BGIN Meeting Report

Date: TBD
Location: Virtual Meeting

Executive Summary

The meeting focused on the structured policy analysis and reasoning for a chatbot designed to enhance cybersecurity in the cryptocurrency industry. Key topics included the importance of information sharing, regulatory compliance, data classification, and international cooperation. The discussion highlighted the need for clear guidelines, secure data handling, and effective incident response plans. Recommendations were made to develop global cybersecurity standards, foster collaboration between experts, and engage stakeholders to create policy proposals.

Key Discussion Points

- **Cybersecurity**: Emphasis was placed on the importance of vulnerability management and incident response in the cryptocurrency industry.
- **Data Sharing**: The need for secure data sharing mechanisms between companies and organizations was highlighted as a critical aspect of enhancing cybersecurity.
- **Regulatory Compliance**: Challenges related to regulatory compliance were discussed, with a focus on developing clear guidelines and protocols.
- **Information Classification**: Implementing effective information classification systems was identified as essential for secure data sharing.
- **Cross-Border Considerations**: The importance of international cooperation and regulatory harmonization was stressed to ensure global cybersecurity measures.

Action Items and Next Steps

- **Conduct Further Research**: Investigate the current regulatory landscape of the cryptocurrency industry to identify areas for improvement.
- **Engage with Stakeholders**: Collaborate with companies, organizations, and governments to develop effective solutions and guidelines.
- **Develop Policy Proposals**: Based on the analysis and recommendations discussed, create policy proposals to enhance cybersecurity in the cryptocurrency industry.

Detailed Session Summary

The meeting began with a structured policy analysis of key regulatory topics relevant to the cryptocurrency industry. The discussion focused on four main areas: cybersecurity, data sharing, regulatory compliance, and information classification. Participants emphasized the importance of vulnerability management and incident response, particularly in an industry where security breaches can have significant financial and reputational impacts.

The need for secure data sharing mechanisms was a recurring theme. It was agreed that companies and organizations must share information about vulnerabilities and incidents to improve collective cybersecurity. This would require the development of clear guidelines and protocols to ensure that data is shared securely and effectively.

Regulatory compliance was another critical topic. The industry faces challenges due to the lack of clear guidelines, which can lead to confusion and inconsistency in how different entities approach compliance. Participants recommended developing global standards and fostering collaboration between experts from various fields to address these issues.

Information classification was also discussed as a crucial aspect of secure data sharing. Implementing systems that classify information appropriately would help prevent sensitive data from being exposed and ensure that only authorized parties have access to critical information.

The meeting concluded with a discussion on cross-border considerations, emphasizing the need for international cooperation and regulatory harmonization. This is essential to develop effective global cybersecurity measures, particularly in an industry where transactions often span multiple jurisdictions. Recommendations were made to establish international cooperation mechanisms and provide regulatory clarity through clear guidelines and protocols.

Appendix: Full Meeting Transcript (Anonymized)

```
0.0 --> 1.8:  This will work out.
4.1 --> 5.3:  How do you want to proceed?
5.5 --> 7.1:  Do you want to introduce it at the very beginning
7.1 --> 7.8:  from the start?
7.9 --> 8.3:  Yeah, yeah.
8.5 --> 12.3:  So, yes, I think we'll start with Michael.
13.8 --> 17.4:  He intended to introduce the overview at first
17.4 --> 19.8:  for a couple of minutes.
20.0 --> 20.3:  Okay.
```

20.3 --> 21.7: About when I introduce something.
23.2 --> 26.8: So, maybe we shall wait for him in that case, no?
26.8 --> 29.8: No, I don't think so.
32.7 --> 35.1: We simply need to talk about
35.1 --> 38.1: what the security information shall be.
38.4 --> 39.1: Yes, yeah, sure.
40.8 --> 43.3: So, then we're just saying, yeah, yeah, no.
45.4 --> 46.5: I'm sorry.
46.9 --> 49.4: It's kind of stupid to do that.
49.6 --> 50.3: So, wait for it to happen.
50.6 --> 51.1: Is that what you're saying?
53.0 --> 53.0: Okay.
53.0 --> 53.1: Okay.
53.1 --> 54.7: So, then, we're just going to keep sharing the screen,
54.9 --> 56.7: and then you can look around one spot.
69.4 --> 72.4: Okay, for those online, please bear with us.
72.5 --> 76.3: We are just setting up our presentation and material,
76.4 --> 78.2: and Mitchell was supposed to,
79.1 --> 81.8: was intended to share this session, as well, with Carol.
83.7 --> 87.5: It's, no, it's delayed because of train metro issues.
88.0 --> 90.2: So, we will start the session with Carol,
90.3 --> 92.9: and we will try then to be sure
94.0 --> 96.6: that Mitchell is up to speed when he will arrive.
97.9 --> 101.5: So, bear with us, as I say, just a few seconds.
117.7 --> 118.1: Okay.
118.5 --> 118.5: Okay.
143.0 --> 145.1: Just a few slides in order to introduce the session.
146.1 --> 149.4: So, as introduced by Shinichiro Matsuo,
150.9 --> 152.9: earlier, we have two sessions planned
152.9 --> 154.5: on cybersecurity information sharing.
155.0 --> 158.2: So, we have quite some time to be able to discuss
158.2 --> 160.0: and enter into the details, but in fact,
160.2 --> 162.2: related to the cybersecurity information sharing,
162.3 --> 164.2: there are different subtopics.
164.4 --> 169.1: Some are related to discuss, well, the status of our wo
rk,
169.4 --> 172.6: status of the document that has been prepared last year,
173.9 --> 178.9: and status also of the agentic project
179.7 --> 186.0: in order to facilitate sharing and also summarizing the,
186.7 --> 188.4: and also retrieving information related
188.4 --> 192.1: to intelligence and vulnerabilities,
192.4 --> 193.9: intelligence threats and vulnerabilities.
194.3 --> 197.7: And also, we are here to discuss what should be,
198.0 --> 201.3: what improved with respect to our current project
201.3 --> 203.3: and what should be done next.
204.2 --> 205.6: For the first session,
206.6 --> 208.7: there was an agenda planned for the session.

208.9 --> 211.8: There was some topics that probably are related
211.8 --> 214.0: to the second session that we are going to touch today.
214.1 --> 216.2: I think we can be flexible on that side.
218.9 --> 223.5: So, let me see how I can change this.
224.9 --> 225.4: Okay.
226.5 --> 227.0: Sorry.
227.4 --> 227.7: Oops.
227.9 --> 229.1: Just very, very slow.
231.3 --> 235.2: We wanted to discuss in particular
235.2 --> 238.2: the current state of threat intelligence
238.2 --> 241.6: and what are the existing initiatives.
241.9 --> 244.7: This is really, and this slide as the other one
244.7 --> 246.3: are really just to introduce
246.3 --> 248.8: and to help framing the discussion.
249.7 --> 251.2: They are not meant to be exhaustive.
251.3 --> 256.3: They are not meant to be necessarily fully correct
256.9 --> 257.7: on some aspects.
257.7 --> 261.8: It's really a quick summary of the current state.
261.9 --> 264.2: And we are here to discuss and to get the input
264.2 --> 267.9: and to see how we can improve the current overview.
268.8 --> 273.4: So, well, as you probably all know,
275.3 --> 279.9: why we are trying to share threat intelligence information
279.9 --> 283.5: among the different stakeholders in general,
283.5 --> 287.8: just because, well, if we don't share,
288.5 --> 291.7: we are kind of in silos between organization,
292.0 --> 294.2: between regions, between jurisdictions,
295.0 --> 299.2: while attackers do not really care
299.2 --> 303.6: of not sharing information among them.
304.5 --> 307.5: They are ready to use any kind of information
307.5 --> 309.7: coming from their way to get
309.7 --> 311.3: some threat intelligence information
311.3 --> 320.4: and kind of understanding of attack vectors,
320.8 --> 322.5: understanding of what can be exploited,
322.7 --> 327.3: what is new and just trying to find a new ones every day.
329.0 --> 331.6: So that's why we want to share information.
332.1 --> 333.8: But at the same time, in the context of,
334.0 --> 335.8: in particular of blockchain application
335.8 --> 338.4: and Web3 and DeFi and so on,
339.1 --> 342.8: we have seen that the speed of exploiting vulnerabilities,
343.6 --> 347.6: well, it's quite awesome in a way.
348.5 --> 351.2: This is about efficiency of exploiting
351.7 --> 354.1: a specific vulnerability in order to really
354.6 --> 356.2: maximize the gain for attackers.
356.9 --> 359.3: So in term of efficiency overall,

359.5 --> 362.6: this is quite impressive, but in terms of impact,
363.0 --> 366.5: this is quite terrible for those managing those applica
tions
366.5 --> 367.4: that are being attacked.
367.4 --> 372.5: So that's why there is a kind of asymmetric status
374.0 --> 378.3: between the time needed to exploit vulnerabilities
378.3 --> 380.9: on new weaknesses versus the time
380.9 --> 382.1: to really share the information
382.1 --> 384.6: among different players in the field.
385.1 --> 387.5: So that's why we started to look at this problem
388.4 --> 391.3: and what trying to think about what is specific
391.3 --> 393.4: for blockchain and Web3 applications.
395.3 --> 399.3: So just for instance, it is well known that,
400.2 --> 404.2: given that we have fragmentation between many protocols,
404.5 --> 407.7: many layers, well, many layers in some words,
407.8 --> 410.0: but at least between layer one and layer two protocols,
410.6 --> 413.3: and also the different centralized exchange
413.3 --> 415.1: versus the DeFi applications,
416.5 --> 419.5: it's kind of very hard to have an unified view
419.5 --> 422.3: of the different movements across chain,
422.3 --> 423.4: across different applications.
424.2 --> 425.7: So there are different initiatives,
426.1 --> 431.8: as you probably know, the CryptoISAC initiative in US,
432.6 --> 435.1: the GP CryptoISAC in Japan,
435.4 --> 438.8: which are more, let's say, driven by,
440.9 --> 443.7: I will call those regular organization,
444.9 --> 449.6: at least generally legal entities and institutions,
450.6 --> 456.1: while in parallel, there is the more grassroots initiat
ive,
456.4 --> 460.6: which is the SEAL-ISAC, which is an initiative
460.6 --> 463.8: that has been created by the Security Alliance Group,
464.1 --> 470.0: which is formed by a group of Web3 blockchain developer
s
470.0 --> 475.3: in particular, and also security experts in that field.
475.9 --> 477.5: And among the different initiatives,
477.5 --> 479.1: there is one which is written more to,
481.2 --> 483.5: not necessarily really about threat intelligence,
483.7 --> 485.5: but more about incidence response
485.5 --> 488.0: on how to coordinate quickly when there is something
488.0 --> 492.9: which is under active exploit in the field,
493.0 --> 494.4: on how to reply quickly.
497.0 --> 499.7: Anything that you would like to add, Carol?
500.5 --> 501.0: No.
503.4 --> 504.8: Any comment, any question
504.8 --> 507.6: respect to the state of threat intelligence?
507.9 --> 510.6: Is there something, an important initiative missing
512.3 --> 513.3: from what you know?

514.9 --> 516.6: Be careful with the...
526.6 --> 528.3: Yeah, this is Carol House,
528.4 --> 530.2: for those who are joining virtually.
531.2 --> 533.6: I wonder, does it make sense to reference
533.6 --> 535.2: something like the T3 partnership
535.9 --> 538.3: that is much more narrow and specific,
538.7 --> 541.2: and is like a very particular partnership
541.2 --> 544.4: between TRM Labs and Tron and Tether?
544.7 --> 547.6: I think Binance might have expanded to include in it.
548.0 --> 550.6: It's not as holistic and meant to be
550.6 --> 552.3: industry-wide as this.
553.0 --> 554.5: That's just something I wanted to flag.
555.4 --> 558.8: And then, I don't think that we would reference it here,
558.9 --> 560.8: but just something that would be valuable
560.8 --> 564.5: for us to keep in mind is the broader ecosystem
564.5 --> 568.0: of cyber threat information sharing,
568.2 --> 571.1: but then also financial crime information sharing.
571.3 --> 574.2: The convergences are continuing to
575.3 --> 577.2: become more and more apparent,
577.9 --> 580.2: including even in just in the standards work
580.2 --> 581.2: that we've been doing at Begin.
581.8 --> 583.3: If you took out the word crypto,
583.6 --> 584.9: it's basically standards around
584.9 --> 586.4: what information sharing looks like,
586.4 --> 589.1: just with a unique ecosystem application.
590.3 --> 594.2: So, in that case, there's a lot of different things
594.2 --> 595.8: that are happening on information sharing
595.8 --> 600.1: on the cyber front, across lots of different ISACs and
GFCE,
600.7 --> 603.5: and then on financial crime, things like CIFAS,
604.3 --> 605.9: and other kinds of exploitation.
606.4 --> 608.7: So, it's more just interesting for us
608.7 --> 610.1: to think about those initiatives.
610.3 --> 612.6: I don't think that we have to necessarily include
612.6 --> 613.3: and map them here.
613.4 --> 615.5: It's just some interesting context for us to consider,
615.6 --> 617.6: given that most of the crypto crime
617.8 --> 622.2: and threat intelligence information that gets shared
622.2 --> 626.1: is in the context of there having been cyber crime,
626.4 --> 628.9: of it being financial crime and fraud related.
629.6 --> 632.7: So, I just wanted to highlight some non-crypto specific,
633.1 --> 635.4: but still related to these crimes,
635.6 --> 637.4: information sharing that happens otherwise.
641.9 --> 642.5: Very good point.
643.3 --> 647.7: Indeed, it's about applications being exploited,
648.0 --> 649.2: and in general, those expectations
649.2 --> 651.7: are related to some specific domains,

652.0 --> 656.0: and so being connected to wider ecosystem
656.5 --> 657.6: makes definitely sense, yeah.
667.6 --> 670.6: Would you like to mention something?
672.5 --> 672.6: No?
679.8 --> 680.0: Okay.
681.2 --> 681.5: Yeah.
683.0 --> 686.2: Before jumping into, let's say,
686.4 --> 688.5: some regulatory and compliance example,
689.1 --> 692.0: we would like to make an introduction
692.0 --> 697.2: on the agentic hackathon session.
698.9 --> 700.9: So, I guess, Shouhi,
700.9 --> 702.7: you want to say a few words?
703.7 --> 704.5: Are you connected to Zoom
704.5 --> 706.6: in order to share your screen as well?
707.6 --> 707.8: Okay.
709.2 --> 711.1: Just stop sharing on my side.
714.5 --> 715.0: Yes.
720.8 --> 726.6: Hello, my name is Shouhi Mitani,
726.8 --> 729.3: a researcher from NEC Corporation.
729.9 --> 736.3: So, today, let me introduce our AI agent
736.3 --> 740.5: for community-driven security information sharing,
741.2 --> 745.4: which is connected to the other session,
746.7 --> 748.3: agent hack session,
749.1 --> 752.6: and this community-driven security agent
752.6 --> 758.7: is one possible direction to solve the cyber issue
758.7 --> 761.8: in blockchain security information sharing,
762.3 --> 767.5: sorry, information security operation incident response
768.1 --> 770.6: and any other security-related work
771.6 --> 775.2: based on information sharing among stakeholders.
776.1 --> 780.8: So, what we are trying to solve is,
780.9 --> 784.0: sort of, fragmented information sharing,
784.7 --> 786.4: and as well as high-cost
786.4 --> 789.2: and inefficient security work,
790.4 --> 791.1: trust barriers,
794.4 --> 797.0: which is specifically important in a blockchain system,
798.0 --> 801.1: and, of course, novice rate classes in blockchain,
802.4 --> 807.4: and we have prepared
812.6 --> 815.9: an example security
815.9 --> 817.0: agent AI.
818.0 --> 823.2: I just posted QR codes and related information
823.9 --> 826.3: on the latest thread
826.9 --> 831.5: on the Begin Disco channel, like this.
831.9 --> 836.3: So, please open it and try to use
836.3 --> 841.8: the latest version of security agent chatbot.
862.6 --> 867.2: Okay, so, yes, so, this is the same slide
867.2 --> 871.1: with what I introduced on the Disco channel.
872.1 --> 876.2: On this first slide, I'd like to share

876.2 --> 881.4: how we'll use today's AI agent for security
881.4 --> 885.5: and security work and information sharing for that.
888.0 --> 892.7: In this session, first, our purpose is,
894.1 --> 898.8: as step one, we can try a very simple security
898.8 --> 901.1: and information sharing agent,
902.0 --> 908.5: and we can get a feel for what it can and cannot do
908.5 --> 913.8: in the current version,
914.7 --> 919.0: and in step two, we'd like to hear your feedback,
919.6 --> 924.1: what kind of needs you have, what use cases you imagine,
924.7 --> 928.1: and, of course, any ideas for improvements.
929.1 --> 932.3: Finally, in step three, we'll use your feedback
932.3 --> 936.1: as input when we design the, for example,
937.8 --> 939.8: discussion in next session,
940.5 --> 946.2: and the next version of the agent, so that, yes.
947.0 --> 949.5: So, if you have time, or, of course,
950.3 --> 955.2: please give it a try on this AI agent.
963.9 --> 968.5: So, yeah, we've prepared two boards,
968.8 --> 970.9: chat boards for today's demo.
972.0 --> 977.4: This is designed as a bilingual board,
977.8 --> 982.7: so, yes, I placed English and Japanese introductions.
983.5 --> 992.8: So, yes, also, we prepared two chat boards,
993.4 --> 996.9: but basically for just a backup purpose,
997.6 --> 1001.5: and part one is a relatively general-purpose agent
1001.5 --> 1006.1: with a limit on the number of conversations
1007.4 --> 1008.1: for today's session,
1009.0 --> 1012.4: so you can quickly try out basic security
1012.4 --> 1016.5: and information sharing interactions on this chat boa
rd.
1017.9 --> 1023.1: The other board, part two, is basically a backup agen
t,
1023.7 --> 1026.6: but without a conversation country limit,
1027.0 --> 1034.5: and has a slight difference from the first chat board.
1035.0 --> 1038.3: The second one is configured for more specific scenar
ios,
1038.3 --> 1040.9: so you may notice, yes,
1041.4 --> 1043.0: slightly different interaction style.
1044.5 --> 1050.1: However, in both boards, as a most important point,
1050.5 --> 1053.6: data is processed by third-party services,
1053.8 --> 1056.4: including OpenAI, Google, and so on,
1056.7 --> 1058.6: so please do not enter confidential
1058.6 --> 1060.0: or sensitive information,
1060.4 --> 1065.2: and what today, in this demo,
1066.0 --> 1071.8: please use only test or, yes, test data,
1073.0 --> 1079.0: if you're willing to try some very specific
1080.0 --> 1080.7: response generation.
1091.0 --> 1094.3: So, once you open the bot from the QR code,
1094.3 --> 1095.3: you'll see this screen.

1096.3 --> 1097.5: To start a conversation,
1097.7 --> 1100.1: just click the Start button at the bottom,
1101.1 --> 1108.6: and a security agent demo will begin the chat with ea
ch of you.
1115.2 --> 1117.0: However, for the first use,
1117.7 --> 1122.8: since this is based on the telegram,
1124.3 --> 1127.9: chat bot, phone number verification is required
1127.9 --> 1132.2: as part of the telegram account setup.
1143.3 --> 1146.3: And once the bot has started,
1146.5 --> 1150.8: you'll see a welcome message like this.
1151.5 --> 1154.8: You can either type one question in the message box
1154.8 --> 1160.7: or pick one of the suggested options below to get sta
rted.
1161.8 --> 1165.6: For example, you might choose the wallet provider opt
ion
1165.6 --> 1170.6: and upload an example PDF policy, just an example,
1172.1 --> 1175.1: so that the agent can review it
1175.1 --> 1180.0: against recent security issues, sorry, security sheet
s.
1190.4 --> 1194.1: And on this slide, let me briefly show
1194.1 --> 1197.4: how this telegram-based security agent works.
1198.5 --> 1203.7: These bots can look up information on public websites,
1204.1 --> 1209.0: such as Web3 Blockchain Incident Database,
1209.0 --> 1211.5: and as well as a vegan website,
1212.2 --> 1215.5: and yes, as I mentioned, other web sources,
1216.5 --> 1219.3: including security and other recent news.
1222.7 --> 1227.6: This bot can also draw on internal knowledge,
1227.8 --> 1230.8: such as vegan agent documents
1231.4 --> 1236.7: and related research in Cybersmart,
1237.3 --> 1239.6: and trustworthiness research and so on.
1240.7 --> 1247.1: It is to help protect, sorry, yes.
1247.9 --> 1255.4: For example, this vegan agent is designed
1255.4 --> 1260.3: to help protect contributor's privacy,
1261.7 --> 1266.7: and this trustworthy AI is to check
1266.7 --> 1269.0: the quality of shared information
1269.0 --> 1271.4: and its processes and so on.
1272.3 --> 1275.5: Finally, the bot is connected to Google Seeds,
1275.5 --> 1280.6: which we use as a shared space, mock information,
1283.2 --> 1285.0: sorry, shared knowledge base,
1285.8 --> 1289.3: where participants can add and update examples
1289.3 --> 1293.7: and incident information and any related information,
1293.7 --> 1300.4: such as internal shared incident response policies.
1310.2 --> 1310.5: Sorry.
1315.1 --> 1319.5: Yes, yeah, as I've already mentioned,
1319.6 --> 1323.3: the users can manage this shared knowledge base
1323.3 --> 1325.0: through the Telegram bot.
1325.8 --> 1330.9: You can either use a command like slash add,

1331.5 --> 1333.8: or you can simply describe in natural language
1333.8 --> 1337.4: what you want to add to the shared knowledge base,
1338.0 --> 1340.3: and the bot will register a new example
1340.3 --> 1343.3: in the Google Seeds knowledge base.
1346.2 --> 1348.4: In advance, knowledge visualization
1348.4 --> 1354.7: and access control are still under development
1354.7 --> 1359.5: and will be, yes, layered on top of this shared data.
1368.0 --> 1372.3: Okay, this slide shows the overall goal.
1373.3 --> 1376.7: It is building a very fast security agent
1376.7 --> 1378.4: for the blockchain ecosystem.
1379.1 --> 1383.7: The most important part is their use side,
1383.8 --> 1387.3: usage side on the right-hand side.
1388.0 --> 1392.9: The agent helps you before even asking
1392.9 --> 1395.5: for any contributions, of course.
1397.1 --> 1400.1: So the usage varies though.
1400.2 --> 1402.8: You start with simple question and answer.
1403.8 --> 1405.3: Once you are using it,
1405.3 --> 1410.6: the agent can support your daily operations,
1411.3 --> 1413.1: including incident response planning,
1413.5 --> 1419.6: audit preparation, risk assessment, yeah, et cetera.
1420.4 --> 1427.0: To do this, the agent draws on a shared knowledge bas
e,
1427.2 --> 1431.5: covering incidents, vulnerabilities, or best practice
s,
1431.5 --> 1435.5: threat intelligence, and yeah,
1436.5 --> 1439.0: post-incident analysis, so on.
1441.3 --> 1446.7: This knowledge base should be powered
1446.7 --> 1449.4: by multi-stakeholder contributions
1449.4 --> 1453.4: from protocol developers, code operators,
1453.8 --> 1456.2: service providers, researchers, auditors, and regulat
ors,
1457.0 --> 1458.7: as shown at the bottom.
1459.7 --> 1464.7: This contribution model should be designed
1465.9 --> 1471.3: so that people can report without fear of blame,
1473.0 --> 1480.9: and so they can share only what's necessary for defen
se,
1481.4 --> 1485.6: and verify sources when registering signatures.
1493.5 --> 1502.1: This roadmap shows one possible evolution path
1502.1 --> 1508.4: from today's simple agent, chatbot,
1509.3 --> 1513.4: you are trying, you may be trying today,
1513.9 --> 1515.8: to a more sophisticated system.
1516.7 --> 1520.7: It's, this figure is not, of course, a promise,
1521.3 --> 1525.6: just an example to, yes, foster our discussion.
1526.8 --> 1529.2: On the left is today's experience,
1529.5 --> 1535.1: the two demo bots you can test today, bot one and bot
 two,
1537.9 --> 1540.4: that help you explore security questions.

1541.4 --> 1546.8: The next step here is privacy and community agent
1547.5 --> 1551.5: that focuses on three things.
1552.4 --> 1555.6: First, establishing trust in a multi-stakeholder sett
ing,
1556.4 --> 1559.7: and handling confidential information
1560.5 --> 1563.0: according to, for example, TRP rules,
1563.7 --> 1568.7: and clearly attributing who contributed what informat
ion.
1570.3 --> 1575.6: And next, the BNZ is a high-assurance agent
1576.4 --> 1580.0: that adds information provenance, for example,
1580.3 --> 1585.0: so you know where each piece of knowledge came from,
1585.4 --> 1588.8: plus quality assessment automation to filter noisy da
ta,
1589.3 --> 1591.1: and accountability assistance,
1591.3 --> 1593.5: so you can track the reason behind any answer.
1594.8 --> 1601.1: The last box shows an integrated agent
1601.1 --> 1604.5: that might connect to standards like STIX, TAXI,
1604.6 --> 1607.8: CVE, and CW, work with threat operations,
1608.1 --> 1612.0: and even put the knowledge base and agent on-chain,
1614.0 --> 1619.0: as for distribution and verification.
1620.0 --> 1628.6: So, yeah, whether these are useful,
1629.0 --> 1635.4: or even necessary, is, yes, often a question
1636.8 --> 1639.0: for this kind of a session.
1641.2 --> 1643.7: And the foundation across all these phases
1643.7 --> 1647.8: is shown as a secure AI platform.
1648.7 --> 1652.6: It means, for example, on-premise deployment for priv
acy,
1653.3 --> 1656.4: access control, supply chain security, and so on.
1665.2 --> 1665.8: Sorry.
1685.0 --> 1686.0: Okay.
1687.1 --> 1690.6: And as I mentioned earlier, yes,
1690.8 --> 1694.2: I'd appreciate your feedback and discussion
1694.2 --> 1702.2: on the how and, well, yes, how this,
1703.3 --> 1708.0: how or whether this agent can help
1708.0 --> 1711.0: the information, security information sharing.
1711.8 --> 1714.1: And there can be several questions,
1715.5 --> 1718.0: but the key question for that,
1719.0 --> 1722.3: for the previous roadmap is, yes,
1722.9 --> 1727.7: at which stage and for which concrete tasks
1728.7 --> 1732.6: of each stakeholder, would, yes,
1733.4 --> 1738.5: such an agent need to cut your current effort dramati
cally?
1740.6 --> 1744.9: Hopefully, yes, for it to be worth adapting
1745.5 --> 1746.7: in your operations.
1748.7 --> 1750.8: Yeah, okay, so, yeah.
1752.9 --> 1753.3: Thank you.
1753.3 --> 1761.0: Okay, I hope you to try the AI agent

1761.0 --> 1766.9: and try to start a chat with it.
1774.7 --> 1775.7: Does anyone have questions?
1785.9 --> 1788.7: Just for the clarity, thank you very much, first.
1790.1 --> 1793.4: So do you want the participants to try now
1793.4 --> 1796.4: or to try in the next few hours
1796.4 --> 1799.5: and to get feedback in the second session,
1799.6 --> 1802.6: or do you expect feedback also after the second sessi
on?
1804.3 --> 1806.9: I mean, what, do you expect feedback
1806.9 --> 1808.9: by the end of the day as well, or?
1827.4 --> 1828.5: Okay.
1828.5 --> 1828.8: Yes, okay.
1831.2 --> 1835.8: Basically, we should focus on discussion anyway,
1836.5 --> 1839.9: because the purpose of this chatbot to,
1840.6 --> 1846.0: yes, facilitate the concrete discussion
1846.9 --> 1852.0: or what can be done for the security incident respons
e.
1855.6 --> 1860.8: But yes, very concrete questions or opinions
1861.9 --> 1864.7: on the utilization of the chatbot
1866.2 --> 1869.7: should help our discussion, I think.
1873.3 --> 1874.0: Thank you.
1874.0 --> 1874.6: Okay, thank you.
1875.5 --> 1878.6: Just again, the warning that you can see on the slide
1879.3 --> 1880.6: that is still displayed here,
1881.2 --> 1882.9: this is a testing environment.
1883.1 --> 1885.5: This is shared with third party.
1886.5 --> 1889.6: We cannot guarantee the security of the information
1889.6 --> 1890.3: that is shared.
1890.4 --> 1894.8: It's really, please, important to use only informatio
n
1894.8 --> 1897.7: that are either public or for testing purposes,
1897.7 --> 1899.7: which is something which is fake,
1899.9 --> 1902.1: but not real computational information.
1902.8 --> 1903.0: Carol?
1906.6 --> 1908.3: So, really appreciate the walkthrough.
1908.5 --> 1910.5: Thank you so much for that thorough review.
1911.0 --> 1913.8: I, given some of the amazing information sharing part
nerships
1913.8 --> 1915.3: that are sitting around the table,
1915.5 --> 1919.4: I was wondering if, just to help me think
1919.4 --> 1922.0: about structuring this, and this might help tee up
1922.0 --> 1926.3: some specific discussion of, and apologies
1926.3 --> 1928.4: that my brain just wasn't working well enough
1928.4 --> 1930.9: to have this answer in my head of like,
1931.3 --> 1934.3: what are the specific problems or issues
1934.3 --> 1938.6: that this agentic model is solving
1938.6 --> 1940.5: for other information sharing partnerships?

1941.3 --> 1943.2: Is there an implementation right now
1943.2 --> 1946.7: with a customer, potential customer or user,
1947.6 --> 1951.3: like to help, obviously there's the user interface,
1951.4 --> 1956.1: and then is that solving friction for the initial cus
tomer,
1956.1 --> 1957.4: the specific platforms,
1957.8 --> 1959.2: the information sharing partnerships?
1959.6 --> 1963.2: Like, I guess, it's just me trying to help think
1963.2 --> 1965.6: through the life cycle of like highlighting,
1965.8 --> 1968.5: like what is this, what infrastructure,
1970.4 --> 1975.3: yeah, what pain points is this proposed infrastructur
e
1975.3 --> 1979.2: gonna solve, we think, and then that will help tee up
1979.2 --> 1981.9: to, you know, amazing organizations like Steel ISAC
1981.9 --> 1984.3: is here, and MITRE, and I don't know if Crypto ISAC,
1984.3 --> 1986.3: I can't see if they're on virtual,
1987.9 --> 1989.8: but if that's a possible walkthrough,
1990.3 --> 1992.5: that if it's okay to walk through it,
1992.6 --> 1994.8: maybe in the course of information sharing,
1995.1 --> 1997.9: like what specifically the pain points are
1997.9 --> 2001.7: that the agentic model wants to be able to solve,
2002.1 --> 2004.5: and then we can maybe tee up some of the questions
2004.5 --> 2006.5: for those partnerships of like does,
2007.0 --> 2010.3: is this something that would be valuable and of use t
o you?
2010.6 --> 2012.8: Or is there a better pain point for us
2012.8 --> 2015.3: to be pointing this underlying infrastructure at?
2024.6 --> 2025.5: Yes, thank you so much.
2025.9 --> 2029.5: Yes, those are really important points.
2030.2 --> 2032.9: So yes, of course, as mentioned,
2033.3 --> 2036.2: today's chatbot is not perfect at all.
2036.8 --> 2042.7: And for example, the initial priority
2042.8 --> 2047.9: prioritization may be privacy preserving infrastructu
re,
2048.5 --> 2049.6: what is chatbot, for example.
2050.4 --> 2054.3: But anyway, we are currently don't know
2054.3 --> 2059.9: if it's really the most important prioritization,
2060.5 --> 2063.3: the points that should be prioritized.
2064.4 --> 2071.0: And so yes, I also suggest to ask
2071.0 --> 2081.8: the pain point for each stakeholder from various sect
ors.
2085.4 --> 2089.1: Yeah, maybe a good place to start would be like,
2089.2 --> 2091.0: who do you envision being the user?
2091.2 --> 2093.5: Is it gonna be Sam at CLISAC?
2093.6 --> 2096.6: Or are you envisioning this being a chat,
2096.7 --> 2098.8: which I think that's what begin,
2098.8 --> 2101.5: the node that begin wants to operate in.

2101.7 --> 2104.6: It's for the operators of the information sharing pla
tform,
2104.7 --> 2108.4: not a chatbot for the consumer at an exchange or what
ever,
2108.6 --> 2113.9: or even interfacing with CLISAC or Ivan or something
else.
2114.2 --> 2116.4: Is that right that the operator, okay, great.
2116.7 --> 2118.2: So sorry, he's nodding his head.
2118.3 --> 2119.0: So anyone virtually.
2119.9 --> 2122.0: So the main users are the operators
2122.0 --> 2123.6: doing the information sharing.
2125.1 --> 2127.5: So then the purpose of this,
2127.5 --> 2129.6: it's just making it like through the chatbot,
2129.7 --> 2133.1: making it easy to identify and distill
2133.1 --> 2135.4: and pull the relevant information
2135.4 --> 2140.3: in like whatever the standardized format is for info
sharing.
2142.9 --> 2144.1: Question mark, I guess.
2144.3 --> 2147.9: Yeah, I think I was, sorry that I'm sure
2147.9 --> 2149.1: that I'm asking you to explain something
2149.1 --> 2151.3: that was already presented and discussed.
2151.5 --> 2154.5: I just wanted to try to in,
2155.6 --> 2157.6: yeah, like more modular terms,
2157.7 --> 2160.7: think about specifically through each step of the pro
cess,
2161.0 --> 2163.5: what it is that the agent will be doing
2163.5 --> 2166.2: and solving as we think it'll operate.
2167.3 --> 2168.7: And we can also turn to Mitchell
2168.7 --> 2169.8: if he's got some thoughts on that.
2170.2 --> 2171.2: Mitchell just arrived.
2173.1 --> 2173.9: No worries.
2175.3 --> 2177.3: I think maybe you can come back to the slide
2177.3 --> 2179.9: presenting the source of information
2182.2 --> 2187.4: because I see different aspects with respect to this
project
2187.4 --> 2190.3: where the interface and being able to use the chatbot
2190.3 --> 2192.7: is one thing and there is definitely a question
2192.7 --> 2195.7: on who is the target user for the chatbot itself.
2196.7 --> 2200.2: But then there are all the other components
2200.2 --> 2203.2: like what are the source of information that are usab
le?
2204.0 --> 2207.3: How you can segregate information among maybe communi
ties
2207.3 --> 2209.2: because some communities will agree
2209.2 --> 2210.6: to share some specific information
2210.6 --> 2214.0: and not necessarily with all the communities.
2214.4 --> 2217.3: So you need to think about how to segregate informati

on.
2218.2 --> 2220.3: Maybe there is also a question
2220.3 --> 2223.8: on how you integrate new evidences
2223.8 --> 2226.4: and how they are weighted in a way
2226.4 --> 2229.9: because you don't want to create a noise
2229.9 --> 2233.6: among database of evidences
2233.6 --> 2235.3: that have been already checked by experts
2235.3 --> 2237.2: and known to be legitimate.
2238.0 --> 2240.8: I guess there are questions also maybe related
2240.8 --> 2245.3: to how you manage sensitive information
2245.3 --> 2249.5: which can be harmful for different reasons.
2252.0 --> 2259.8: But I guess it's all about the perspective of the end users
2259.8 --> 2261.8: of the system and that's a very good point.
2262.1 --> 2263.9: Maybe Mitchell will have comments on this.
2264.2 --> 2267.0: I'm definitely gonna throw this mic straight at Mitchell
2267.0 --> 2268.9: across the room so he better be able to catch.
2269.2 --> 2270.9: You can catch a mic, you can dodge a ball.
2272.9 --> 2275.8: So the question that I have right now,
2275.9 --> 2278.7: so we just got a great presentation on the vision
2278.7 --> 2281.6: for the, because Mitchell just walked in
2281.6 --> 2284.7: for those who are joining us virtually.
2285.5 --> 2287.0: It's just me trying to understand
2287.0 --> 2288.7: from a product development perspective
2288.7 --> 2292.7: and who is the customer and what needs it's filling.
2293.2 --> 2295.6: And maybe it's that it's because we're at step one
2295.6 --> 2298.2: of a lot of steps for developing the capabilities
2298.2 --> 2302.0: of like what is the agent and the chat bot
2302.0 --> 2303.7: that we want to build, like what is that?
2304.1 --> 2306.8: Is this actually part of a broader vision
2306.8 --> 2311.4: of begin creating and operating
2311.4 --> 2313.7: a privacy preserving data lake for enabling
2313.7 --> 2316.0: like the sharing and segregating of specific information
2316.0 --> 2320.4: or like now this is actually part of a broader coalition
2320.4 --> 2323.1: of work that we may do with information sharing organizations
2323.1 --> 2324.8: about how each of them may want
2324.8 --> 2327.1: to manage their data but then with the standards
2327.1 --> 2330.0: of what is necessary for information sharing
2330.0 --> 2334.0: for things like asset recovery and cyber defense
2334.0 --> 2337.0: that the agent allows for like you to input
2338.1 --> 2340.0: based on this particular use case,
2340.1 --> 2341.9: whether it's cybersecurity to patch a fix
2341.9 --> 2345.4: in a smart contract or if the fix is to go

2345.4 --> 2350.2: and alert to Julian at Begin Exchangers,
2350.4 --> 2353.7: I don't know, whatever, that these proceeds are fraud
ulent
2353.7 --> 2354.6: so please stop it.
2355.4 --> 2358.0: Just trying to understand like is the current vision
2358.0 --> 2359.4: just thinking about the chat bot
2359.4 --> 2361.8: and that initial phase of info sharing
2361.8 --> 2365.2: or is it in fact part of a broader ecosystem
2365.2 --> 2368.8: since the slide showed a really more comprehensive fr
amework
2368.8 --> 2369.5: of info sharing.
2370.2 --> 2372.1: I'm not sure like where we are
2372.1 --> 2373.4: if all's kind of on the table.
2374.3 --> 2376.3: So like, oh good, I don't have to throw it at Mitch.
2376.3 --> 2377.1: He's got his own mic.
2377.5 --> 2379.5: Yeah, good to be here.
2380.2 --> 2381.6: Sorry, I'm a little bit late.
2381.6 --> 2383.4: To answer that question directly,
2384.4 --> 2385.7: yes, broader ecosystem.
2387.2 --> 2392.1: The Telegram chat bot is almost like the public face
of that
2392.8 --> 2395.9: and what's interesting about the way
2395.9 --> 2397.7: that you can set up these knowledge graphs
2397.7 --> 2402.2: that the chat bots query is that you can choose
2402.7 --> 2409.5: which graph and how much of the episodic knowledge
2410.1 --> 2410.8: it is asking.
2410.8 --> 2414.1: So if Carol goes to this chat bot
2414.1 --> 2417.3: and has discovered some new threat
2417.3 --> 2420.4: and starts learning that threat
2420.4 --> 2423.3: or understanding that threat with the chat bot,
2423.4 --> 2425.8: that is specific to your episodic knowledge
2425.8 --> 2428.3: and your relationship with that agent.
2428.8 --> 2432.7: So what's interesting there is other people
2432.7 --> 2435.0: can then go query that agent
2435.0 --> 2440.6: and unless they have received some sort of signal fro
m you
2440.6 --> 2444.4: and you could choose to do a selective disclosure
2444.4 --> 2448.5: via the agent to enable discovery
2448.5 --> 2450.8: that you've analyzed this new threat that's happened
2451.3 --> 2453.5: and then when people discover that,
2453.9 --> 2456.7: they can just share a short,
2458.3 --> 2461.1: perhaps even machine readable string of information
2461.1 --> 2465.4: to then haul that episodic knowledge of information
2465.4 --> 2468.6: that you went through and improved the knowledge base
 with.
2468.6 --> 2470.9: So two things are cool here.
2471.0 --> 2474.3: One is the agent acts as a layer of obfuscation

2474.9 --> 2478.8: to allow for the investigators
2479.8 --> 2483.9: to maintain privacy from prompt injection.
2484.5 --> 2487.2: So if someone goes to the same chat bot
2487.2 --> 2489.9: and works out like it's trying to work out
2489.9 --> 2491.2: who the investigators are,
2492.3 --> 2494.4: that can be hidden behind the agent
2495.2 --> 2498.2: who is the query of the knowledge graphs.
2498.2 --> 2501.9: So you can have pseudonymity with the agent
2501.9 --> 2506.4: and then the other cool thing is you can create versi
ons
2507.0 --> 2508.4: which you were alluding to
2508.4 --> 2510.7: where we have a different graph for ISAC,
2510.8 --> 2511.5: we have a different graph
2511.5 --> 2513.6: for all of these different organizations
2514.4 --> 2516.3: and then there is some sort of protocol
2517.5 --> 2521.3: of information sharing and like governance around tha
t
2521.3 --> 2523.6: when we converge these graphs.
2523.7 --> 2526.5: So you have one organization,
2526.7 --> 2527.8: maybe it's a government department
2527.8 --> 2529.1: that has a whole bunch of information
2529.1 --> 2530.8: that they're querying on the chat bot
2530.8 --> 2534.8: so then it matches with the knowledge
2535.5 --> 2540.0: in terms of the strategies for mitigating that threat
2540.0 --> 2543.9: or just guidance on how to deal with that issue.
2544.7 --> 2548.4: And then based on that, it then compiles up
2548.4 --> 2551.8: and then we can have these almost like a merge situat
ion
2551.8 --> 2555.4: where we have one begin knowledge graph database
2555.4 --> 2556.9: that the agent always queries
2556.9 --> 2559.6: but in a privacy preserving way
2559.6 --> 2566.0: and then there are other versions of that
2566.0 --> 2573.3: which give more information based on trust over time
2573.3 --> 2576.5: with the participants, hope that makes sense.
2577.7 --> 2579.8: Yeah, and if I'm dragging this out,
2580.3 --> 2583.9: some of it is also I think there's some really intere
sting
2583.9 --> 2586.4: like unique diverse stakeholders sitting in the room
2586.4 --> 2588.8: and so even though I know that you've already
2588.8 --> 2589.8: kind of talked through some of this
2589.8 --> 2592.1: where I think the implications are there.
2592.9 --> 2594.6: If you don't mind maybe humoring me
2594.6 --> 2596.2: or highlighting if you think that this would be
2596.2 --> 2597.5: not a super helpful exercise.
2598.6 --> 2600.4: Thinking about like on the slide,
2600.5 --> 2602.3: you guys mapped out all the different stakeholders
2603.8 --> 2606.9: like with we've got, is CryptoISAC in here

2606.9 --> 2607.8: or did they go next door?
2607.9 --> 2608.6: They may have gone next door.
2609.4 --> 2612.0: The Japan CryptoISAC, well, so Japan CryptoISAC is he
re,
2612.1 --> 2613.1: CL911 is here.
2614.3 --> 2620.1: We also have NIST is on, MITRE is here like represent
ing,
2620.5 --> 2621.8: like if you're thinking about them
2621.8 --> 2624.3: from like a national vulnerability database, CVE,
2624.8 --> 2627.5: sort of like repository folks versus the operators
2627.5 --> 2630.5: that are trying to enable specific investigators
2630.5 --> 2633.1: and their partnerships to go and actually do what the
y do
2633.1 --> 2635.7: to try to help defend like the sector
2635.7 --> 2640.0: and go try to recover assets and proceeds for victims.
2640.9 --> 2645.1: You have CCSS as well, like in their work
2645.9 --> 2646.9: focusing on standards,
2647.2 --> 2650.3: like maybe thinking about a couple of those specific
players
2650.3 --> 2655.0: like how do we think that this model,
2655.6 --> 2656.8: like even just in a minute,
2656.9 --> 2657.9: even though I know I've taken five minutes
2657.9 --> 2663.3: asking this question, like how would they best use i
t?
2663.3 --> 2664.7: Like for each of those archetypes,
2664.8 --> 2665.8: maybe if we walk through that,
2665.9 --> 2667.0: that might also be helpful
2667.0 --> 2669.5: in like stirring some interesting thoughts for them
2669.5 --> 2671.4: on like does this solve a problem for them
2671.4 --> 2675.1: and what are the right questions around like data pro
tection
2675.1 --> 2678.0: and minimization and conditions
2678.0 --> 2681.3: and standard work on the kind of information to be sh
ared.
2681.5 --> 2683.8: I don't know, I was just thinking that walking throug
h
2684.2 --> 2686.5: like two of those scenarios might be really interesti
ng.
2686.6 --> 2687.7: Oh, we also have regulators in the room.
2688.2 --> 2691.8: So whatever, pick your poison on which stakeholder,
2691.9 --> 2693.3: but maybe that kind of walkthrough would be fun.
2693.8 --> 2698.6: Yeah, so one thing that I'll just start with
2698.6 --> 2703.1: is the AEI technologies LLMs that we're talking about
2703.6 --> 2706.8: and LLMs are really good at two things.
2707.3 --> 2708.9: One is compression of knowledge
2708.9 --> 2711.3: and the other is reconstruction of that knowledge
2711.3 --> 2712.7: in someone else's context.

2713.3 --> 2716.5: So when we think about creating an interface
2717.0 --> 2719.8: between multi-stakeholders and for example,
2720.5 --> 2724.2: Crypto ISAC who has an interface with the industry
2724.2 --> 2726.8: that receives threats and then tries to roll them up
2726.8 --> 2728.2: to then talk to NIST
2728.2 --> 2730.4: who has how to deal with those threats,
2732.6 --> 2735.6: you get a process of compression and reconstruction
2735.6 --> 2736.8: at every single layer there,
2737.1 --> 2741.6: which means that what happens is the compression of t
hat
2741.6 --> 2746.1: becomes almost like the key to unlock the reconstruct
ion
2746.1 --> 2747.8: across multiple stakeholders.
2748.4 --> 2752.0: So if all of these organizations receive the same doc
ument,
2752.1 --> 2753.3: which is this long document,
2753.4 --> 2756.3: which is an investigation analysis of a particular th
reat
2756.3 --> 2760.1: or response that happened and using their agent,
2760.4 --> 2763.0: which has access to the either shared
2763.0 --> 2765.9: or multiple knowledge graphs,
2766.0 --> 2768.5: depending on the way that the information security is
 set up
2769.3 --> 2772.5: all go and do a prompt that compresses that informati
on
2773.2 --> 2775.3: into I like Proverbs.
2775.8 --> 2778.6: Proverbs is the language device in grammar
2778.6 --> 2781.9: and what's unique or what's cool about it
2781.9 --> 2784.6: is that it exists in all languages
2785.2 --> 2789.0: and it becomes cross language, a proverb.
2789.9 --> 2794.3: So you can compress all of the information into a pro
verb
2794.3 --> 2797.0: and then share that proverb among each other.
2797.6 --> 2800.6: And say, for example, Carol, you had a particular ana
lysis
2800.6 --> 2803.4: from your perspective of this threat or response
2803.4 --> 2804.7: and you compress it into a proverb,
2805.2 --> 2806.4: you then send that to NIST,
2806.9 --> 2808.6: NIST then writes that proverb
2808.6 --> 2811.0: through an encrypted secure channel.
2811.5 --> 2813.1: So there is an information leakage.
2813.1 --> 2816.3: So the whole information isn't being shared
2816.3 --> 2818.6: when you send it to the counterparty,
2818.6 --> 2819.5: you just send the proverb.
2820.0 --> 2821.1: And then the counterparty NIST
2821.1 --> 2822.9: puts the proverb into the knowledge graph.
2823.1 --> 2825.9: What the AI is good at is reconstructing that

2826.4 --> 2828.3: and being able to episodically work out
2828.9 --> 2831.8: all of the full information
2831.8 --> 2833.5: that was compressed into the proverb,
2833.8 --> 2837.5: but because it's NIST who has their own system prompt
2837.5 --> 2842.1: and their own LLM design that accesses that knowledge graph,
2842.1 --> 2844.6: it then gets reconstructed in NIST's perspective
2845.5 --> 2846.6: and then they compress it.
2846.8 --> 2848.7: And then you get this semantic matching
2848.7 --> 2852.0: along the way of proverb into full document
2852.0 --> 2853.6: into proverb into full document.
2854.2 --> 2857.5: And me personally, and on a research side,
2857.6 --> 2862.2: I'm really interested in like how much we can,
2862.5 --> 2865.3: how much information or weight we can give to these words.
2865.6 --> 2871.0: And if we're able to give lots of weight to two sentences
2871.0 --> 2872.9: or one and a half sentences,
2873.4 --> 2875.7: then that information never exists,
2876.3 --> 2878.8: but access to the knowledge graph to reconstruct
2878.8 --> 2880.2: to the specific episode
2880.2 --> 2883.6: that someone contributed that information, that exists.
2884.1 --> 2885.4: So you just need to make sure
2885.4 --> 2887.4: that that knowledge graph is highly secure
2887.4 --> 2889.3: in terms of access control,
2889.5 --> 2894.5: but interacting with it within your own stakeholder context
2895.4 --> 2896.3: just happens naturally
2896.3 --> 2899.8: because you get this compression key along the way
2899.8 --> 2901.8: by just building that into the process.
2903.3 --> 2904.6: Hope that answers your question.
2905.5 --> 2908.6: The overlap is what I think is most important here
2908.6 --> 2911.0: where you have all of these organizations
2911.0 --> 2915.8: recreating the same document from the same initial source.
2916.1 --> 2918.1: And then that overlap then compiles
2918.1 --> 2921.1: and creates this new sort of master document.
2921.4 --> 2923.1: And then that gets rolled up
2923.1 --> 2926.7: into the almost like the master knowledge graph in a way
2926.7 --> 2933.7: that is, I don't know if it's more secure,
2933.9 --> 2934.8: or it's more public.
2935.0 --> 2937.6: I guess it would depend on the governance and the structure.
2937.9 --> 2941.2: It could be the greater knowledge graph is the public one

2941.2 --> 2942.5: that has all of the information.
2942.7 --> 2946.2: And then there's smaller subsets that each organizati
on has
2946.2 --> 2947.5: that then rolls up into that.
2950.0 --> 2952.4: I'm excited for that process,
2953.3 --> 2955.0: creating a secret language
2955.0 --> 2958.2: among threat and information response.
2958.4 --> 2961.4: And the follow on to that is
2961.4 --> 2963.9: you can actually then compress the proverbs
2963.9 --> 2966.3: into machine readable language
2967.1 --> 2969.3: and just share machine readable signals,
2970.0 --> 2975.4: which then has a human readable version of that, righ
t?
2975.9 --> 2981.7: So the red team attacked this smart contract
2981.7 --> 2984.4: and discovered this threat.
2985.3 --> 2990.5: And that is not as beautiful as the LLM is gonna make
 it
2990.5 --> 2993.1: because LLMs are good at compressing the language
2993.1 --> 2996.8: into like the right terms based on all of the text.
2997.0 --> 2998.6: But if I then sent to you,
2998.9 --> 3001.9: the red team is going to attack this smart contract
3001.9 --> 3004.1: and you got that proverb
3004.1 --> 3006.4: and sent it into our shared knowledge base,
3006.9 --> 3008.9: you could then prompt your way through
3008.9 --> 3011.3: the full reconstruction of how we got to that point
3011.3 --> 3017.7: without revealing who trained the knowledge on that.
3019.2 --> 3020.0: I'm gonna pause.
3026.3 --> 3031.2: So, Michel, you mentioned a few things
3031.9 --> 3032.8: which are very interesting.
3033.8 --> 3038.6: I guess the, what is to me,
3038.6 --> 3040.9: what you emphasize with respect to
3041.5 --> 3043.7: being able to compress the information
3043.7 --> 3047.2: that is being shared between different communities
3047.2 --> 3048.3: or different organizations
3049.1 --> 3053.2: in order to kind of minimize the potentially
3053.2 --> 3055.2: is the leakage of information
3055.2 --> 3056.8: that you provide to another organization.
3057.3 --> 3061.0: It's one aspect, it's being able to share information,
3061.2 --> 3064.0: but basically you share the minimum
3064.5 --> 3066.7: to allow another party to reconstruct
3067.3 --> 3070.1: within their own knowledge based on what you shared.
3070.3 --> 3072.1: So, it's a kind of, it's an information sharing
3072.7 --> 3075.5: with minimizing information
3075.5 --> 3078.1: that might not be known by someone else
3078.7 --> 3080.5: and they would be able to reconstruct
3081.0 --> 3085.5: and to kind of finding something which is comprehensi
ve

3085.5 --> 3088.3: only if they already have sufficient knowledge
3088.3 --> 3090.1: in order to interpret this information.
3091.3 --> 3092.1: So, that's the first thing.
3092.2 --> 3094.3: And the second one is being able, at the end,
3094.9 --> 3098.7: to facilitate somehow the interoperability
3098.7 --> 3103.2: between different AI models among different organizat
ions.
3103.6 --> 3108.3: So, even if you have a different knowledge graph,
3108.4 --> 3110.6: a different structure, a different way to analyze
3110.6 --> 3113.2: and to investigate threat intelligence,
3113.7 --> 3116.9: then you are able to transfer the information
3116.9 --> 3121.9: to make it, well, meaningful in a new context,
3122.1 --> 3123.4: which is a second one.
3123.4 --> 3128.7: The fact that is, maybe the fact that we can do it
3128.7 --> 3131.2: with kind of a secret language
3131.9 --> 3135.8: might be something which is an interesting feature,
3135.9 --> 3137.1: but maybe it's not something
3137.1 --> 3139.0: that the stakeholders are looking at.
3139.4 --> 3141.8: So, maybe this is just an additional feature,
3142.0 --> 3144.8: but it's something which can be seen also as,
3145.6 --> 3146.9: well, at least so far,
3147.7 --> 3151.1: maybe we need to define whether this is something
3151.1 --> 3154.2: for which they have a needs or not.
3155.4 --> 3158.8: But I think the explanation was quite interesting
3159.7 --> 3160.9: on that side.
3161.7 --> 3163.8: And those are, yes.
3164.1 --> 3165.3: On the secret language point,
3166.2 --> 3168.7: it's to what extent the information needs to be secur
e.
3168.9 --> 3171.5: Like, you could go as far as zero knowledge,
3172.2 --> 3176.3: or you could be as exposed as we,
3176.7 --> 3179.1: this is just a sanctions thing
3179.1 --> 3182.0: that we need to expose on the knowledge graph now
3182.0 --> 3182.6: to everyone.
3183.3 --> 3185.4: So, yeah, just to answer that question,
3185.5 --> 3187.3: I think it's to what extent, but go ahead.
3191.2 --> 3191.6: Yeah.
3192.7 --> 3196.8: So, and I know, like, I love the beautiful,
3197.1 --> 3198.0: like holistic vision,
3198.3 --> 3200.1: which is really helpful to also know, like that,
3201.2 --> 3203.0: like, and I guess, and I did ask about,
3203.1 --> 3204.6: like what the whole ecosystem was
3204.6 --> 3205.9: that we wanted to enable and build.
3205.9 --> 3209.8: I'm also trying to think about how to really clearly
3209.8 --> 3213.2: articulate to some of like what the participants here,
3213.4 --> 3216.7: like what it would look like for them in practice.
3217.3 --> 3220.5: Like, so I don't know if there is a scenario

3220.5 --> 3221.7: and maybe like this is some,
3221.8 --> 3223.8: whether we do it right now in this session,
3223.8 --> 3225.8: or that's something that we collab on
3225.8 --> 3227.7: and try to throw into the next session,
3228.4 --> 3231.7: thinking on like, okay, like a, you know,
3231.7 --> 3234.2: like North Korea just hacked by a bit,
3234.7 --> 3236.7: there's a lot of cyber and vulnerability information
3236.7 --> 3238.7: around things that need to get fixed and patched.
3239.2 --> 3241.7: And there's now proceeds that are being moved
3241.7 --> 3243.9: and a lot of different regulatory ecosystems,
3244.1 --> 3245.5: including sanction stuff,
3245.6 --> 3247.1: like thinking through like step-by-step,
3247.6 --> 3250.5: what is the vision of what this,
3250.8 --> 3254.7: of what this agent looks like for interaction,
3255.0 --> 3258.7: for, you know, like one of those customer archetypes
3258.7 --> 3260.6: that you guys had at the bottom of the screen
3260.6 --> 3261.7: on like the different stakeholders.
3262.2 --> 3264.8: Maybe we could think about like highlighting for them,
3264.9 --> 3267.5: like, this is what you interacting with this
3267.5 --> 3268.5: looks like right now,
3268.6 --> 3273.1: which is maybe solving language translation issues
3273.1 --> 3275.3: and like enabling that, that info sharing.
3275.5 --> 3278.6: So like, that's like one of many different benefits,
3278.7 --> 3280.2: but like trying to think through,
3280.3 --> 3281.5: walking through that kind of scenario
3281.5 --> 3283.3: of the way that we would want it to operate
3283.8 --> 3287.0: and trying to make really tangible to the partners
3287.0 --> 3288.9: that would use it in the ecosystem,
3289.1 --> 3289.8: what that would look like.
3290.3 --> 3291.0: I don't know.
3291.2 --> 3292.9: We can think about that in the next session,
3293.0 --> 3294.8: do you want to, or talk about it now,
3295.2 --> 3296.6: whatever you want.
3296.8 --> 3298.3: That's what I was trying to get at,
3298.3 --> 3300.3: but I think I didn't clearly articulate it before.
3301.4 --> 3303.7: So we wanted to have some kind of discussion
3303.7 --> 3306.8: about the use cases of this identity care system.
3307.4 --> 3309.8: Carol, so we want to have this kind of discussion
3310.8 --> 3311.8: about the use cases.
3313.3 --> 3316.9: One of the important, interesting use cases about
3317.9 --> 3322.0: what we couldn't do that at the Bybit hack incident,
3322.5 --> 3324.3: you know, that the methodology of attack
3324.3 --> 3327.5: for the Bybit hack was almost all
3327.5 --> 3331.5: had the attacking methodology to, you know,
3331.8 --> 3336.8: GMA, Japanese GMA Bitcoin.
3337.5 --> 3339.3: It's almost the same methodology,
3340.2 --> 3342.3: but then, you know, at that moment, you know,

3342.3 --> 3345.2: there are Bybit guys that didn't know about it,
3345.9 --> 3351.8: but if we have already had some kind of knowledge bas
e
3351.8 --> 3354.2: about attacking methodology or something like that,
3354.4 --> 3356.1: or potential vulnerability,
3357.1 --> 3361.3: so if, you know, Bybit guys find some suspicious thin
gs,
3361.5 --> 3362.9: or they're wrong, something like that,
3363.0 --> 3365.2: they put that log to the identity care system,
3365.3 --> 3368.6: then they can have a clear idea of what might be happ
ening.
3369.4 --> 3372.6: So that is one strong use case of this identity care
system.
3374.3 --> 3378.0: Yeah, just to add to that, it's to do with discovery.
3379.2 --> 3382.3: So if the Bybit hack,
3382.5 --> 3385.0: if the knowledge base was trained on the Bybit hack,
3385.1 --> 3387.6: or the DMM hack, sorry, which happened first,
3388.2 --> 3391.2: and then the Bybit hack happened all of a sudden,
3391.8 --> 3394.2: and someone put their investigation
3394.9 --> 3397.5: and full reconstruction of analysis of the Bybit hack
3398.2 --> 3399.8: into this knowledge base,
3399.8 --> 3404.9: the compression will be very similar to the DMM compr
ession.
3405.5 --> 3407.5: So then there's a discoverability around,
3407.7 --> 3409.0: this has happened before,
3409.8 --> 3412.4: maybe we should use some of the episodic knowledge
3412.4 --> 3414.1: that we went through for the DMM hack
3414.1 --> 3416.0: in order to inform how,
3417.0 --> 3419.0: and that creates almost like a,
3420.7 --> 3423.5: the longer you are participating in this graph,
3423.6 --> 3425.9: the more promises you make
3425.9 --> 3428.3: to improve the knowledge base as a participant,
3428.3 --> 3431.4: the more trust you get into the graph,
3431.7 --> 3434.1: the more access you could potentially get
3434.1 --> 3438.5: on in terms of a ratio for how much information
3439.2 --> 3440.8: the agent in terms of,
3441.2 --> 3443.8: and you can just code this because it's the tokens,
3444.2 --> 3445.5: like the total token spend.
3446.4 --> 3449.6: So how much information the agent is going to service
3449.6 --> 3453.4: back to the person when they write a proverb
3453.4 --> 3456.7: or give the machine readable string to the agent.
3456.7 --> 3461.7: And then that creates this sort of chain of,
3462.0 --> 3466.8: within the way that the AI tracks that information,
3467.0 --> 3471.7: it creates a chain of reason, reasoning.
3472.3 --> 3475.5: So then the DMM hack is always going to be cited
3475.5 --> 3477.2: when the Bybit hack is cited
3477.2 --> 3479.0: because they had the same exploit,

3480.9 --> 3482.1: if that makes sense.
3482.5 --> 3485.6: And to,
3486.7 --> 3489.4: add to that in terms of the use case,
3490.5 --> 3493.4: when you get these multiple participants
3493.4 --> 3496.6: all contributing and making promises and following th
rough
3496.6 --> 3498.5: or making promises and not following through,
3500.0 --> 3504.0: that is an independent graph or,
3505.4 --> 3509.2: yeah, graph that you overlay to the shared begin
3509.9 --> 3511.1: knowledge graph of all the information
3511.8 --> 3515.6: and the overlap of that then creates an emergent grap
h,
3515.6 --> 3516.9: which is a trust graph.
3517.7 --> 3520.0: And I'll talk more about that
3520.0 --> 3523.0: in the proof of personhood session,
3524.3 --> 3526.3: but this has been like a lot of the work
3526.3 --> 3528.7: that I've been doing for the last eight months
3528.7 --> 3533.1: is trying to express
3533.6 --> 3536.7: that this three graph one coordinate system
3536.7 --> 3540.9: is actually a way better proof of personhood system
3540.9 --> 3543.2: for knowledge sharing communities.
3543.5 --> 3545.1: Obviously, when we're going to the airport,
3545.1 --> 3546.4: we're still going to use biometrics,
3546.5 --> 3548.3: but for communities like begin,
3548.9 --> 3552.5: if you need to do some sort of proof of personhood cr
edential
3552.5 --> 3554.2: for the participants in this room,
3554.8 --> 3558.2: if I could prove that I was here today
3558.2 --> 3559.9: and I contributed to the knowledge graph
3559.9 --> 3561.9: and then in six months time in DC,
3562.3 --> 3565.3: I could prove that I contributed to the knowledge gra
ph.
3565.5 --> 3568.2: All I would need to do is show that it was my traject
ory
3568.2 --> 3570.9: through the graph from point A to point B
3573.5 --> 3576.6: that I am a person that participates in this ecosyste
m.
3576.9 --> 3579.1: And again, that is information minimalization.
3579.8 --> 3583.0: So all I'm doing is saying that I contributed at this
 point
3583.0 --> 3584.8: and everyone respected that
3584.8 --> 3586.3: because I followed through on my promise
3586.3 --> 3587.7: to contribute to this knowledge.
3588.2 --> 3591.1: And then six months down the time, I contributed to t
his.
3591.6 --> 3596.1: We mapped the, it would be helpful,
3597.4 --> 3600.7: can begin admin chair,

3600.7 --> 3602.9: screen and go to a website.
3605.1 --> 3607.8: I can visualize this quickly.
3608.6 --> 3609.7: Yeah. Oh, is it over there?
3610.8 --> 3613.5: I can, I can jump on the computer over there.
3618.0 --> 3621.1: So I've built a visualization of this
3621.1 --> 3624.2: over the last week for my research.
3624.5 --> 3628.3: So if we could share screen and go to Spellweb.ai.
3640.4 --> 3641.7: Spellweb.ai.
3646.2 --> 3648.9: Okay, now click, zoom in
3648.9 --> 3650.5: and click on one of these little bubbles.
3651.3 --> 3655.0: Actually search, what should we search, ZKP?
3657.2 --> 3662.2: Sorry, it's at the top, search ZKP.
3665.4 --> 3667.6: And then hold on one of those
3671.8 --> 3673.1: and zoom out a little bit
3673.1 --> 3676.1: so we can see what's going on here.
3678.5 --> 3680.6: So let me control for a bit.
3682.6 --> 3685.3: Oops, sorry.
3687.8 --> 3690.7: Okay, yeah, yeah, not really.
3691.4 --> 3691.5: Okay.
3695.4 --> 3696.7: I'm used to inverse.
3698.3 --> 3701.2: So this is just a zero knowledge proof here,
3701.7 --> 3704.1: but imagine this to be all of the knowledge
3704.1 --> 3705.3: of the threat response.
3707.1 --> 3711.0: And what I've done here is I prompt my way through.
3711.4 --> 3715.7: I then create a connection from here.
3717.0 --> 3718.5: We'll start a waypoint.
3719.7 --> 3721.7: And I'm just randomizing,
3721.8 --> 3724.8: but you could imagine the AI pulls this themselves
3724.8 --> 3726.9: based on the types of prompts that you do.
3729.7 --> 3732.8: And this is the logic that the AI goes through, righ
t?
3733.0 --> 3734.9: That you're almost dictating.
3736.3 --> 3740.6: We'll then give that a machine readable string.
3740.9 --> 3743.8: So this is that compression key that I was talking ab
out.
3749.0 --> 3750.4: And we'll save it.
3752.2 --> 3753.1: Oops.
3760.6 --> 3764.6: So the path that is created here
3764.6 --> 3767.1: is incredibly unique.
3768.1 --> 3772.5: The overlap and the way that the person prompts
3772.5 --> 3775.5: through the knowledge graph will be unique
3775.5 --> 3777.8: and probabilistic every single time.
3778.5 --> 3782.4: And if there is a way for us to get the coordinates
3782.4 --> 3784.8: or the trajectory and then wrap that
3784.8 --> 3786.9: into a zero knowledge proof,
3787.4 --> 3791.4: then it's a proof of person based on knowledge sharin
g,

3792.3 --> 3792.9: if that makes sense.
3793.6 --> 3795.8: And that adds trust over time.
3796.4 --> 3800.2: And over time, that trust can then give more access
3800.9 --> 3803.3: and you can draw larger constellations.
3803.7 --> 3804.9: And perhaps even over time,
3805.3 --> 3809.6: that contributing and having these proofs of trajecto
ry
3809.6 --> 3810.8: through the knowledge graph
3810.8 --> 3813.6: then gives you the access to write directly to it.
3814.3 --> 3816.6: But that would be a progressive trust system.
3817.0 --> 3820.6: So I hope that maybe helps the visualization of this.
3821.6 --> 3823.6: But the shape that you make based on your path
3823.6 --> 3826.1: through the knowledge graph is extremely unique
3826.1 --> 3829.7: and it can help us maintain trusted actors
3829.7 --> 3833.1: within the ecosystem that is sort of accessing
3833.1 --> 3834.5: these knowledge graphs, right?
3835.4 --> 3836.4: I'm gonna pause.
3844.5 --> 3847.5: Hi, it's okay to share this session.
3847.5 --> 3851.6: Sorry, this is Sasaki from J.P. Kudo-Isaac.
3852.1 --> 3855.7: So J.P. Kudo-Isaac was organized last January
3856.5 --> 3858.0: to gather many information,
3858.5 --> 3860.5: to communicate with each other
3860.5 --> 3862.8: in cryptocurrency company in Japan.
3863.5 --> 3867.3: So the objective of this AI agent is because
3867.3 --> 3871.5: J.P. Kudo-Isaac would like to receive many informatio
n.
3872.1 --> 3873.4: And if something happens,
3873.5 --> 3876.8: so J.P. Kudo-Isaac would like to ask this AI agent
3877.8 --> 3881.6: by using the Japanese language and so on.
3882.2 --> 3884.8: So I think this is useful for J.P. Kudo-Isaac
3884.8 --> 3888.5: if we can get this information easily.
3889.0 --> 3890.1: So this is one opportunity.
3892.7 --> 3896.2: And the good thing about having AI as the interface
3896.2 --> 3900.4: is as we said, the language barrier is somewhat solve
d
3900.4 --> 3901.6: by how good the model is.
3902.9 --> 3905.7: Yes, so unfortunately, so J.P. Kudo-Isaac,
3905.7 --> 3907.7: so cryptocurrency company in Japan
3908.8 --> 3911.0: cannot so understand English,
3911.3 --> 3914.8: but if so we can ask with Japanese,
3915.3 --> 3916.7: so it's really important thing
3916.7 --> 3919.0: to receive the information soon.
3931.2 --> 3932.9: Please excuse my English.
3932.9 --> 3936.1: I am with a cryptocurrency vendor named Ginkgo,
3936.4 --> 3939.0: and I would like to share a brief thought
3939.0 --> 3942.2: based on my recent practical experience.
3942.9 --> 3945.6: Driven by a very similar problem awareness

3945.6 --> 3947.7: to what was discussed today,
3948.3 --> 3951.5: I recently led a working group at JCBA,
3951.9 --> 3954.4: Japan Crypto Asset Business Association,
3954.8 --> 3959.4: under Sasaki, to build a knowledge base.
3959.4 --> 3964.2: We actually just released a beta version last month,
3964.3 --> 3966.2: starting with a leading list
3966.2 --> 3969.4: that aggregate past industry documents.
3970.1 --> 3972.8: Through that process, I strongly agree
3972.8 --> 3976.7: with the direction of this CHAPO initiative
3976.7 --> 3978.0: at the same time.
3979.1 --> 3983.2: I would like to humbly share two learnings
3983.2 --> 3987.5: from our R&D that might be helpful for this project.
3988.5 --> 3992.2: First, we realized that while a chatbot
3992.2 --> 3995.1: is an excellent interface,
3995.7 --> 4000.0: that the core focus needs to be
4000.0 --> 4003.1: on database operation and management,
4003.9 --> 4009.7: especially exploring how to automate data ingestion
4010.4 --> 4012.5: to minimize manual operation,
4012.5 --> 4017.5: while strictly managing input permissions
4017.5 --> 4023.0: and data quality and incentives seems very important.
4023.9 --> 4028.1: Second, we found that merely sharing
4028.1 --> 4031.7: publicly available information
4031.7 --> 4036.0: is not enough to truly break down silos.
4036.4 --> 4039.9: What seems more critical is establishing
4039.9 --> 4046.0: a safe harbor, a liability-free environment.
4046.7 --> 4051.6: This is necessary so that security practitioners
4054.2 --> 4057.6: within organizations can smoothly share
4057.6 --> 4066.0: their tech knowledge and early-stage threat instituti
ons
4066.0 --> 4071.5: without fear of compliance or reputational risks.
4071.9 --> 4077.0: I hope these insights are helpful for the discussion.
4077.2 --> 4077.8: Thank you.
4080.2 --> 4080.5: Sorry.
4083.4 --> 4083.8: I agree.
4084.0 --> 4086.9: This all leads to a shared database.
4088.5 --> 4091.4: Just the chatbot is the interface
4092.0 --> 4094.0: and you can have a private chatbot
4094.0 --> 4095.4: and you can have a public chatbot
4097.0 --> 4100.0: and you can have versions of,
4100.3 --> 4104.3: so one chatbot could learn
4104.9 --> 4107.5: based on the current state of the database
4107.5 --> 4111.6: and then Ginkgo has their own version of that
4111.6 --> 4115.9: and they add all of their own knowledge to that chatb
ot
4116.6 --> 4118.4: and then there would be some sort of ceremony
4119.2 --> 4121.6: between Ginkgo to then update
4121.6 --> 4125.4: the begin sort of parent knowledge base.

4125.7 --> 4130.2: So then all of the chatbots that get spawned,
4130.2 --> 4134.6: which have access to this, get that knowledge update
4135.2 --> 4139.5: and then that's where, as I was mentioning before,
4140.0 --> 4145.3: you use that path as the mechanism
4145.3 --> 4150.1: for developing a progressive trust.
4151.1 --> 4153.2: So the more things that you contribute,
4153.9 --> 4156.9: the more times that those contributions are correct
4156.9 --> 4160.6: and effectively add to the knowledge base,
4160.9 --> 4166.9: the more ability you have to write to the database
4166.9 --> 4168.6: as opposed to just read it.
4169.8 --> 4174.2: Yeah, so LLM is about the language model.
4174.7 --> 4176.8: So it's a technology to overcome
4176.8 --> 4177.8: the difference of language.
4178.7 --> 4180.4: That is the main functionality
4180.4 --> 4182.2: of the language model technology.
4183.0 --> 4186.4: So the reason why that using LLM
4186.4 --> 4190.4: and the agentic system for their knowledge base
4190.4 --> 4192.4: of the cyber security is very important
4192.4 --> 4195.4: because so we can overcome the difference
4195.4 --> 4197.1: of the natural language, Japanese, English,
4197.3 --> 4201.4: other languages because that's the DMA Bitcoin
4202.1 --> 4203.2: isn't happening in Japan.
4203.4 --> 4206.2: Many discussion was done in Japanese
4206.2 --> 4208.5: but this is one of the reason why,
4208.7 --> 4211.2: not many reason, but one of the reason why
4211.2 --> 4215.0: that private didn't know about that,
4215.1 --> 4215.7: what happened in Japan.
4216.8 --> 4220.2: Of course that Japanese, it's a discussion,
4221.5 --> 4224.9: the Japanese police ask DMM or other companies
4226.4 --> 4228.2: don't anything about that but anyway,
4228.7 --> 4230.9: this is another story but at the same time
4230.9 --> 4232.6: that so when some incident happened,
4233.2 --> 4235.7: the language among engineers, operators
4235.7 --> 4237.6: are very different from the language
4238.2 --> 4241.9: in regulators like the JFSA or police.
4242.5 --> 4244.4: So we need to have some translator
4244.4 --> 4246.2: between the different stakeholders.
4246.7 --> 4248.5: You know, LLM is a very powerful tool
4248.5 --> 4249.9: to overcome that kind of difference.
4255.8 --> 4258.9: Is part of implementation of it,
4259.3 --> 4260.7: and it sounds like some of the partnership
4260.7 --> 4264.3: that's already underway, do we feel like we know
4264.3 --> 4267.3: what some of the besides playing with the chat bot
4267.3 --> 4268.9: that's now live and using that,
4269.0 --> 4271.4: like what the steps are that you see
4271.4 --> 4275.3: to optimize its integration and efficacy?
4275.7 --> 4278.7: Like you mentioning how much a lot of this,

4278.8 --> 4281.2: how much it relies upon the common database.
4282.6 --> 4285.8: Is the implication for like for begin
4285.8 --> 4288.2: to pull information from a lot of public repositories,
4288.6 --> 4292.2: is it that how much of it is asking for institutions
4292.2 --> 4296.7: and entities to proactively push information
4296.7 --> 4299.5: specifically into this central data repository?
4300.8 --> 4305.3: Is that also like presumably that is operated by begi
n,
4305.9 --> 4307.6: so it's not just the chat bot,
4307.7 --> 4309.8: it's also like the infrastructure for managing that d
ata,
4309.9 --> 4311.5: but also like I don't know if that's something
4311.5 --> 4312.7: that you're thinking about,
4312.7 --> 4317.8: like what the steps are for like if for some kind
4317.8 --> 4319.9: of company institution, whatever,
4320.4 --> 4322.6: to participate in this or to use it,
4322.7 --> 4325.4: like what the steps are for what would be needed
4325.4 --> 4328.5: and what the phases are for growing its efficacy.
4328.8 --> 4331.3: So first starting from just being a really hopeful
4331.3 --> 4334.1: like language translation tool and deconfliction
4334.1 --> 4336.2: and sharing of information,
4337.4 --> 4339.5: and then like growing into more broadly
4339.5 --> 4343.0: like you mentioning this broader trust graph ecosyste
m,
4343.0 --> 4345.2: but I recognize that like there's phases of maturity
4345.8 --> 4346.4: on how that looks.
4346.6 --> 4347.8: I don't know if that's something that we've done
4347.8 --> 4349.9: or that we would think about mapping out.
4350.5 --> 4353.1: Just wanted to flag that again,
4353.2 --> 4356.2: trying to help make it tangible
4356.2 --> 4358.8: for some of the specific potential partners in the ro
om,
4359.2 --> 4361.9: like what that might look like for their participatio
n
4361.9 --> 4363.4: in that ecosystem.
4365.1 --> 4367.1: I would add something which is related
4367.1 --> 4368.3: to your question, Carol.
4370.6 --> 4373.9: We have to wonder ourself what would be the incentive
s
4374.5 --> 4378.1: for those players to kind of break the system
4378.1 --> 4381.1: to this in order to provide information
4381.1 --> 4382.1: based on their knowledge.
4389.6 --> 4390.9: So I do have a recommendation.
4391.3 --> 4394.8: So I'm Jesus from MITRE Corporation.
4396.1 --> 4399.0: So a suggestion would be to kind of gather
4399.6 --> 4401.8: all the problems that everybody have.
4402.5 --> 4405.6: And then based on defining the problem first,

4406.0 --> 4409.1: we now can actually figure out what is a good use cas
e
4409.9 --> 4413.8: to build the actual requirements for this AI to solve
4413.8 --> 4414.7: and bridge the gap.
4415.3 --> 4417.3: So typically that's how I'm typically,
4418.0 --> 4420.6: I try to kind of, if there's a new technology out the
re,
4421.4 --> 4424.5: I first identify all the problem sets
4425.1 --> 4426.7: and then start saying like,
4426.8 --> 4430.5: yes, can this technology solve it?
4430.5 --> 4431.5: So over.
4435.2 --> 4437.3: If I may, I think it's related
4437.3 --> 4440.1: to one of the earliest question from Carol as well.
4440.1 --> 4444.5: It's basically, who are the players, different end us
ers?
4444.9 --> 4447.2: And I guess what we can try to do is a mapping
4447.2 --> 4450.6: of their problems, depending on the use cases
4450.6 --> 4453.3: and the kind of factors and which kind of problems
4453.3 --> 4458.5: we are solving or at least resolving partially.
4459.4 --> 4465.8: I think giving the players the chatbot as the first s
tep
4465.8 --> 4467.8: is almost two birds, one stone,
4467.8 --> 4469.9: because we work out the problems based on the prompts
4469.9 --> 4473.2: that they provide to that chatbot.
4476.8 --> 4479.9: As long as the permissions are set up
4479.9 --> 4481.6: that they're willing to share that information,
4482.2 --> 4485.7: you can do private inference and we can set that up a
s well.
4486.6 --> 4488.0: And we should set that up
4488.0 --> 4490.2: because that's something we discussed in the working
group.
4490.6 --> 4493.5: If we have a public version of this,
4493.7 --> 4497.8: it shouldn't add to the ongoing inference
4497.8 --> 4500.0: because then we could get attacked
4500.0 --> 4502.4: and people could try and poison the bot
4502.4 --> 4503.4: and those sorts of things.
4503.6 --> 4505.1: So you need two versions.
4505.3 --> 4507.0: One is the public private inference
4507.5 --> 4511.3: and then the private public inference, if that makes
sense.
4511.4 --> 4515.1: So within the network, you have the private
4515.6 --> 4519.9: but public inference from the greater knowledge graph,
4520.2 --> 4524.9: but then the Telegram bot that sits exposed to the wo
rld
4524.9 --> 4528.5: that other people can see or can defer to
4528.5 --> 4532.9: or as like a mechanism and tool for people
4532.9 --> 4535.1: to get a bit more clarity on what's going on,

4537.9 --> 4539.2: that should be private inference.
4539.6 --> 4544.9: So we're not adding their data to our knowledge base
4544.9 --> 4549.4: without permissions in place or trust in place.
4550.6 --> 4555.3: One way that we plan on doing this with Begin
4555.9 --> 4559.7: and this is, I've just been trying to like log in
4559.7 --> 4563.5: to the meeting so I can share my screen more easily.
4566.6 --> 4569.5: But there's a platform that we've been developing
4569.5 --> 4574.3: called Begin AI and it kind of does this first step
4574.3 --> 4578.2: for us and we'll be experimenting it through the,
4579.1 --> 4580.9: sorry, I just need to go to my calendar
4580.9 --> 4583.4: and get into this Zoom.
4592.0 --> 4592.4: One moment.
4600.1 --> 4602.3: Maybe I'll go use the computer up there.
4603.1 --> 4606.5: Yeah, if you could give me five minutes, I'll share.
4606.9 --> 4610.6: During that, so I'd like to add some words about that.
4612.9 --> 4617.1: Our strategy to produce this type of thing,
4618.3 --> 4623.7: so when we create some AI, some AI agent or AI tool,
4624.2 --> 4628.5: but the accuracy of the answer is just 50%, no one us
e it.
4629.2 --> 4633.3: But it's accuracy of that AI system is 85%.
4633.3 --> 4636.8: So many people will start to use it too
4636.8 --> 4642.7: and we have more input we have for the AI system
4642.7 --> 4648.0: if it is accurate so we can improve that AI system.
4648.2 --> 4651.4: So that is needed and of course we can start
4651.4 --> 4654.5: with that exploring so many use cases first
4654.5 --> 4659.4: but so our strategy we discussed during the past
4659.4 --> 4663.2: working group call is let's concentrate on that one s
ingle
4663.2 --> 4665.0: but important use case.
4665.4 --> 4669.5: Then create that 85% or 90% AI system.
4670.1 --> 4673.4: Same that after we have the one single but a strong o
ne,
4673.7 --> 4677.5: we can create the other one with 90% or 95%
4677.5 --> 4679.1: strong AI use case.
4679.5 --> 4683.5: So that is the reason why that JPCrypto has some pain
 point
4683.5 --> 4685.2: in their daily operation.
4685.6 --> 4688.4: So they need more accurate information.
4689.1 --> 4692.2: So coming from English language but they need
4692.2 --> 4694.5: the Japanese written accurate information.
4696.1 --> 4700.3: JPCrypto has a strong request to the agent system.
4700.6 --> 4704.6: So we are starting with their request first.
4705.2 --> 4708.6: So that is what is our past discussion
4708.6 --> 4709.7: at the working group call.
4712.4 --> 4716.1: So the first step is with respect to this use case
4716.1 --> 4719.6: is basically finding a way to gather as much informat
ion

4719.6 --> 4723.9: as possible and then would be English or Japanese
4723.9 --> 4729.3: and then for JPCrypto to be able to kind of request
4730.3 --> 4732.8: through the chatbot or through another interface
4732.8 --> 4737.6: to request this information in order to either to retrieve
4737.6 --> 4744.7: some previous evidences or to investigate a new case,
4744.8 --> 4745.1: I guess.
4746.3 --> 4749.4: Yes, so it's a really important thing because JPCrypto
4749.4 --> 4756.1: would like to join this PLC by using Japanese and so on.
4757.1 --> 4761.3: So JPCrypto asked cryptocurrency companies to try
4762.0 --> 4765.2: whether it's useful or not because so currently
4765.2 --> 4767.3: this is a concept model.
4767.9 --> 4772.2: So but to try something is important thing.
4772.5 --> 4773.8: So let's proceed together.
4775.8 --> 4777.7: I also have a comment about this.
4778.1 --> 4781.5: And yeah, we are very welcome to use this kind of tools
4781.5 --> 4784.2: in JPCrypto ISAC and also I think it's important
4784.2 --> 4787.7: to classify the data or label the data.
4788.5 --> 4790.3: This is maybe that is a private information
4790.3 --> 4793.1: but there are some labels of the private information.
4793.6 --> 4798.0: Really confidential or almost public
4798.0 --> 4799.6: but still some kind of confidential.
4799.7 --> 4802.3: So I think that it's important to label the information
4802.3 --> 4806.4: and I think it's better to classify some kind of data
4806.4 --> 4808.5: so that we can share easily.
4809.3 --> 4814.2: And for example, then CL901, CLISAC is a very strong team
4814.9 --> 4818.4: from strong world-class engineers, that great.
4819.3 --> 4822.9: And so they are creating very strong knowledge,
4822.9 --> 4825.7: from the engineering point of view, that's fantastic.
4826.6 --> 4829.5: But at the same time, the C-suite of crypto company
4829.5 --> 4833.9: or C-suite of Ginkgo need another type of language
4834.5 --> 4838.4: to discuss their governance or something like that.
4839.0 --> 4841.9: That kind of translation caused by the difference
4841.9 --> 4845.1: of a role in the companies, another reason why
4845.1 --> 4847.4: that AI chatbot can help their needs.
4854.1 --> 4855.5: So I just have a question.
4855.7 --> 4857.6: In terms of knowledge, right?
4857.8 --> 4862.0: For the 85 solution that we're shooting for,
4862.3 --> 4864.9: what type of information are we interested in?
4865.0 --> 4868.8: Because at a CVE level, that's very low level, right?
4869.1 --> 4872.4: Or are we more at a categorization level
4873.1 --> 4875.4: type of information, right?

4875.4 --> 4876.5: So I think that's one thing too,
4876.6 --> 4880.3: because depending on the, from a user point of view t
oo,
4880.9 --> 4882.4: you don't wanna get information
4882.4 --> 4885.0: that you can't really process and understand.
4885.6 --> 4889.9: So that cognitive load is also part of that equation,
 so.
4892.6 --> 4894.5: Yeah, so for JPEG to ISAC,
4894.7 --> 4900.3: their point is how to steal or how to,
4900.8 --> 4903.6: for example, so the case of the incident,
4904.0 --> 4906.2: so we want to see the process, for example,
4907.1 --> 4909.3: because in case of the DML Bitcoin,
4910.0 --> 4913.9: so unfortunately we didn't, how to, what happened.
4915.0 --> 4918.6: So because after that, so cryptocurrency companies
4919.1 --> 4920.6: didn't do anything.
4921.3 --> 4923.1: So this is a really important thing.
4923.2 --> 4927.3: On the other hand, we want to gather some information,
4927.5 --> 4930.3: for example, the Yamaita information and so on,
4930.5 --> 4932.7: because so currently, honestly speaking,
4932.8 --> 4935.8: so we don't know which information is useful or not.
4935.8 --> 4939.0: So we would like to try this,
4940.0 --> 4942.8: and we want to gather some information
4942.8 --> 4944.5: from cryptocurrency company.
4947.1 --> 4948.7: Okay, yeah, in addition to that, yeah,
4948.9 --> 4951.4: of course we can gather information about like a CBE
4951.4 --> 4954.6: or public information, yeah, because it's public.
4954.7 --> 4957.5: So we'd like to know more about in details,
4957.8 --> 4960.5: IOCs or the case or, yeah,
4960.6 --> 4963.4: that's really difficult to disclose,
4963.4 --> 4966.4: but if we have some kind of a protocol to share,
4966.8 --> 4968.3: so if you'd like to know more,
4968.4 --> 4971.7: there are more deep knowledge or information.
4974.4 --> 4975.9: In its current form,
4976.1 --> 4977.6: because I know we're in like beta
4977.6 --> 4979.6: or alpha whatever stage we're in,
4980.5 --> 4983.6: curious if like in trying to articulate
4983.6 --> 4985.6: what the current phase of capability is,
4985.6 --> 4987.2: because I know we're going to be like building out
4987.2 --> 4989.9: lots of different phases of capability right now,
4990.4 --> 4992.9: are we envisioning kind of prioritizing
4992.9 --> 4995.4: in the near term, in the nearest term,
4995.9 --> 4998.6: so translator definitely on utility
4998.6 --> 5001.2: of like cross different language communication.
5002.3 --> 5006.5: So is it that plus router,
5006.8 --> 5011.9: so I guess like routing of the request to XYZ partici
pant,
5013.2 --> 5016.5: and then I don't know like, I don't know what other,

5016.6 --> 5018.6: like what's another, I'm really bad at metaphors,
5019.3 --> 5021.1: like a setup wizard in the sense
5021.1 --> 5022.3: like it's walking through and asking
5022.3 --> 5023.8: for like very specific information,
5024.1 --> 5026.1: like I guess that like I don't know
5026.1 --> 5027.4: whether the current capability is
5027.4 --> 5029.2: or what the current capability is
5029.2 --> 5031.3: that we want to prioritize building in first.
5031.8 --> 5033.3: Do we have thoughts on that?
5033.4 --> 5035.9: Is that actually what you guys want to dig into
5035.9 --> 5037.7: based on the questions that you had teed up
5037.7 --> 5038.8: at the end of your presentation?
5039.1 --> 5040.8: What would be the most valuable thing
5040.8 --> 5045.9: for either exploring the current focus of the chatbot
5045.9 --> 5047.6: and its capability right now?
5047.7 --> 5050.3: Is it mostly just like language translation tool,
5050.3 --> 5053.4: which awesome, is it that plus router
5054.2 --> 5056.5: and other like sort of help desk functionality
5056.5 --> 5058.6: of like walking through troubleshooting or whatever,
5059.6 --> 5062.4: or are there certain things that would be the most he
lpful
5062.4 --> 5067.1: to dig into with the people around this table right n
ow
5067.1 --> 5068.3: on thinking about some of that,
5068.4 --> 5071.1: like some of the chatbot specific like that functiona
lity?
5071.8 --> 5073.0: Yeah, that's a great question.
5073.3 --> 5076.8: And I think what the most value we can get
5076.8 --> 5080.5: from this venue at this time
5080.5 --> 5082.6: is to come up with the pathways.
5083.5 --> 5085.7: So the templates and the pathways
5085.7 --> 5088.5: that the experts in this room would use
5088.5 --> 5090.3: when they are prompting it themselves.
5091.3 --> 5096.9: And then for that to be like we can get that
5096.9 --> 5099.3: by just being the one to host the AI agent.
5099.4 --> 5100.6: But if you were to,
5101.0 --> 5103.0: after you went through a really good pathway
5103.5 --> 5105.0: of discovery and knowledge
5105.0 --> 5109.2: and educating this AI agent that we give you,
5109.8 --> 5112.2: for you to write a chronicle of that,
5112.7 --> 5114.6: and that chronicle then becomes a template.
5115.3 --> 5117.5: And then we can distribute those templates
5117.5 --> 5120.1: as these are the pathways that you can take
5120.1 --> 5122.3: to understand this particular problem
5122.3 --> 5124.3: of which an expert has gone through.
5124.8 --> 5126.3: And what is interesting about that,
5126.3 --> 5129.1: again, getting into the probabilistic nature of LLMs

5129.1 --> 5132.1: is based on the context that the person is coming fro
m,
5132.8 --> 5135.7: that pathway then gets reconstructed in their own mea
ning.
5136.2 --> 5138.9: So you have a MITRE pathway that's developed,
5139.1 --> 5141.3: which is following standards
5141.3 --> 5148.0: and the more detailed way to deal with these incident
s.
5148.5 --> 5150.7: And then you get a crypto company
5150.7 --> 5152.1: that is going through the incident
5152.1 --> 5154.7: that uses that template and follows that path.
5154.9 --> 5156.0: And then they at the end,
5156.4 --> 5158.5: write a chronicle and a template of that.
5159.1 --> 5161.6: And that then acts as,
5162.2 --> 5167.3: and just picturing our minds back to that beautiful g
raph
5167.3 --> 5169.3: of constellations that draws lines,
5169.5 --> 5171.8: what you're doing is you're drawing your own constell
ation
5171.8 --> 5173.1: through the knowledge graph.
5173.8 --> 5177.7: And if everyone in this room has their own version of
 that,
5177.7 --> 5179.5: and we can find a way to share that,
5179.9 --> 5184.2: then the end result is this thing,
5186.3 --> 5188.7: discovery across disciplines,
5189.0 --> 5192.0: which I think is one of Begin's most valuable attribu
tes
5193.0 --> 5195.6: is that we do bring multiple minds
5195.6 --> 5197.5: from very specific topics.
5198.3 --> 5202.5: And a cypherpunks pathway through the knowledge base
5202.5 --> 5203.7: is going to be very different
5203.7 --> 5206.1: to a regulators pathway through the knowledge base.
5206.5 --> 5210.9: However, if their reconstructions and compressions mi
rror,
5211.7 --> 5214.5: then there is discovery between them.
5216.0 --> 5218.2: And I'm super excited about that.
5218.4 --> 5221.4: I think that would be the most instructional value
5221.4 --> 5222.5: I would give to the room
5222.5 --> 5225.8: is that when you receive one of these chatbots,
5226.0 --> 5229.9: which is either, as I said, private or the public ver
sion
5229.9 --> 5234.2: to go through the experience in your own context,
5234.2 --> 5235.1: in your own meaning,
5235.3 --> 5238.1: and to record that in a chronicle,
5238.1 --> 5241.0: you can easily ask the AI, once you've finished the c
hat,
5241.4 --> 5243.4: hey, could you write this as a chronicle for me?

5244.0 --> 5246.5: Could we do it as a step-by-step process,
5246.6 --> 5247.6: what we just went through?
5247.9 --> 5249.6: And then to share that with us directly,
5250.8 --> 5252.9: obviously that can be through an encrypted channel or not.
5253.2 --> 5255.0: It's kind of depending on the information,
5255.4 --> 5261.4: but that would help us create these streamlined pathways.
5262.1 --> 5265.5: So then the AI agents actually develop skills,
5266.3 --> 5269.4: which are formed by experts.
5270.3 --> 5275.0: And then that is when we can distribute it as a product
5275.0 --> 5276.9: to the greater community,
5277.2 --> 5280.2: because it's actually got like that essence and value
5280.2 --> 5284.5: and that magical pathway that you would not have taken
5284.5 --> 5287.3: if you were just some person who got hacked
5287.3 --> 5290.6: and lost 5,000 or 1,000, 1,000 or whatever.
5291.4 --> 5295.2: And then you look, oh, this is a phishing attack
5295.2 --> 5296.6: and there's been this full reconstruction
5296.6 --> 5299.1: of a phishing attack by an expert.
5299.8 --> 5304.4: I just have to add that as a skill to the agent, right?
5305.3 --> 5307.9: And the interesting thing about that as well
5307.9 --> 5311.5: is you then get this, everyone is contributing
5311.5 --> 5313.4: and everyone is reconstructing the skill
5313.4 --> 5314.2: in their own version.
5314.7 --> 5317.7: So there isn't like, we're not like stealing from each other.
5317.9 --> 5321.5: We're just using the same skill, but within our own context.
5321.8 --> 5324.2: So if someone fits the same context as us,
5324.2 --> 5325.8: then they'll choose to use the MITRE one
5325.8 --> 5327.7: or they'll choose to use the crypto exchange one.
5328.1 --> 5331.9: If someone is curious about what the MITRE one would be
5331.9 --> 5333.8: and they're a crypto exchange operator,
5334.1 --> 5336.1: then they can just follow that path on their own
5336.1 --> 5339.2: with the MITRE reconstruction of the pathway.
5339.7 --> 5341.2: And then maybe discover something
5341.2 --> 5342.9: because their context that they're coming with
5342.9 --> 5344.9: is very different.
5346.0 --> 5348.5: Okay, it's time to take 10 minutes break
5348.5 --> 5349.8: before continuing this discussion.
5350.2 --> 5352.2: So we have coffee, but before that,
5352.2 --> 5354.9: so I need to tell that another session, the next slot.
5355.6 --> 5359.6: But so I think Shouhei need to explain a little bit m

ore
5359.6 --> 5362.9: about that chat bot, what is behind the chat bot?
5363.6 --> 5366.5: Because that's so, you know, so when,
5366.7 --> 5369.8: so the engineers see that CVE recorder,
5370.0 --> 5372.3: new vulnerability information, so they take serious.
5372.9 --> 5377.0: So he or she need to report to his boss or C-suite.
5377.3 --> 5378.7: So what is serious about it?
5379.2 --> 5380.8: But the question from the C-suite,
5380.8 --> 5387.0: because if we need to tackle with this or not,
5387.6 --> 5388.8: so it's a very, another question
5388.8 --> 5390.0: from the C-suite point of view,
5390.2 --> 5392.0: that's, you know, so there, you know,
5392.5 --> 5394.3: Shouhei's system behind that chat bot
5394.3 --> 5396.3: is, you know, doing some, you know,
5396.8 --> 5398.6: analysis of the profitability graph
5398.6 --> 5400.7: or dependency analysis, something like that.
5400.9 --> 5403.4: It's a crucial information for C-suite
5403.4 --> 5405.4: or management team to judge.
5405.8 --> 5408.7: So if they need to deal with it or not.
5409.3 --> 5411.2: So that kind of analysis is, you know,
5411.2 --> 5413.2: additional value for C-suite.
5414.2 --> 5418.4: So we call that, so if they have unlimited budget,
5418.8 --> 5419.8: they need to do anything,
5419.9 --> 5421.9: but if they have very limited budget,
5422.3 --> 5424.5: they need to judge every day, every day,
5424.8 --> 5427.9: about what, how they need to deal with that,
5428.1 --> 5429.8: any small or big vulnerabilities.
5430.1 --> 5433.8: That is a, you know, major question C-suite every day
 has.
5433.9 --> 5436.8: As you know, Eric is an expert on that,
5436.8 --> 5440.1: but so if that, this AI agent system
5440.1 --> 5442.1: could help the judge by C-suite,
5442.4 --> 5443.8: that is a very, you know,
5444.3 --> 5446.7: valuable system for cryptocurrency industry.
5451.4 --> 5453.8: Anyway, let's take a 10 minutes break
5453.8 --> 5455.5: and then let's resume that discussion.
5496.8 --> 5497.0: All right.