GLOBAL RESILIENCE FEDERATION

January 2024 Newsletter

TLP CLEAR

IN THIS ISSUE: VPN Threats & Payment Systems Interruptions

BRC Webinar on Civil Unrest

The Business Resilience Council recently held a webinar on the potential for civil unrest, activism and extremism surrounding the 2024 US Presidential Election cycle. Foresight Chief Analyst Harris Stephenson provided a forecast of potential unrest, as well as possible business implications. He covered how to monitor these threats and how to protect your organization and personnel. Watch the webinar recording here.

Stop VPNs from becoming Virtual "Public" Networks

On February 20 at 1:00pm ET join GRF and Zero Networks' Nicholas DiCola for a presentation on VPN security. According to Top10VPN, in 2023 alone, 133 VPN vulnerabilities were disclosed and at least 20 are known to have been exploited – as evidenced by recent headlines involving Cisco, Ivanti, and others. The period from when these vulnerabilities are disclosed to the point they are patched (if at all), poses a major potential security risk for many organizations. Join to:

- Better understand why VPNs are explicitly targeted
- Consider several of the underlying flaws common to most VPNs
- Discuss risk mitigation strategies and alternative solutions

Register here.

LS-ISAO NY Workshop

Save the date for the first LS-ISAO workshop of 2024! Join your peers at Lowenstein Sandler in New York on Thursday April 4th, 2024. More information will be coming soon. If you have suggestions for a particular speaker or topic send them to Rsantiago@grf.org

Community Tabletop – Payments Disruption

Join Global Resilience Federation and Nacha for a free tabletop exercise to assess your organization's resilience after a simulated, but plausible destructive wiperware incident that includes a major ACH outage. In addition to IT operations and risk, exercise components will include media management, law enforcement and regulatory engagement, and an examination of your prioritizations. The half-day event will strengthen the ACH community through the sharing of risk, resilience and continuity practices.

Exercise players will need to triage operations and recovery actions based on a cyber risk control framework, incident response, evaluation of critical business services, service delivery, data recovery/restoration and communications plans, among other actions.

The exercise is designed for resilience practitioners from commercial banks, credit unions, and core systems processors. Institutions may also bring observers to watch segments of the exercise as it unfolds. Attendance is anonymous.

Choose from either Tuesday, March 19 or Wednesday, April 17, 2024 from 12:00 PM – 4:30 PM ET.

Learn more about the exercise here.

Interested in becoming a member, sponsor, or partner? Contact info@grf.org.

OT-ISAC Roundtable Event and Upcoming Table Top Exercise

OT-ISAC Executive Roundtable Philippines

On January 31, OT-ISAC hosted the Executive Roundtable Philippines with senior leaders from various critical infrastructure sectors. The group met for engaging discussions on the complexities of Operational Technology (OT) and Industrial Control Systems (ICS) security. Practitioners shared insights and strategies across key areas, emphasizing the need for tailored approaches in risk management in ICS/OT, OT threat intelligence, regulatory & compliance, and fostering a culture of continuous learning and adaptation. Highlights and takeaways include:

1. Risk Management in ICS/OT

Discussions underscored the unique challenges in ICS/OT risk assessment and mitigation, diverging significantly from traditional IT paradigms. Highlighted topics included the importance of specialized tools for threat identification and the necessity of comprehensive impact assessments. Strategies were shared on crafting adaptable, system-specific response plans that consider the physical implications and operational demands unique to ICS/OT environments.

2. Resilient Response Planning

The event spotlighted the creation of resilient incident response plans, tailored to the ICS/OT sector's distinct requirements. Regulatory compliance emerged as a critical pillar in reinforcing system resilience, guiding organizations in navigating the intricate landscape and ensuring robust, compliant, and effective incident response mechanisms.

3. Transparency and SBOM in ICS/OT

The significance of transparency in ICS/OT was a focal point, with particular emphasis on the role of Software Bill of Materials (SBOM) in unveiling and mitigating hidden threats.

OT-ISAC cont.

Insightful discussions revolved around the implementation of effective SBOM practices, enhancing the security posture of ICS/OT, and preparing for unforeseen challenges through comprehensive vulnerability management.

4. Actionable OT Threat Intelligence

The Roundtable concluded with a focus on actionable OT threat intelligence, highlighting the crucial role of in-depth system analysis in risk comprehension and mitigation. Strategies for integrating intelligence with security measures, using case studies, provided practical insights. Furthermore, the importance of collective defense was amplified through collaboration with community partners, showcasing the power of shared intelligence and coordinated response strategies.

OT-ISAC INCIDENT RESPONSE SIMULATION GAME

OT-ISAC is pleased to announce an upcoming table top exercise in Singapore on Thursday, February 22 from 9am-5pm. The training event with real-world scenarios will allow teams to immerse themselves in the incident response process, hone skills in detecting and analyzing artifacts, reconstructing the actions of attackers, and minimizing damage. The final stage of the event will analyze the tactics used by the teams and discuss best practices for responding to such incidents. Register here.

Community Contacts

OT-ISAC (John Lee)
LS-ISAO (Raquel Santiago)
EASE (Tim Chase)
ProSIX (Mark Orsi)
K12 SIX (Doug Levin)
BRC (Chris Denning)
Manufacturing ISAC (Tim Chase)
ONG-ISAC (Zabrina Antry)
Newsletter contact (Pat McGlone)