RELATÓRIO DE VIAGEM

DADOS DO EVENTO

DATA DE INÍCIO	DATA DE TÉRMINO	NOME DO EVENTO	CIDADE/PAÍS
28 de abril de 2025	1 de maio de 2025	RSAC CONFERENCE	SAN FRANCISCO/ESTADOS UNIDOS

RESUMO DO EVENTO

ENTIDADE ORGANIZADORA	PROCESSO	PARTICIPANTES
RSA CONFERENCE LLC	172/2025 (ISC TC-004.001/2025-7	ALAN GUILHERME DE OLIVEIRA

JUSTIFICATIVA (RESUMO)

A participação na RSAC Conference 2025, realizada em San Francisco, CA, entre 28 de abril e 1º de maio de 2025, foi fundamental para a atualização profissional em segurança cibernética, com foco em inteligência artificial (IA), gestão de identidade em ambientes multicloud, riscos de Shadow AI e soberania de dados. O evento, reconhecido como o maior do setor, proporcionou acesso a palestras técnicas, exposições de soluções inovadoras e networking com especialistas globais, incluindo um evento pré-conferência da Microsoft em 27 de abril e uma visita técnica à sede da Microsoft em Mountain View em 2 de maio. A troca de experiências com órgãos como SERPRO, Receita Federal, Tesouro Nacional, Consulado, Ministério das Relações Exteriores e Caixa Econômica Federal reforçou a relevância da ação para o fortalecimento das práticas de segurança cibernética no Tribunal de Contas da União (TCU), alinhando-as às melhores práticas internacionais.

RELATO

A RSAC Conference 2025, realizada no Moscone Center, San Francisco, é uma plataforma global que reúne profissionais, empresas e pesquisadores para discutir tendências e soluções em segurança cibernética. O evento incluiu palestras técnicas, laboratórios práticos, exposições de fornecedores e sessões de networking, com ênfase em temas como IA, gestão de identidade, segurança em ambientes multicloud, soberania de dados e mitigação de riscos emergentes, como Shadow AI.

As palestras frequentadas abordaram tópicos críticos para a segurança cibernética moderna:

- **IA e Segurança**: Sessões como "Shaping the Future of AI Security Through Collaboration" (PNG-T01), "The Cybersecurity Framework and AI" (SAT-M01) e "Principles of GenAI Security" (FND-M02) discutiram o papel da IA na automação de detecção de ameaças, governança de modelos generativos e mitigação de riscos em sistemas autônomos. A palestra "Analyzing VirusTotal's Malware Executables Collection with LLMs" (ANI-T09) apresentou técnicas de análise de malwares usando grandes modelos de linguagem, destacando a necessidade de frameworks éticos para IA.

- **Gestão de Identidade**: "AI Era Authentication" (IDY-M05) e "Standardizing a Privileged Access Model for a Multi-Cloud Environment" (CLS-R03) exploraram autenticação inclusiva e modelos de acesso privilegiado em ambientes híbridos, enfatizando a importância de controles granulares para prevenir acessos não autorizados.
- **Segurança em Nuvem e SaaS**: "Your Microsoft Cloud Is the Attacker's Computer" (CLS-R02) e "Beyond Login Attempts: Detecting Threats in SaaS Applications" (NCS-R01) detalharam vulnerabilidades em plataformas de nuvem e estratégias para monitoramento proativo de ameaças.

- **Resposta a Incidentes e Vulnerabilidades**: "10 Common Flaws in Incident Response Plans" (IMT-M03) e o laboratório "Case Studies in Vulnerability Prioritization" (LAB3-W08) ofereceram insights práticos sobre planejamento de resposta a incidentes e priorização de vulnerabilidades em ambientes complexos.

- **Inovação e Riscos Emergentes**: O "OWASP AI Security Summit" (OWASP-W01) listou os 10 principais riscos de aplicações de IA generativa em 2025, incluindo injeção de prompts e abuso de lógica de agentes. A palestra "The Cryptographers' Panel" (KEY-T02Y) abordou avanços em criptografia pós-quântica, relevantes para a proteção de dados soberanos.

A exposição contou com diversas empresas visitadas, como CrowdStrike, SentinelOne, Trellix e Rubrik, que demonstraram soluções para detecção de ameaças, proteção de dados e gestão de vulnerabilidades. A Cymulate apresentou simulações de ataques para validação de defesas, enquanto a Orca Security destacou monitoramento de segurança em nuvens híbridas. A OWASP reforçou a importância de padrões abertos para segurança de aplicações.

No dia 27 de abril, o evento pré-conferência da Microsoft abordou o uso de IA em segurança cibernética, com foco em ferramentas como Microsoft Security Copilot para automação de análise de ameaças. A visita à sede da Microsoft em Mountain View, em 2 de maio, permitiu a troca de informações com representantes de órgãos brasileiros sobre desafios em ambientes de TI governamentais, como conformidade, interoperabilidade e proteção de dados sensíveis.

Para colegas do TCU, as sessões sobre multicloud e gestão de identidade são particularmente úteis, dado o aumento da adoção de nuvens híbridas no setor público. A ênfase em Shadow AI alerta para a necessidade de monitoramento de ferramentas de IA não autorizadas. Comparado ao contexto do TCU, o evento destacou a importância de integrar frameworks como o NIST AI RMF para governança de IA e de adotar modelos de acesso privilegiado padronizados, áreas onde o Tribunal pode avançar.

ENCAMINHAMENTOS POSSÍVEIS, NO ÂMBITO DO TCU, DECORRENTES DESTA AÇÃO

Com base nas informações assimiladas na RSAC Conference 2025, seguem propostas de melhoria para o TCU:

1. **Gestão de Identidade em Ambientes Multicloud**:
    - **Contexto**: A palestra "Standardizing a Privileged Access Model for a Multi-Cloud Environment" (CLS-R03) destacou que ambientes multicloud aumentam a complexidade da gestão de identidades devido à heterogeneidade de plataformas (AWS, Azure, Google Cloud). A falta de controles centralizados pode levar a acessos não autorizados ou configurações inconsistentes.

    - **Proposta**: Implementar um modelo unificado de gestão de identidades e acessos (IAM) no TCU, utilizando soluções como zero trust. Recomenda-se a adoção de ferramentas como as apresentadas por SentinelOne, Microsoft e CrowdStrike para monitoramento contínuo de identidades humanas e não humanas (e.g., bots, agentes de IA). Um projeto-piloto já foi iniciado iniciado para mapear e consolidar identidades em nuvens utilizadas pelo Tribunal, reduzindo riscos de escalonamento de privilégios.

2. **Riscos Associados ao Shadow AI**:
    - **Contexto**: O "OWASP AI Security Summit" (OWASP-W01) e outras sessões alertaram para o Shadow AI, ou seja, o uso de ferramentas de IA não sancionadas por equipes internas, que podem expor dados sensíveis ou introduzir vulnerabilidades (e.g., injeção de prompts). Isso é crítico em órgãos públicos, onde a conformidade é essencial.

    - **Proposta**: Criar uma política de governança de IA no TCU, incluindo inventário de ferramentas de IA em uso e auditoria de fluxos de dados. Soluções como as da Varonis, vistas na exposição, podem ajudar a detectar Shadow AI por meio de monitoramento de comportamento de dados. Treinamentos baseados no "AI Phishing Coach" da Abnormal AI (apresentado na RSAC) podem ser adaptados para sensibilizar servidores sobre riscos de IA não autorizada.

3. **Soberania de Dados e Provedores Privados de Nuvem**:
    - **Contexto**: Discussões em "AI, Security, and Trust" (KEY-T10Y) e no evento da Microsoft abordaram implicações da soberania de dados, especialmente quando dados sensíveis são processados em nuvens privadas. Modelos de IA hospedados em provedores como Azure ou AWS podem conflitar com requisitos de residência de dados em jurisdições específicas, como o Brasil.

    - **Proposta**: Desenvolver diretrizes para soberania de dados no TCU, priorizando a hospedagem de dados sensíveis em nuvens com garantias de residência local ou em infraestruturas próprias. Recomenda-se avaliar soluções como as da Rubrik para backup e recuperação de dados com foco em conformidade. Um grupo de trabalho pode ser formado para alinhar as práticas do TCU com a Lei Geral de Proteção de Dados (LGPD) e padrões internacionais, como o GDPR, considerando parcerias com o SERPRO para soluções de nuvem soberana.

4. **Capacitação e Transferência de Conhecimento**:
    - **Contexto**: A sessão "10 Common Flaws in Incident Response Plans" (IMT-M03) e o laboratório "Case Studies in Vulnerability Prioritization" (LAB3-W08) reforçaram a importância de treinamentos práticos para equipes de segurança. A troca com outros órgãos na visita à Microsoft destacou lacunas em capacitação no setor público.

    - **Proposta**: Instituir um programa de capacitação contínua em segurança cibernética no TCU, com foco em resposta a incidentes, priorização de vulnerabilidades e uso seguro de IA. Simulações de ataques, como as oferecidas pela Cymulate, podem ser integradas aos treinamentos. Além disso, criar um repositório interno de conhecimentos adquiridos em eventos como a RSAC para disseminação entre as equipes.

Essas ações visam fortalecer a postura de segurança cibernética do TCU, alinhando-a às tendências globais e aos desafios de ambientes multicloud, Shadow AI e soberania de dados, contribuindo para a proteção de informações críticas e a conformidade regulatória.