

IAITAM ACE 2025

ITAM - Another Brick In The Wall

**Effectively Secure Your Software
Supply Chain With SBOM Management**





Terry Divelbliss

Sr. VP, Marketing and Technical Alliances

- CSAM, CMAM, CAMSE, CITAD, CAIAM
- IAITAM Member #24
- Avid musician and car guy



April 22-24, 2025 | The M Resort Spa Casino | Las Vegas, NV



About Eracent

- ITAM, SAM and Cybersecurity solutions since 2000
- Headquarters in PA, R&D in Warsaw, global operations
- IT Management Center™ (ITMC)
- IT-Pedia® product enrichment data library
- Cybersecurity Management Suite™ (CSMS)



April 22-24, 2025 | The M Resort Spa Casino | Las Vegas, NV



Software Supply Chain Under Threat

- Ongoing cyber incidents, breaches and hacks
- Current cybersecurity tools aren't stopping them
- Significant threat to the software supply chain
- Largely derived from open source software

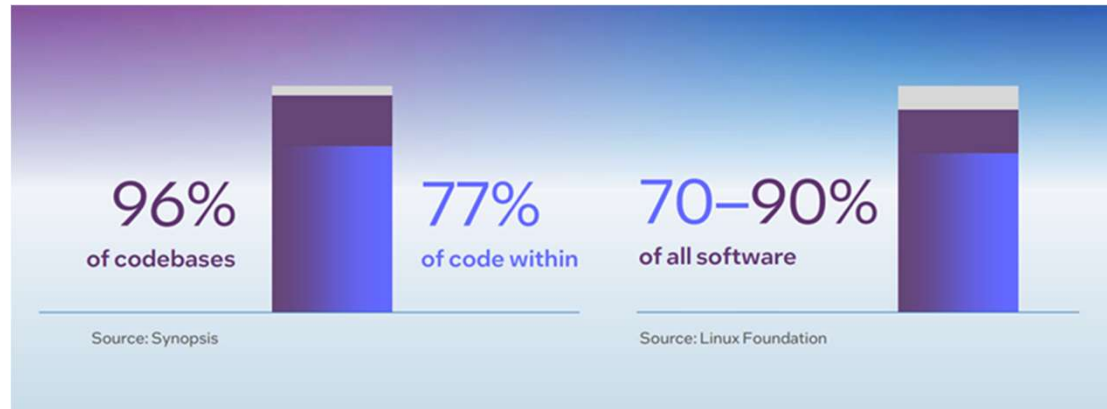


April 22-24, 2025 | The M Resort Spa Casino | Las Vegas, NV



Open Source Software Introduces Risk

- Open Source software is everywhere!



- Potential Vulnerabilities
- Obsolete Code
- License Risk



April 22-24, 2025 | The M Resort Spa Casino | Las Vegas, NV



Threat: Vulnerabilities

- Legacy vulnerability management tools monitor at the product and application level
- They didn't prevent high-profile hacks:
 - Log4j exploit
 - Solar Winds supply chain attack (2020)
 - XZ Utils Backdoor Incident (April 2024)



April 22-24, 2025 | The M Resort Spa Casino | Las Vegas, NV



Why? An Analogy...

- Designed and constructed a building
- Gated complex
- State-of-the-art locks
- Alarm system and cameras
- Protection from external threats, but...
- Nobody checked that door under the basement stairs
- ***Bad actors are already hiding in there.***



April 22-24, 2025 | The M Resort Spa Casino | Las Vegas, NV



Threat: Vulnerabilities

- Components and Libraries can have vulnerabilities
- Behind the scenes, but critical
- Origin point of many hacks and exploits
- Tracked by NIST, GitHub Advisory, OSV, and other trusted organizations



April 22-24, 2025 | The M Resort Spa Casino | Las Vegas, NV



Threat: Obsolete Code

- Very old libraries and code are still used
- May be undermanaged or completely unmanaged
- Can be targeted by hackers



April 22-24, 2025 | The M Resort Spa Casino | Las Vegas, NV



Threat: License Type Risks

- License Types dictate how code may be utilized
- Wide range of restrictions and consequences
 - Permissive licenses
 - Strong CopyLeft licenses
- Legal and financial ramifications
- AppDev teams: Choose wisely!

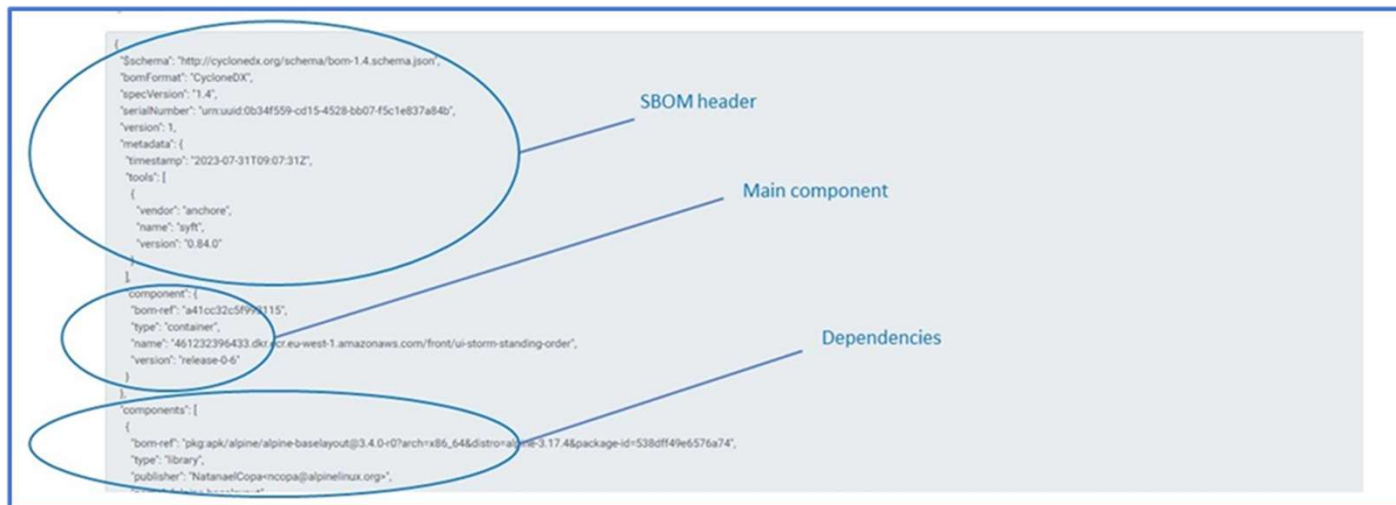


April 22-24, 2025 | The M Resort Spa Casino | Las Vegas, NV



The Software Bill of Materials (SBOM)

- Provides an “ingredients list” of all components and libraries that comprise an application
- Shows the origin of each line of code



April 22-24, 2025 | The M Resort Spa Casino | Las Vegas, NV



SBOM Management

- SBOMs are not new
- App Dev teams use for spot checks
- Use by end-user organizations for security *is* newer
- Embraced by CISA and other global standards organizations
- Different requirements for managing and analyzing contents
 - Software creators
 - Software consumers



April 22-24, 2025 | The M Resort Spa Casino | Las Vegas, NV



Mandates and Directives

- Regulations intended to ensure security of software supply chain
 - Executive Order 14028 (U.S.)
 - Section 3305 - Consolidated Appropriations Act (U.S. / FDA oversight of medical devices)
 - NYS DFS500 (U.S. - any bank conducting business in N.Y.)
 - Network and Information Security directive (NIS2) (EU)
 - Digital Operations Resilience Act (DORA) (EU)
- SBOM use is specifically prescribed
- Organizations must comply with mandates



April 22-24, 2025 | The M Resort Spa Casino | Las Vegas, NV




Structuring SBOM Data for Use

```
{
  "type": "issue-tracker",
  "url": "https://github.com/spring-projects/spring-framework/issues"
},
{
  "type": "vcs",
  "url": "https://github.com/spring-projects/spring-framework"
}
],
"type": "library",
"bom-ref": "pkg:maven/org.springframework/spring-aop@5.3.18?type=jar"
},
{
  "publisher": "spring io",
  "group": "org.springframework",
  "name": "spring-expression",
  "version": "5.3.18",
  "description": "spring expression language (spel)",
  "scope": "optional",
  "hashes": [
    {
      "alg": "md5",
      "content": "240d2a18a4e363082c9748a9663fb7b8"
    }
  ]
}
```

- Impractical to use data as-is
- Huge task to manage one at a time

Upload Status	Processed (Partial)		Processing date	9/4/2024 2:40:26 PM	
Total Reported Components	129	Dependencies	211	Total Added Components	19
Unidentified dependencies count	0	Fixed dependencies count	0	Not recognized components count	1

File Name	bom-Phase-Framework-3-16-1.json				
Publisher	Demo	Line of Business	Phase1	Application Component	RunMeNow
Module Name	phase-frame-parent	Version	3.16.2		
SBom Format	CycloneDX 1.3	Used tool	cyclonedx cyclonedx maven plugin 2.5.3		
Uploaded At	9/4/2024 2:34:43 PM	Uploaded By	Andrzej Biernacki		Source Site



April 22-24, 2025 | The M Resort Spa Casino | Las Vegas, NV



Consolidated SBOM List

	File Name	Application Module	Module Version	Source	Upload Status	Rep.	Deps.	NMC	NC	ND	INV	NB	UD	FD	IC	NRC	VNFC
<input type="checkbox"/>	tensorflowspdx.json	tensorflowspdx	0.9	Site	✓	1	0	⚠	⚠				0	0	0	0	0
<input type="checkbox"/>	Sparkspdx.json	sparcspdx	1.0	Site	✓	1	0	⚠	⚠				0	0	0	0	0
<input type="checkbox"/>	manifest.spdx.json	manifest	1.0 spdx	Site	✓	778	777	⚠		⚠			0	0	2	0	0
<input type="checkbox"/>	core signature-2023.4.0.json	core	2023.4	Site	✓	193	351						0	0	3	58	2
<input type="checkbox"/>	Gnyp-1.0.b.json	Gnyp	1.1b	Site	✓	158	157						0	0	0	143	7
<input type="checkbox"/>	Gnyp-1.0.json	Gnyp	1.1	Site	✓	158	157						0	0	0	155	2
<input type="checkbox"/>	grype_photoshop_sbom.json	Gnyp	1.0	Site	✓	158	157			⚠			0	0	0	155	2
<input type="checkbox"/>	grype_photoshop_sbom.json	Adobe_Photoshop_2024	1.0	Site	✓	158	157			⚠			0	0	0	155	2
<input type="checkbox"/>	Photoshop_dir.cdx (1).json	Adobe_Photoshop_2024	2024	Site	✓	277	276					⚠	2137	0	276	0	0
<input type="checkbox"/>	sbom.json	new	1.0	Site	✓	1	0	⚠	⚠				0	0	0	0	0
<input type="checkbox"/>	core signature-2024.1.0ab.json	lilisig	2024.1.0	Site	✓	196	367						0	0	3	65	2
<input type="checkbox"/>	researchfactor-rp-bdf-2.2.5.json	researchfactor-rp-bdf	2.2.5	Site	✓	196	340						0	0	0	1	2
<input type="checkbox"/>	bom (4).json	dependency-track	4.11.7	Site	✓	185	389						0	0	0	0	0
<input type="checkbox"/>	phase-frame-parent-3.22.9 demo.json	phase-frame-parent	6.3.29.demo4	Site	✓	119	276						0	0	0	1	0
<input type="checkbox"/>	phase-frame-parent-3.22.9 demo.json	phase-frame-parent	3.22.9.Demo	Site	✓	119	276						0	0	0	1	0



April 22-24, 2025 | The M Resort Spa Casino | Las Vegas, NV



Leveraging SBOM Content

- Vulnerability data from NIST NVD, GitHub Advisory, OSV, and other trusted sources
 - Risk scores, levels of criticality, dependencies, and more
- Mitigation and exemptions
- Alerts when new vulnerabilities are reported
- Version tracking and obsolescence management
- Visibility into license types for each component and library
- Associations with applications and installations



April 22-24, 2025 | The M Resort Spa Casino | Las Vegas, NV



Libraries Summary and Details

PkgTyp	Library	Version	Age	Obsolescence	Latest Version	Latest Age	wEPSS	KEV	C	H	M	L	N	T	mV	License Type	Mods	Mm\	mL	MmL
✓	struts2-core	2.5.8	8 years	Not Current and Obsolete	7.0.3	27 days	97.36%	3	13	14	8	0	0	35	2	Apache-2.0	2	1	0	0
✓	log4j-core	2.9.1	7 years	Not Current and Obsolete	2.24.3	3 months	97.11%	2	4	1	3	2	0	10	0	Apache-2.0	1	0	0	0
✓	xstream	1.4.9	9 years	Not Current and Obsolete	1.4.21	4 months	97.31%	1	9	46	15	0	0	70	0	BSD-3-Clause BSD	2	0	0	0
✓	spring-webmvc	5.3.1	4 years	Not Current	6.2.4	3 days	97.45%	1	2	3	2	0	1	8	1	Apache-2.0	2	1	0	0
✓	spring-webmvc	5.2.2.release	5 years	Not Current	6.2.4	3 days	97.45%	1	2	3	2	0	1	8	0	Apache-2.0	1	0	0	0
✓	spring-beans	4.3.29.RELEASE	4 years	Not Current	6.2.4	3 days	97.45%	1	2	1	1	0	0	4	1	Apache-2.0	1	1	0	0
✓	spring-beans	4.3.1.RELEASE	9 years	Not Current	6.2.4	3 days	97.45%	1	2	1	1	0	0	4	0	Apache-2.0	2	0	0	0
✓	spring-beans	3.0.5.release	14 years	Not Current	6.2.4	3 days	97.45%	1	2	1	1	0	0	4	1	Apache-2.0	1	1	0	0
✓	spring-beans	5.3.1	4 years	Not Current	6.2.4	3 days	97.45%	1	2	1	1	0	0	4	1	Apache-2.0	2	1	0	0
✓	spring-beans	5.2.2.release	5 years	Not Current	6.2.4	3 days	97.45%	1	2	1	1	0	0	4	0	Apache-2.0	1	0	0	0



April 22-24, 2025 | The M Resort Spa Casino | Las Vegas, NV



Vulnerability Details and CVEs

Vuln Name	Library Name	Library Version	Age	Vector	KEV	Score	EPSS	Mods	MmV	mV
<input type="checkbox"/> CVE-2021-44228	log4j-core	2.9.1	a month	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H	🔥	10	97.11%	1	0	0
<input type="checkbox"/> CVE-2022-22965	spring-beans	4.3.29.RELEASE	a month	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	🔥	9.8	97.45%	1	1	4
<input type="checkbox"/> CVE-2022-22965	spring-webmvc	5.2.2.release	a month	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	🔥	9.8	97.45%	1	0	4
<input type="checkbox"/> CVE-2022-22965	spring-beans	3.0.5.release	a month	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	🔥	9.8	97.45%	1	1	4
<input type="checkbox"/> CVE-2022-22965	spring-beans	5.3.1	a month	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	🔥	9.8	97.45%	2	1	4
<input type="checkbox"/> CVE-2022-22965	spring-webmvc	5.3.1	a month	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	🔥	9.8	97.45%	2	1	4
<input type="checkbox"/> CVE-2022-22965	spring-beans	4.3.1.RELEASE	a month	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	🔥	9.8	97.45%	2	0	4
<input type="checkbox"/> CVE-2017-5638	struts2-core	2.5.8	a month	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	🔥	9.8	96.02%	2	0	0
<input type="checkbox"/> CVE-2020-17530	struts2-core				🔥	9.8	96.68%	2	1	1
<input type="checkbox"/> CVE-2022-22965	spring-beans				🔥	9.8	97.45%	1	0	4

CVE-2021-44228 Detail

MODIFIED

This CVE record has been updated after NVD enrichment efforts were completed. Enrichment data supplied by the NVD may require amendment due to these changes.

Description

Apache Log4j2 2.0-beta9 through 2.15.0 (excluding security releases 2.12.2, 2.12.3, and 2.3.1) JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. From log4j 2.15.0, this behavior has been disabled by default. From version 2.16.0 (along with 2.12.2, 2.12.3, and 2.3.1), this functionality has

QUICK INFO

CVE Dictionary Entry:

CVE-2021-44228

NVD Published Date:

12/10/2021

NVD Last Modified:

02/04/2025

Source:

Apache Software Foundation



April 22-24, 2025 | The M Resort Spa Casino | Las Vegas, NV



License Type Details

LoB	App. Comp.	Application Module	Version	Group Name	VCount (for dep.)	Worst Lic. Cat. (dep.)	HScore
Phase1	RunMeNow	phase-frame-model-common	3.16.1	com.warsawbanking	24	CopyLeft	8.7
Phase1	RunMeNow	ebank60	6.3.20	com.warsawbanking...	108	CopyLeft	9.8
Phase1	RunMeNow	ebank60	6.4.12	com.warsawbanking...	94	CopyLeft	9.8
Phase1	RunMeNow	phase-frame-parent	3.16.2	com.warsawbanking	88	CopyLeft	9.8
Phase1	RunMeNow	phase-frame-parent	3.14.2	com.warsawbanking	118	CopyLeft	9.8
Phase1	RunMeNow	phase-frame-parent	3.10.3	com.warsawbanking	226	CopyLeft	9.8

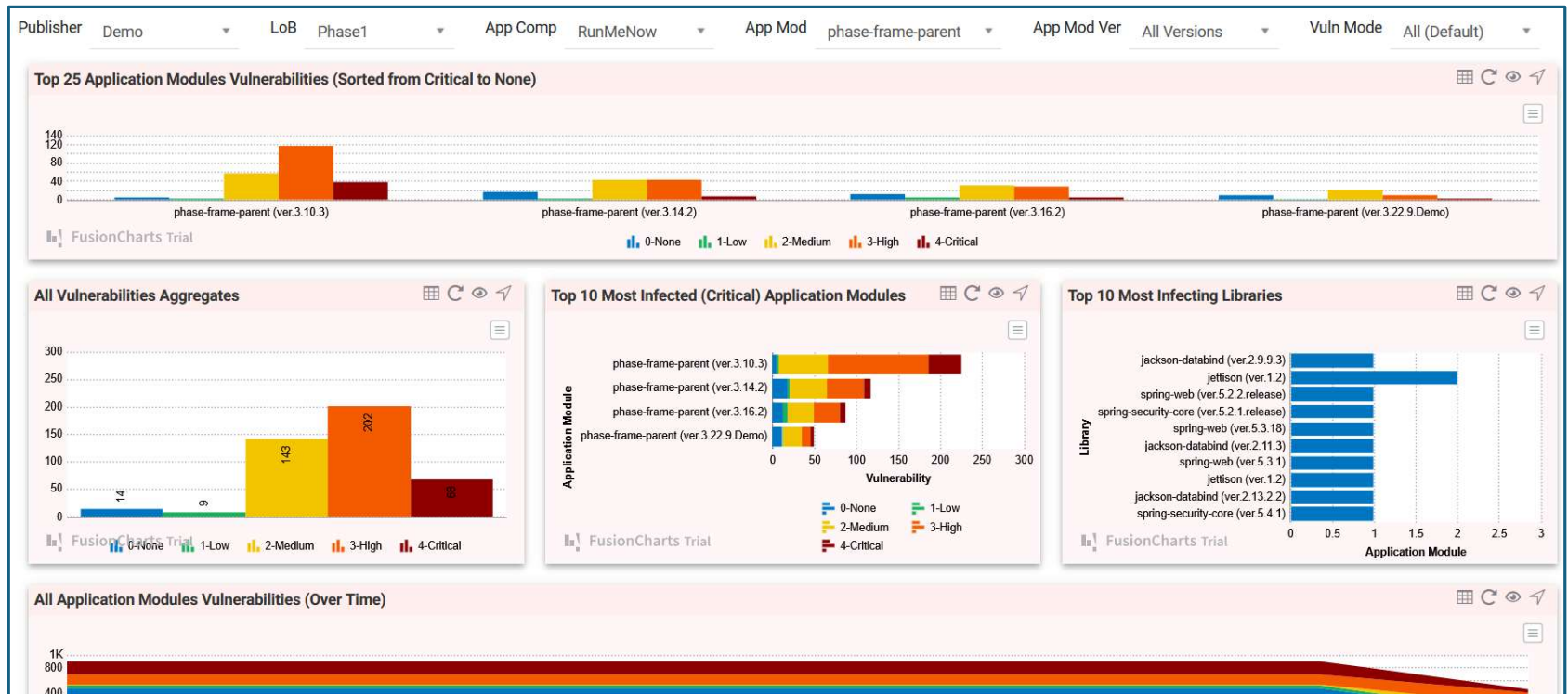
Library	Version	Age	Obsolescence	Latest Version	Latest Age	wEPSS	KEV	C	H	M	L	N	T	mV	License Type	Mods	Mm
struts2-core	2.5.8	8 years	Not Current and Obsolete	7.0.3	27 days	97.36%	3	13	14	8	0	0	35	2	Apache-2.0	1	1
log4j-core	2.9.1	7 years	Not Current and Obsolete	2.24.3	3 months	97.11%	2	4	1	3	2	0	10	0	Apache-2.0	1	0
xstream	1.4.9	9 years	Not Current and Obsolete	1.4.21	4 months	97.31%	1	9	46	15	0	0	70	0	BSD-3-Clause BSD	2	0
spring-webmvc	5.3.1	4 years	Not Current	6.2.4	3 days	97.45%	1	2	3	2	0	1	8	1	Apache-2.0	2	1
spring-webmvc	5.2.2.release	5 years	Not Current	6.2.4	3 days	97.45%	1	2	3	2	0	1	8	0	Apache-2.0	1	0



April 22-24, 2025 | The M Resort Spa Casino | Las Vegas, NV



Goal: Minimize Risk Scores



April 22-24, 2025 | The M Resort Spa Casino | Las Vegas, NV



Vulnerability Score Mitigation

Propose Mitigated Score - CVE-2022-22965

Current Score 9.8 (Not mitigated)

Aliases			
Vulnerability	Original Score	Last Accepted Score	Current Score
GHSA-36p3-wjmg-h94x	9.8		9.8

Proposed Score: 6

Mitigate with related Vulnerabilities: ☒

Decision Reasoning: Not using library in the manner that introduces risk per the CVE description.

BACK MITIGATE SCORE

Vuln Name Library Name

CVE-2022-22965	spring-b
CVE-2022-22965	spring-w
CVE-2022-22965	spring-beans
CVE-2022-22965	spring-webmvc

Score EPSS Mods mScore mV

9.8	97.45%	1	2
9.8	97.45%	1	2
9.8	97.45%	1	2
9.8	97.45%	1	2



April 22-24, 2025 | The M Resort Spa Casino | Las Vegas, NV



Who Should Be Using SBOMs

- Risk Management (vulnerabilities, obsolescence and license risk)
- AppDev (vulnerabilities, obsolescence and license risk)
- Cybersecurity (vulnerabilities and obsolescence)
- ITAM and SAM (gatekeepers)
- Procurement (gatekeepers)
 - Request SBOMs!
 - Review during the sourcing/PoC process



April 22-24, 2025 | The M Resort Spa Casino | Las Vegas, NV



Benefits

- Improve visibility and proactive planning
- Identify and mitigate behind-the-scenes threats
- Minimize incident response time
- Increase software supply chain security



April 22-24, 2025 | The M Resort Spa Casino | Las Vegas, NV



Summary

- Mandate compliance is driving urgency and adoption
 - Government, Financial, Healthcare, Defense
 - Utilities and Critical Infrastructure
- Other industries are likely to follow as benefits are realized and publicized



April 22-24, 2025 | The M Resort Spa Casino | Las Vegas, NV



Questions?

Thank You!

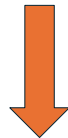


April 22-24, 2025 | The M Resort Spa Casino | Las Vegas, NV





Connect with Me!



terryd@eracent.com



[linkedin.com/in/terry-divelbliss-581969/](https://www.linkedin.com/in/terry-divelbliss-581969/)



April 22-24, 2025 | The M Resort Spa Casino | Las Vegas, NV