Highlights

[It's a Bad Week to be Microsoft (or Last Couple of Years?)]
[Cybersecurity Startups Banks with SVB]
[Forbes Guidance: 15 Cybersecurity Protocols E-Commerce Companies Need to Follow]
[Cerebral Valley: Co-working & Co-living Communities in SF]
[Webinar Schedule]
[Upcoming Conferences]

It's a Bad Week to be Microsoft (or Last Couple of Years?)

Posted by Mike Heumann, March 17, 2023

We all have become accustomed to Microsoft's "Patch Tuesdays", where the weekly batch of bugfixes are put out. This week, Microsoft released some big ones, releasing fixes for over 80 windows security flaws. One of the most pronounced flaws addressed in this release was CVE-2023-23397, an already-exploited critical defect in Microsoft Outlook. According to a variety of sources, this security flaw allows specially-crafted emails to exploit user credentials from Outlook (specifically the Net-NTLMv2 hash), allowing the attackers to log onto an Exchange Server as the exploited user. Most interestingly, this bug can do as soon as the email hits the Outlook client, before the user opens the sees it in the Preview Pane. As usual, Microsoft's security response center provided only the barest details on this bug, with no indicators of compromise (IOC) information that would allow defenders to identify infected machines.

Also of interest was the CVE-2023-24880 exploit that Microsoft identified this Tuesday. This exploit allows attackers to actively bypass Microsoft's SmartScreen feature. SmartScreen, which is an extension of Microsoft Defender for the Microsoft Edge Web Browser, was intended to stop web-based phishing attacks (including downloaded malicious code). However, SmartScreen has turned into vector for malware – this is the second exploit to take advantage of its's weaknesses (CVE-2022-44698 was the first one). The specific attack methodology that the CVE utilizes is bypassing of the Mark-of-the-Web (MOTW) security feature, which forces web pages to execute in security zone, which has been extended to other internet payloads such as files. Once MOTW is bypassed in SmartScreen, malicious payloads such as ransomware can be delivered through the unopened email. The The primary use of CVE-2023-24880 is to deliver the Magniber ransomware package, and it is believed that this weakness has been utilized to deliver roughly 1,000 malware packages to targets in the European Union.

Both of these exploits are indicative of a larger problem – that of "narrow" patches that enable attackers to build slight variants of the original exploit to get around the patches. While these narrow patches have the advantage of being able be developed and tested quickly, they do allow new exploits to be created just as quickly, as evidenced by CVE-2023-24880 (itself a variant of CVE-2022-44698).

Bret Arsenault, Chief Information Security Officer (CISO) at Microsoft likes to say, "Hackers don't break in, they log in."

A final issue identified was the increasing use of Microsoft OneNote to promulgate malware. Unlike the Microsoft Edge example above, OneNote does not utilize the MOTW indicator, making OneNote a great carrier for malicious payloads. While Microsoft silently patched this OneNote issue in January, the patch is not perfect. As a result, OneNote is quickly becoming a method of choice for the delivery of infected payloads, including remote access trojans (RATs), form stealers, and other credential stealers such as Quakbot/Qbot/Pinkslipbot. The only effective mitigation strategy relies on users to not open attachments that are from unknown sources.

Actually, 2021 and 2022 were also bad years (if not worse years) for Microsoft. Some of the more notable exploits during those two years include:

- March 2021: Exchange server vulnerability CVE-2021-26855
- June 2021: Six serious zero-day exploits patched (CVE-2021-33742, CVE-2021-31955, CVE-2021-31956, CVE-2021-33739, CVE-2021-31201, CVE-2021-31199)
- July 2021: PrintNightmare vulnerability (CVE-2021-34527)
- August 2021: Exchange Autodiscover vulnerability (credentials leakage); Microsoft Azure database service unrestricted access flaw
- September 2021 (a REALLY bad month): MSHTML vulnerability (CVE-2021-40444); disclosure of several “non-exploited” vulnerabilities (CVE-2021-36968, CVE-2021-38647, CVE-2021-36965, CVE-2021-36952, CVE-2021-38667, CVE-2021-36975, CVE-2021-38639); APT exploitation of ManageEngine Component of Active Directory (CVE-2021-40539); APT29/CozyBear targeting of Microsoft AD Federation Services
- January 2022: Exchange Server remote execution vulnerability (CVE-2022-21846)
- February 2022: SharePoint vulnerability (CVE-2022-22005)
- March 2022: HEVC Video Extensions remote code execution (CVE-2022-22006)
- April 2022: PrintNightmare local privilege escalation (CVE-2022-26796)
- May 2022: Windows NFS remote code execution (CVE-2022-24491/CVE-2022-24497)
- June 2022: LSA Spoofing Vulnerability (CVE-2022-26925); Internet Explorer component reuse vulnerabilities.
- July 2022: More zero-day vulnerabilities (CVE-2022-22047)
- August 2022: More Exchange Server vulnerabilities (CVE-2022-21980/CVE-2022-24516/CVE-2022-24477)
- September 2022: Windows TCP/IP remote code execution (CVE-2022-34718)
- October 2022: Workaround guidance for actively exploited Exchange Server vulnerabilities (CVE-2022-41033)

- November 2022: Exchange server patches; print spooler update (CVE-2022-41073); out-of-band Kerberos authentication issues

I have always been a used Microsoft products (since early MS-DOS in 1985!), but for a company with over $200B in revenue, and more than 100,000 software engineers as of July 2021, this is an awful security record. Seems like all of us that are Microsoft subscribers are paying Microsoft to be (at best) beta testers….Ah, I could implement Microsoft Defender!

Cybersecurity Startups Bank with SVB

Posted by Karen Heumann, March 17, 2023

As we reported in our March Enterprise Storage and Technology newsletter, Silicon Valley Bank (SVB) surprised investors with news that the bank needed $2.25B to correct its financial deficiencies. The news caused panic and a massive sell-off resulting in the second-biggest bank collapse in US history. Customers withdrew $42B by the end of the next day, according to a California regulatory filing, decimating the remains of the 40-year-old investment bank, and leaving SVB with a negative cash balance of $958M. The California Department of Financial Protection and Innovation closed SVB, seized remaining cash deposits, and named the FDIC as receiver.

Rob Ackerman, Founder and Managing Director of AllegisCyber Capital, says that virtually every venture firm was engaged with SVB at some level — be it the venture firms themselves or their portfolio companies banking at SVB. And within the security community, they were vital to the banking and financing needs of the sector in the US, Israel, and the UK. "Financial support in the form of lines of credit and venture debt is going to become much more difficult [for startups] to come by," says Ackerman. "SVB was the leading source of that financing and with them gone, the slope of the hill for young startups just became that much more difficult."

Reports indicate that at least 500 cybersecurity vendors banked with SVB. Silicon Valley Bank's willingness to lend money to venture-backed startups with limited cash flow has made the institution appealing to cyber vendors. CrowdStrike established a $150M revolving line of credit with SVB in April 2019, two months before their initial public offering. In January 2021, CrowdStrike expanded the credit

line to $750M and pushed the maturity date out from 2022 to 2026. Sumo Logic had a credit line with SVB since January 2016 and borrowed $24.3M.

CyberWire provides a summary of the factors leading to the SVB fall:

> "SVB catered mainly to the insular ecosystem of startups and the investors that fund them," the Wall Street Journal reported. "Its deposits boomed alongside the tech industry, rising 86% in 2021 to $189 billion and peaking at $198 billion a quarter later. The bank poured large amounts of the deposits into U.S. Treasuries and other government-sponsored debt securities."
>
> Silicon Valley Bank invested heavily in long-term US Treasury bonds at a time when the Federal Reserve had established low interest rates. Bloomberg observes that, "SVB took in tens of billions of dollars from its venture capital clients and then, confident that rates would stay steady, plowed that cash into longer-term bonds."
>
> Most investors missed signs of trouble, but some short-sellers had begun to take an interest in Silicon Valley Bank in January, Bloomberg reports. "They had bought all these mortgages at the top of the market and were sitting on a massive unrealized loss," one of the shorts, William C. Martin, told Bloomberg. "And it was sitting there in plain sight. There were a number of other banks and insurance companies with similar issues, but I haven't seen anyone anywhere near the scale of Silicon Valley Bank." A combination of fixed-income exposure and dependence on volatile venture-capital-backed depositors rendered the bank especially vulnerable.

"They were the gold standard, it almost seemed weird if you were in tech and didn't have a Silicon Valley Bank account," Stefan Kalb, CEO and Co-Founder of Seattle startup Shelf Engine, said during a Monday interview as he started the process of transferring millions of dollars to other banks.

Forbes Guidance: 15 Cybersecurity Protocols E-Commerce Companies Need to Follow

Posted by Mike Heumann, March 17, 2023

Forbes gathered experts in all facets of cybersecurity to provide a robust list of protocols for e-commerce companies to follow to provide appropriate cybersecurity measures. 15 members of Forbes Technology Council offer the following recommendations:

1. Implement Privacy By Design

"Privacy by design" implies you don't put the organization in harm's way by collecting or processing data in a way that could lead to a privacy violation. For example, data should be encrypted while at rest and in transit, with the key for that data stored with the user. This way, the processor does not have access to the data without the user being involved and consenting to the transaction. - Michael Engle, 1Kosmos

2. Know And Control Your Data

Every company that collects, processes and/or stores customer information needs to be able to understand the data they have—whose it is, what it is and where it is—and take action to protect it while meeting regulatory compliance. - Dimitri Sirota, BigID

3. Focus On First-Party Data Management

E-commerce companies should be looking at how they create, manage and own first-party data to ensure that it is being protected and that they're complying with local legislation around the globe. Continuing to focus on third-party data strategies or building data partnerships that put consumer data at risk should be frowned upon. - Bill Bruno, D4t4 Solutions

4. Practice Data Rationalization

The low-hanging fruit is data rationalization. Store only the data your business can define value for. You don't need to secure data you don't keep. For data that has a defined value, weigh that value against the cost of keeping it secure, the required cyber insurance and the costs of a breach. If the cost outweighs the value, purge it. - Joe Onisick, transformationCONTINUUM

5. Consider Cybersecurity As Part Of Risk Management

Organizations need to consider cybersecurity as risk management. Establishing a plan for when they will be a target is critical. When an organization starts approaching cybersecurity as a risk-management process, it will realize the need for an established framework that constantly audits the environment. - Chris Schueler, Simeio

6. Buy Access To Or Build Secure Infrastructure

The three questions e-commerce companies must ask themselves are 1. if they need the data, 2. if they do need the data, how they will store it (for example, will it be encrypted), and 3. how they will prevent malicious actors from accessing the data. For the third point, e-commerce companies must use or build secure infrastructure, either by subscribing to an external service or building it in-house. We employ a team of QA analysts and periodically contract white hat hackers. - Greg Soh, RoadFlex

7. Store Only Business-Critical Data

E-commerce companies must base their cybersecurity strategies on a comprehensive data inventory, frequently reevaluating the data they have and continuously monitoring their security posture over time. Storing and securing only business-critical data and eliminating unnecessary data reduces risk, improves performance and lowers environmental impact. - Stephen Cavey, Ground Labs

8. Conduct Regular PII Audits

Smart cybersecurity strategy consists of three key steps: identifying what personally identifiable information applies to your business, determining how this data is stored in encrypted form when at rest, and seeing how data is encrypted when it is in transit. The strategy should involve identifying an in-house subject matter expert who can lead this initiative, spreading awareness of PII among employees, conducting regular audits and optimizing to stay current. - Raja Epsilon, WrkSpot

9. Have An Incident Response Plan Ready

One critical cybersecurity protocol for e-commerce companies is to implement secure data storage. This involves encrypting sensitive customer information, regularly backing up data and implementing strict access controls to prevent unauthorized access to the data. Additionally, companies should regularly monitor their systems for potential breaches and have incident response plans in place. - Satish Shetty, Codeproof Technologies Inc

10. Use Encryption Everywhere

Start with HTTPS within your microservice and externally; this makes sure the data in transit is encrypted. My typical guidance is to keep the data encrypted at all times until it’s ready to be analyzed

or displayed. Routinely rotate the encryption keys, and don't keep data forever—archive it if you have to, using a different encryption key for each step. - Varun Singh, Daily

11. Leverage TLS And AES Encryption Strategies

Data encryption is a must-have cybersecurity protocol for e-commerce firms to secure customer data. It converts sensitive information into code to prevent unauthorized access. Encryption protects against cyberattacks and is a key component of a comprehensive cybersecurity strategy. E-commerce companies should use appropriate encryption methods such as TLS for online transactions or AES for data at rest. - Imane Adel, Paymob

12. Explore Post-Quantum Cryptography

E-commerce companies should encrypt sensitive data during transmission and storage and use the NIST-winning quantum-resistant cryptographic algorithms. Quantum-resistant algorithms and quantum-proof solutions prevent unauthorized access and data breaches. Post-quantum solutions ensure the security of encrypted data against quantum computing attacks and "steal now and decrypt later" attacks. - Tracy Levine, SonKsuru

13. Employ Proper Key Management

It's essential to employ proper key management. The biggest problem companies face today is the disclosure of personal data when a compromise occurs, and the reason behind this is that everyone focuses on encryption solutions. Most regulations state that critical data and/or personal data need to be encrypted, which most companies do; however, they are silent on key management. - Eric Cole, Secure Anchor Consulting

14. Carefully Guard Access To Production Data

Invest in encryption in transit and at rest, especially for personally identifying information (TLS/AES-256). Ensure only the right personnel have access to production data. Add a layer of application and/or database encryption and decryption for very sensitive data (such as credit cards, Social Security numbers and so on). - Sreenivasan Iyer, Antares Vision Group (RfXcel)

15. Look For A Robust Data Security Tool

E-commerce companies handle large amounts of sensitive data, like personally identifiable information, making them vulnerable to criminals. The volume of transactions and the use of various cloud platforms create further vulnerability. They need a robust data security tool that provides complete visibility into their data security posture, including data usage and access inventories. - Liat Hayun, Eureka Security

Cerebral Valley: Co-working & Co-living Communities in SF

Posted by Karen Heumann, March 17, 2023

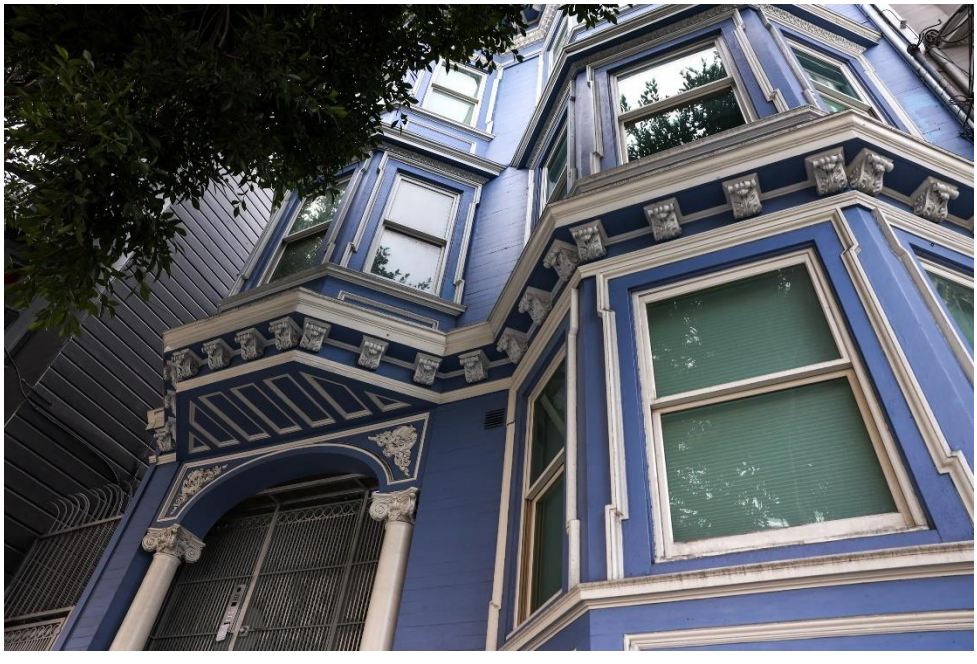
Cerebral Valley is an area of San Francisco, in the Hayes Valley neighborhood, where AI techies are forming coworking and co-living communities. Genesis House is lauded as the hottest hacker spot in the city, a 21-bedroom collective founded in March 2021 and operated out of a bright-blue Victorian home.

Amber Yang, an AI investor with Bloomberg Beta who popularized the term Cerebral Valley, explains that "OpenAI has almost democratized and made it easier to build these smaller companies," "People want to move fast, and there's lots of competition. Whoever is going to win is going to be who gets to the market faster—and who gets to the market faster will be determined by team culture, dynamics and being in person." "They're like, I would willingly work seven days a week in person and live with these people," said Yang. "Many people who, in the last few months, had been saying that SF is dead are now feeling like it's really stupid if you're not in SF and working on AI," said Yang. "The quality and caliber of AI startups in communities outside of SF just can't compare."

"Compared to Covid, when everywhere was restricted and there were no events, right now the speed is so much faster and more exciting," said Sofiia Shvets, the CEO and Co-founder of Claid, who once lived in an eight-person founder's house. "We're seeing more and more hacker houses appear, events starting again and people are moving back to the city because they want to be part of a community again." "The whole idea, especially when you're building something new, is you basically work on that 24/7," Shvets said. "It's not the same when you go to the office, because you have to leave at some point—it's having this 24/7 access, where you can work together with someone until 4 a.m., you discuss something, and that's how ideas get born."

AGI House, run by Rocky Yu, is an eight-bedroom mansion, located in Hillsborough, about halfway between the headquarters for Google and San Francisco-based OpenAI. The allure of events at AGI House is the possibility of meeting Silicon Valley elite. A weekend hackathon attracted 150 Bay Area techies for a marathon coding session to build apps with AI language tools, was sponsored in part by Hugging Face, an open-source AI company valued at $2B, with welcome remarks from Sebastian

Thrun, the self-described godfather of self-driving cars. AGI is short for “artificial general intelligence,” a phrase popularized by OpenAI to describe the idea of AI that is smarter than a human. OpenAI argues that tools like ChatGPT, which can instantly answer questions or generate text like software code and college essays, or the text-to-image generator DALL-E, can respond to a user’s natural language prompt, as steppingstones toward superhuman AI. AGI house was previously called Neogenesis and was started by OpenAI’s Andrej Karpathy, Tesla’s former head of AI who was known for throwing lavish parties with guests like Google co-founder Sergey Brin. The term “AGI” has become a watchword for proponents who share the belief that this technological wave of AI will transform the internet.



Cerebral Valley AI Summit is a one-day, invite-only artificial intelligence summit on March 30 in Cerebral Valley. The Cerebral Valley AI Summit is presented by Samsung Next, Oracle Cloud Infrastructure, NVIDIA, Greylock, akash, felicis, Lambda, Kiarity, Richmond Global, and Rackhouse Venture Capital. The 200 spots are filled but this story is noteworthy because these are the names and companies of the future for AI. If interested, you can subscribe to Newcomer to follow along with the coverage and watch recordings of the summit.

Panelists include (i.e. companies and people to watch): Cristóbal Valenzuela, CEO, Runway; Caryn Marooney, Partner, Coatue; David Luan, CEO, Adept; Gaurav Gupta, Partner, Lightspeed; Caroline Zhang, CEO, Knowtex; Lydia Ding, Co-founder, Code Complete; Clem Delangue, CEO, Hugging Face; Saam Motamedi, Partner, Greylock; Hema Raghavan, Co-founder, Kumo.ai; Deep Nishar, Mng. Dir., General Catalyst; Amber Yang, Investor, Bloomberg Beta; Harrison Chase, Founder, Langchain; Emily Dorsey, Co-founder, Pyq; Amjad Masad, CEO, Replit; Konstantine Buhler, Partner, Sequoia; Adam

D'Angelo, CEO, Quora; Leigh Marie Braswell, Principal, Founders Fund; Miles Grimshaw, Partner, Benchmark; Chun Jiang, CEO, Monterey AI; Medha Basu, Co-founder, Defog; Emad Mostaque, CEO, Stability AI; John Curtius, Founder, Cedar; Lisha Li, CEO, Rosebud; Bucky Moore, Partner, Kleiner Perkins; Shane Orlick, President, Jasper; Yasmin Dunsky, CEO, Wild Moose

The host, Eric Newcomer, provides the following commentary regarding the event:

> It's a big milestone for a 2-year-old Substack that's just me and my chief of staff, Riley Konsella. Generative artificial intelligence is the first hype cycle that I've lived through in Silicon Valley that I've really believed in. Self-driving cars and crypto felt absurd. The shift to mobile had already happened before I started covering tech. On-demand and marketplaces have been less disruptive than many declared that they would be. But generative artificial intelligence companies are showing us the results of their work as they're developing- and regular people get it.

Cerebral Valley AI hosts co-working sessions in start-up offices. Aqeel Ali, a former operations manager who helps organize Cerebral Valley AI, said he barely left his bedroom for two weeks after ChatGPT was released in late November because it was clear the technology could do the work of "eight junior employees." Ali says adopting this type of AI will lead to new jobs, not just take old ones. He pointed to Anthropic's help wanted listing for a prompt engineer (a nontechnical role for people good at talking to AI models) that advertised a salary of at least $250,000. "You want to know why those jobs exist," Ali said. "I just want to find one I'm excited about that I'm good at and that's needed." Ali, recently started his own Hayes Valley group house called Luminance, said there has been a cultural shift since the pandemic back to "community." Event organizers have even opted against a Zoom conference option for talks. "We're trying to maintain a high-fidelity, high-quality experience."

Hacker houses are "symptomatic of when people are just all in on building a company and when people are like trying to immerse themselves and learn from others," said investor Sarah Guo, founder of the early-stage venture capital firm Conviction Partners, who recently attended a dinner at AGI House. "Obviously it doesn't work for people at every life stage in every lifestyle," she explains. But co-living is working for the employees of one of her portfolio companies, Harvey, which is building AI models for law firms, because they're excited about growing their company quickly. "They don't really do anything else right now. They just work," she said.

Moritz Wallawitsch, CoFounder for RemNote, explains “When you live with someone, you’re definitely more at the edge of what’s happening. Things like being introduced to a roommate’s interesting friends, isn’t something you necessarily get at an event,” said Wallawitsch, who introduced a former housemate to one of the investors in his company RemNote, an app for studying and organizing information.

“People are excited by moving fast again,” Yang said. “When you’re remote, especially if you’re like a five-person startup, you just don’t have as much accountability. A lot of my friends working on AI companies in Hayes Valley all sort of live in their office space, they’re just working all the time—and I think that’s super exciting. If you’re living and working with your team all day long, then you’re more incentivized to just grind all the time.”

G2M Research Multi-Vendor Webinar Series

Our webinar schedule is below. We are offering a Cybersecurity series and an Enterprise Storage & Technology multivendor series.

"The Need for Speed: NVMe™, NVMe-oF™, and Data Processing Accelerators" webinar featured Tony Afshary, Vice President, Products and Marketing at Pliops; Rob Davis, Vice President of Storage Technology at NVIDIA; and Peter Onufryk, Intel fellow for NVMexpress. Companies are focused on storage/networking/processing acceleration. Higher-level networking protocols and custom protocols for specific workloads require "offloads" to lower CPU utilization and increase application performance. Advanced storage capabilities such as those offered by NVMe and NVMe-oF can also tax CPUs, reducing cycles available for workloads. And then there is security, data resilience, and other very real needs that take CPU cycles away from workloads. This webinar explored where non-hyperscalers go to accelerate their workload in the same way hyperscalers do. The webinar video is available to view and a copy of the slidedeck is available here.

Interested in Sponsoring a webinar? Contact **G2M** for a prospectus. We can create custom webinar, custom webinar series, and add or modify topics to specifically appeal to your target audience. View our webinars and access slide deck presentations on our website.

Enterprise Storage & Technology

Supercharging Oracle MySQL Performance, Scalability, & Efficiency with Pliops	March 21
Storage Architectures for Artificial Intelligence & Machine Learning	April 4
Software-Defined Flash Memory Architectures	May 9
Storage & Compute Architectures for Healthcare & Imaging Applications	June 27

NVMe & NVMe-oF – Past, Present, & Future	July 11
GPUs, SSDs, & Shared Memory: Accelerating Computing?	August 22
Securing Data – How Storage & Cybersecurity Technologies Can Work Together	Sept 26
The Open Compute Platform (OCP) Movement – Providing Compute-At-Scale Value to On-Premises Deployments	October 24
Storage Architectures for HPC Clusters	November 21
2024 Trends – Cloud, On-Premises, & Hybrid Compute/Storage	December 12

Cybersecurity

The Increasing Complexity of Cybersecurity Regulatory & Compliance for the Financial Services Industry	May 25
xDR- The Promise versus the Reality	August 3
10 Features of an Effective Attack Surface Management Tool	September 7
How Secure is the Cloud for Your Workloads?	October 12
Do You Need a SIEM? Use Cases Where a SIEM Makes Sense.	November 9

Upcoming Conferences

March 20-22	Gartner Data & Analytics Summit, Grapevine, TX
March 20-23	GTC CPU Technology Conference, San Jose, CA
March 28-29	Gartner Security & Risk Management, Sydney, Australia
March 28-31	ISC West, Las Vegas
April 5-7	IST Information Security Expo, Tokyo, Japan
April 15-19	NABShow, Las Vegas
April 17-21	HIMMS Global Health Conference, Chicago, IL
April 17-21	Privacy Symposium, Venice, Italy
April 19-20	CyberSec Europe, Brussels, Belgium
April 24-27	RSA Conference, San Francisco
May 1-3	IAHSS AC&E, Nashville, TN
May 2-4	ACT Expo, Anaheim, CA
May 9-12	Black Hat Asia 2023, Singapore
May 15-17	Forth Roadmap Conference, Portland, OR
May 16-17	SIA GovSummit, Washington DC
May 17-18	Expo Summit Global, Santa Clara, CA
May 21-25	ISC, Frankfurt, Germany
May 22-25	Dell World, Las Vegas
May 22-25	Government Fleet Expo, Dallas, TX

June 2-6	School Transportation Network Expo East, Indianapolis, IN
June 4-8	Cisco Live, Las Vegas
June 5-7	Gartner Security & Risk Managemnt, National Harbor, MD
June 7-9	Synnex Red, White and You, Greenville, SC
June 11-14	36th Electric Vehicle Symposium & Expo, Sacramento, CA
June 11-16	2023 VLSI Symposium, Kyoto, Japan
June 14-16	Interop Tokyo, Chiba, Japan
June 20-22	HPE Discover, Las Vegas
June 20-22	Info Security Europe, London
July 14-19	School Transportation Network Expo, Reno, NV
August 5-10	Black Hat USA, Las Vegas
August 8-10	Flash Memory Summit, Santa Clara, CA
August 28-31	VMWare Explore, San Francisco, CA
August 30-Sept 1	Security Expo, Sydney, Australia
September 11-13	Gartner Security & Risk Management, London
September 11-13	Global Security Exchange, Dallas, TX
September 18-20	Crowdstrike fal.con, Las Vegas
September 18-21	SDC 2023, Fremont, CA
October 2-4	DattoCon, Miami, FL
October 3-4	CyberTech Europe, Rome
October 16-19	Gartner IT Symposium/Xpo, Orlando, FL
November 15-16	Microsoft Ignite, TBD
Nov 27- Dec 1	AWS re:Invent, Las Vegas