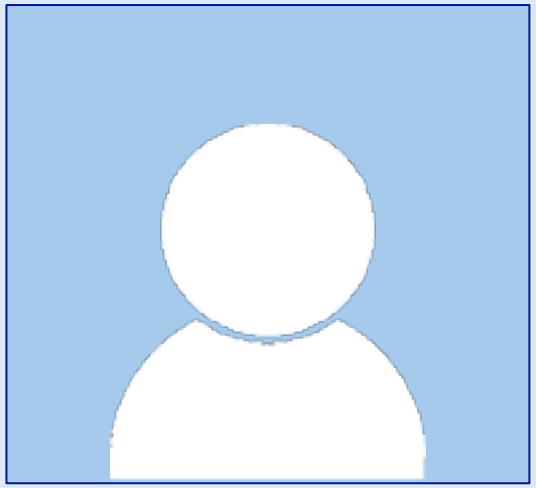
PRELIMINARY

Privacy + Security Forum

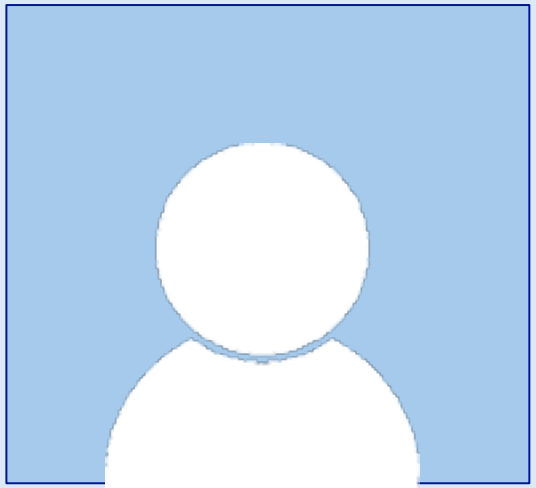
Session:
Whose Role is it Anyway? Scenarios for Incident Response Stakeholders

Privacy+ Security Forum

Speakers: Whose Role is it Anyway? Scenarios for Incident Response Stakeholders

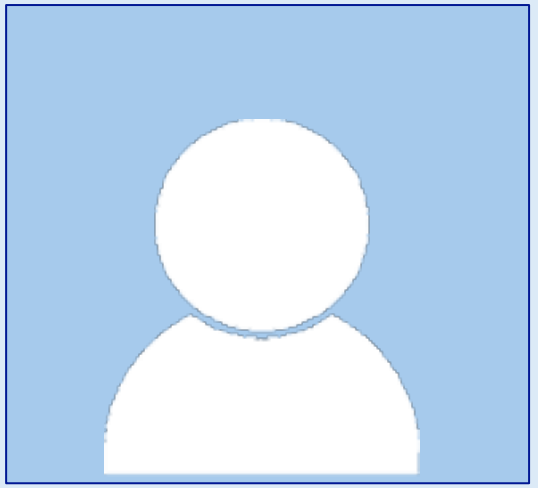


Noah Rubin
Senior Director,
Complex Digital
Events
Kroll



Nathan Salminen
Partner
Hogan Lovells

Jonathan Sander
Field CTO
Astrix Security



Heidi Wachs
Managing Director,
Complex Digital
Events
Kroll

Privacy+ Security Forum

Meet WeStaffIT

- WeStaffIT is a small IT and physical security staffing company that through connections, grit, and luck has secured contracts with a number of much larger, name-brand customers
- WeStaffIT relies heavily on PM4U, a start-up that provides project management software with AI capabilities
- Brian, the CEO of WeStaffIT and Robert, the CEO of PM4U are longtime buddies and struck a deal to help each other out by supporting each other's businesses

Thursday, 4pm

Brian receives an email from WeStaffsSecrets@proton.me alleging:

- Many high-profile WeStaffIT customers have unfilled IT and physical security roles
- Because of Brian and Robert's relationship, PM4U was not thoroughly vetted from a cybersecurity standpoint prior to procurement and implementation
- Claiming knowledge of many high-profile customers who have unfilled IT and physical security roles

The email threatens to go to the press with information about WeStaffIT's customers and their IT and security gaps. It also includes screenshots from within WeStaffIT's instance of PM4U showing job listings of their five largest customers, including specific locations needing physical security protection.

WeStaffIT's GC contacts outside counsel, who quickly engages a forensics firm.

Thursday, 6pm – Investigation Scoping Call

- Who is on the call?
  - Who *should* be on the call?
- What are the goals of the investigation?
- What evidence sources are available?
  - System diagrams?
  - Logs?

Thursday, 10pm – Investigation Begins

- How will the forensics firm gain access to the evidence?

Based on what is known at this time, and the screenshots in the email, there is significant concern that this is an insider. All parties agree that the investigation may need to be done stealthily so as not to tip of the insider.

- How does this change the investigative approach?
  - How will internal communications about the investigation be handled?
  - Can you centralize the investigation with a minimum of staff involvement?
  - How does the role of the potential insider affect the investigative approach?

Friday, 8am – Investigation Continues

On the morning update call, WeStaffIT's head of IT mentions that some of the information included in the extortion note is stored in their PM4U system. Since their operations rely so heavily on PM4U and they have a lean team, WeStaffIT implemented an internal chat bot to answer questions and perform actions on behalf of project managers.

The chat bot uses the built-in PM4U MCP server, which allows LLMs to more easily integrate with third-party systems. To integrate with PM4U, WeStaffIT's internal chat bot system uses a service account with its own username/password to connect to PM4U. Employees using the chat bot system authenticate via WeStaffIT's standard SSO.

- What evidence is available from WeStaffIT's chat bot?
- What evidence is available from PM4U?

Weekend – Investigation Continues

- The forensic team reviews logs, email, and available evidence from the chat bot and PM4U.
- On Saturday afternoon, Brian receives a second email from WeStaffsSecrets@proton.me demanding 2.5BTC or they will go public with the information.
- Sunday night at 10:45pm, forensic analysis of the email environment discovers that a WeStaffIT college intern in the marketing department sent himself documents with proprietary information including a list of current WeStaffIT customers and current open positions.

Monday, 2pm – Investigation Concludes

- Monday morning, forensic analysis is able to match the intern's email address with logs from the WeStaffIT chat bot.
- The logs show that the intern asked the chat bot:
  - What are the five highest value contracts?
  - What staff openings does company [INSERT NAME] have?

Key Takeaways

- Know your key stakeholders for an active incident. Make sure they understand their responsibilities.
- Understand what evidence you do (and don’t) have in your environment. Determine whether that needs to change.
- Have a plan for granting access to different types and locations of evidence. Have a backup plan if you need to conduct a stealthy investigation.
- Conduct risk assessments of your third-party vendors.

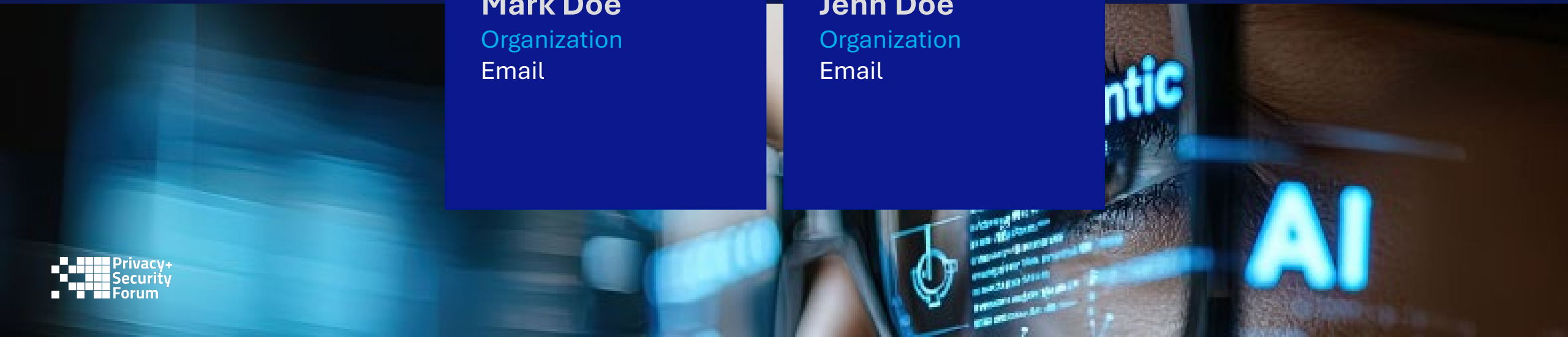
Stay in touch: Continue the conversation with us

Jenn Doe
Organization
Email

Jenn Doe
Organization
Email

Mark Doe
Organization
Email

Jenn Doe
Organization
Email



Privacy+ Security Forum