Keep in mind that PBAC platforms are relatively new and persist with some static control use.
- Where possible, deploy emerging open source tools (like Hexa and SPIFFE) to ease identity and access management efforts across cloud platform components.

TREND NO. 06

Planning for a Post-Quantum Cryptography Future



↓ HOW TO RESPOND

> "Too few enterprises grasp their future vulnerability because they haven't completed simple discovery or inventory activities."
>
> **Dustin Hoff**
> *Global Partner*
> *IBM Security*

INTRODUCTION

Of all the alarming cybersecurity scenarios imaginable, Quanta Magazine **recently described** a most unsettling one:

> If today's cryptography protocols were to fail, it would be impossible to secure online connections — to send confidential messages, make secure financial transactions, or authenticate data. Anyone could access anything; anyone could pretend to be anyone. The digital economy would collapse.

As quantum computing advances, encryption methods once considered unbreakable find themselves vulnerable. Experts call it "Q-day"–or the day when quantum computers **finally break** the Internet.

As concerns mount, the U.S. Department of Homeland Security (DHS) and the Department of Commerce's National Institute of Standards and Technology (NIST) released a **post-quantum cryptography roadmap** to help organizations identify and protect vulnerable data, algorithms, protocols, and systems.

Although quantum computers present vast risk, IBM **points out** how expanded computing power also creates new opportunities to harden security postures, including deploying quantum-era cybersecurity to detect and deflect cyber attacks –

> "Quantum cybersecurity can provide more robust and compelling opportunities to safeguard critical and personal data than currently possible. It is particularly useful in quantum machine learning and quantum random number generation."

Unfortunately, security leaders often find themselves preoccupied with more tangible cyber threats, and ignore hardware and system assessments with respect to quantum risks.

Dustin Hoff, Global Partner at IBM Security, warns of shocking unpreparedness: “Too few enterprises grasp their future vulnerability because they haven’t completed simple discovery or inventory activities.”

While Hoff disagrees that quantum computing is fundamentally hostile, he urges enterprises to create a basic encryption roadmap to ensure “system agility so that security practitioners can upgrade cryptographic protocols when needed to maintain quantum resilience.”

These reviews must be pre-planned, as required cryptographic upgrade processes from public key infrastructure (PKI) to post-quantum cryptography (PQC) for large enterprises or government agencies **may take years**.

Quantum computing power offers transformative business opportunities. But myriad system and communication security upgrades are tied into taking advantage of these capabilities. Transitions represent the **largest upgrade cycle** in computer history, and all public-key encryption needs to change to provide a completely quantum resilient ecosystem.

As the superhero adage goes, "With great power comes great responsibility." Enterprises can anticipate newfound compute capabilities, but must also prepare to resist advanced threats. The hardening should start now.

HOW TO RESPOND TO THIS TREND:

- Consider an IT estate audit to discover and inventory where encryption is applied and where upgrades need to take place to grow quantum protection.
- Consider implementing hybrid (or crypto-agile) security approaches combining NIST’s standardized algorithms with traditional encryption to ensure backward compatibility and interoperability.

TREND NO. 07

(Shift) to the Left, to the Left

↓ HOW TO RESPOND

> "For many, deploying disparate tools and technologies to shift security left actually creates more blind spots. Demand is growing and I anticipate a wave of packaged, automated solutions emphasizing consumability and accessibility."
>
> **Lalit Ahluwalia**
> *CEO and Global Cybersecurity Head*
> *Inspira*

INTRODUCTION

An article detailing a recent white-hat continuous integration/ continuous deployment (CI/CD) pipeline exploit cheekily begins, "*It always starts with an S3 bucket*." Of course, the point is not to indict AWS. The story only symbolizes the relative ease of CI/CD exploits and how a small misconfiguration in an upstream cloud resource can lead to a devastating compromise.

According to **research from** SlashData and the Continuous Delivery Foundation, nearly 60% of enterprise developers use CI/CD delivery in their workflows. Of these, 11% deploy code changes multiple times per day, while 19% deploy changes anywhere from once per hour to once per week.

While CI/CD promotes speed, it expands the threat surface for malicious actors. In particular, threat vectors extend as varied code, open-source software, data sets, containers, and cloud-infrastructure are put to use. Given this, widespread shift-left campaigns are underway.

Shift-left security means incorporating security both earlier – and within every layer of the software supply chain. Deployment haste invites a range of issues like poorly vetted integrations leading to insecure code, poisoned pipeline execution (PPE), or deficient pipeline-based access controls.

But without specific security measures, including software supply chain inventorying via a software bill of materials (SBOM), shift-left remains a hollow ideal. With an SBOM, enterprises can understand the first and third-party software components in use within the software supply chain and map potential risks.

With Log4Shell and SolarWinds top of mind, the White House remains committed to improving the security of software vendors supplied to federal agencies, in particular, ensuring software component transparency. While security practitioners say executive orders thrust the idea into the security zeitgeist, some **are cautious** about overstating SBOM benefits: "It's a data layer–and that's all it is," suggests Allan Friedman, Senior Adviser and Strategist at the Cybersecurity and Infrastructure Security Agency.

The notion of shifting left is not new; yet, breach volume continues to swell. Lalit Ahluwalia, CEO and Global Cybersecurity Head at Inspira points to enterprises' flawed shift-left approaches as a key reason:

> **"Moving security upstream has degenerated into stuffing a mix of products, processes, and security solutions earlier in the cycle. This isn't a genuine shift-left strategy incorporating security by design in the DNA of the software development cycle. We must stop expecting developers to understand functional security requirements, threat vectors, and business risks in a vacuum. Adoption and integration is a team sport."**

Regarding the near term future for shift-left products, Ahluwalia believes that solution providers will prioritize simplicity and automation. "For many, deploying disparate tools and technologies to shift security left actually creates more blind spots. Demand is growing and I anticipate a wave of packaged, automated solutions emphasizing consumability and accessibility."

HOW TO RESPOND TO THIS TREND:

- Recognize the tendency to overlook supply chain risk. Consider ongoing component analysis; start with SBOM to develop a baseline view and implement a plan to regularly identify your dependencies.
- Understand crucial identity security implications within shift-left efforts. For instance, distinguish who (or what) accesses code repositories or CI/CD tools used by human or machine users.
- Do not assume security is the responsibility of the developer. Business, application, and functional teams must identify supply chain risks and mitigate them together.

TREND NO. 08

Breakthroughs to Normalize and Unify Threat Data

HOW TO RESPOND

"Governments possess a unique ability to make frameworks like this stick by leveraging directives, regulations and fines. If they can find the right balance and connect appropriately to both public and private sector goals, this initiative offers tremendous potential against increasingly coordinated cyberthreats."

Vibhuti Sinha
Chief Product Officer
Saviynt

INTRODUCTION

We previously highlighted progress around coordinated threat intelligence (TI) sharing. While we remain encouraged by signs of vendor collaboration, issues like rapid application growth and incompatible risk signal formats still reinforce TI silos inside most organizations.

However, as 2023 unfolds, an interesting shift is underway.

Leading enterprises appear ready to coalesce around a goal to standardize the data that cybersecurity tools generate. The effort signals an advantageous “the whole is worth more than the sum of its parts” security dynamic.

Recently, Amazon Web Services (AWS), Splunk, CrowdStrike, Palo Alto Networks, Rapid7, and JupiterOne announced the release of **Open Cybersecurity Schema Framework (OCSF)** project. CSO Online highlights the importance of this new framework:

> **“The announcement acknowledges the problem of security professionals needing to wrestle with proprietary data formats and outputs rather than their actual roles of risks and threats [...] By standardizing on security product schemas and formats, security practitioners can spend more time addressing threats that pose risks to organizations.”**

In particular, **OCSF delivers** a sought-after extensible framework for developing schemas and includes a vendor-agnostic core security schema. Industry observers

note that this “Rosetta Stone” for risk information is an important step to coordinate the growing variety of tools and platforms – and help CISOs compile a comprehensive view of IT environments.

While this isn’t the first attempt at better shared intelligence (STIX and TAXII come to mind), it is the most robust in terms of major cybersecurity provider and practitioner cooperation.

Moving forward, we are cautiously optimistic about the potential to bridge organization silos and collectively improve security efforts regardless of industry. However, security teams must do more than just ingest information and leech off the schema – they must commit to sharing as well.

To this point, Vibhuti Sinha, Chief Product Officer at Saviynt advises that eventual success may require outside intervention:

“Governments possess a unique ability to make frameworks like this stick by leveraging directives, regulations and fines. If they can find the right balance and connect appropriately to both public and private sector goals, this initiative offers tremendous potential against increasingly coordinated cyberthreats."

HOW TO RESPOND TO THIS TREND:

- Participate with an industry-specific Information Sharing and Analysis Center (ISAC) to normalize data sharing about cyber threats and mitigation.
- Consider adopting OCSF. For cybersecurity vendors, contribute to the framework to reduce integration debt, improve schema definition, and spur adoption.
- Temper expectations of a panacea with respect to managing multiple security solutions. OCSF adoption and tool integrations will take time.

Conclusion

From expanding threat landscapes to looming economic slowdowns, one thing is sure: The job of security leadership will only intensify in 2023. The unknowns will be a source of stress, but within the high-stakes work is an opportunity to make a meaningful difference.

While we contemplate the future of threats, CISO leadership tactics, machine identity security, coordinated data sharing, and needed responses, the point isn't whether we agree or disagree about eventual outcomes.

Instead, we ought to reflect on the trends and proposed responses to assess our readiness.

Will we embrace a status-quo, business-as-usual mindset this year?

Or will we ruthlessly prioritize, getting ahead of the security curve to ready our businesses for what's next…whatever that is?

After all, how we respond today dictates how we perform tomorrow.

SAVIYNT

Want to talk to an identity and security expert?

SCHEDULE A CALL