

BGIN Meeting Report

Date: TBD

Location: Virtual Meeting

Executive Summary

The meeting focused on addressing the challenges and opportunities for information sharing in the crypto industry, particularly around high-value data elements and standards. The discussion emphasized the need for a private sector-led approach to standardize key data elements that can facilitate effective information sharing while addressing legal and regulatory concerns. Key stakeholders agreed to pursue quick wins by co-hosting targeted workshops aimed at creating the first version of these standards, which will be socialized publicly and potentially feed into broader initiatives like FATF and FSB.

Key Discussion Points

1. **Legal and Regulatory Challenges:**
 - Legal challenges have been a recurring issue in information sharing.
 - Quick wins, such as developing high-value data elements, could help overcome these barriers.
2. **High-Value Data Elements:**
 - There is a need to identify and standardize high-value data elements that are crucial for effective information sharing.
 - Government regulators and law enforcement will have significant interest in these elements.
3. **Workshops and Collaborations:**
 - NIST is hosting a workshop on April 16, which could serve as a forum for discussing ways to motivate information sharing.
 - Co-hosting targeted discussions with industry partners to create the first version of high-value data standards was proposed.
4. **Government and Industry Roles:**
 - The private sector should lead in developing agreed-upon standards, which can then be supported by government initiatives.
 - Government authorities are uniquely positioned to address areas like liability protections and policy frameworks.

Action Items and Next Steps

1. **Co-host Targeted Workshop:**
 - BEGIN will co-host a targeted workshop with industry partners to create the first version of high-value data standards.
 - The workshop will aim to socialize these standards publicly and gather feedback.
2. **NIST Workshop Participation:**
 - Participants will engage in NIST's April 16 workshop to discuss ways to motivate information sharing and feed into broader initiatives.
3. **Socialize Standards Publicly:**
 - BEGIN will work on creating the first version of high-value data standards and socialize them publicly for feedback.
 - This will include feeding into other ongoing efforts such as FATF and FSB.
4. **Policy Framework Development:**
 - JFSA and other government authorities will focus on developing policy frameworks and governance models to support information sharing.
 - These frameworks will be discussed at higher-level forums like FSB and FATF.

Detailed Session Summary

- The meeting began with a discussion on the challenges of information sharing in the crypto industry, particularly focusing on legal and regulatory barriers. Participants agreed that quick wins could help address these issues.
- A key participant highlighted the need for high-value data elements to be identified and standardized. They emphasized that government regulators and law enforcement will have significant interest in these elements.
- Another participant suggested co-hosting targeted workshops with industry partners to create the first version of high-value data standards. This approach would allow for public feedback and socialization of the standards.
- A third participant brought up policy issues, suggesting that JFSA and government authorities should focus on developing policy frameworks and governance models to support information sharing.
- The same key participant agreed that BEGIN could focus on creating the most valuable information elements needed for the system, reinforcing what they have already done. They noted that this would feed into broader initiatives like FATF and FSB.
- The meeting concluded with a discussion on the upcoming NIST workshop on April 16, which participants will engage in to discuss ways to motivate information sharing.

- Participants thanked each other and took a one-hour break.
-

Appendix: Full Meeting Transcript (Anonymized)

95.0 --> 95.3: . .
95.3 --> 95.5: . .
95.5 --> 95.8: .
129.0 --> 131.8: . .
133.6 --> 135.0: .
153.5 --> 154.9: . .
154.9 --> 157.6: . .
157.6 --> 157.7: .
182.5 --> 183.9: . .
183.9 --> 185.4: .
239.8 --> 240.0: . .
240.0 --> 240.0: .
246.6 --> 249.4: . .
260.0 --> 261.4: .
270.0 --> 271.5: . .
276.7 --> 278.1: .
304.9 --> 305.3: . .
310.0 --> 310.4: . .
310.4 --> 310.7: . .
310.7 --> 311.0: .
334.8 --> 335.2: . .
340.8 --> 341.2: . .
341.2 --> 341.5: . .
341.9 --> 342.4: .
364.2 --> 364.3: . .
368.6 --> 368.6: .
369.0 --> 369.0: .
370.9 --> 370.9: .
372.4 --> 372.4: .
374.4 --> 374.5: .
389.6 --> 389.6: .
389.6 --> 389.7: .
389.7 --> 389.7: .
389.7 --> 389.7: .
389.7 --> 389.7: .
389.7 --> 389.8: .
389.8 --> 389.8: .
389.8 --> 389.8: .
389.8 --> 389.8: .
389.8 --> 389.8: .

389.8 --> 389.9: .
389.9 --> 389.9: .
389.9 --> 389.9: .
389.9 --> 389.9: .
389.9 --> 389.9: .
389.9 --> 390.0: .
390.0 --> 390.0: .
451.4 --> 452.8: Okay.
455.6 --> 457.0: Okay.
462.1 --> 463.2: Okay.
503.4 --> 504.8: Okay.
508.4 --> 509.1: Okay.
540.0 --> 540.4: Okay.
547.7 --> 549.1: Okay.
555.2 --> 556.6: Okay.
557.7 --> 558.8: Okay.
559.3 --> 559.5: Okay.
564.4 --> 564.5: Okay.
569.7 --> 571.1: Okay.
634.4 --> 635.8: Okay.
645.7 --> 647.1: Okay.
653.4 --> 654.8: Okay.
657.0 --> 658.4: Okay.
658.4 --> 659.1: Okay.
664.0 --> 665.4: Okay.
666.1 --> 666.2: Okay.
667.4 --> 667.6: Okay.
667.6 --> 667.8: Okay.
670.5 --> 670.6: Okay.
702.2 --> 703.0: Okay.
711.2 --> 712.6: Okay.
735.1 --> 736.5: Okay.
746.1 --> 747.5: Okay.
761.8 --> 763.2: Okay.
774.1 --> 775.5: Okay.
782.7 --> 783.7: Okay.
784.2 --> 784.3: Okay.
787.2 --> 788.6: Okay.
788.6 --> 789.7: Okay.
789.7 --> 790.0: Okay.
790.0 --> 790.6: Okay.
790.6 --> 791.5: Okay.
791.5 --> 791.5: Okay.
792.1 --> 793.4: Okay.
793.4 --> 794.0: Okay.
795.8 --> 797.2: Okay.
799.8 --> 801.2: Okay.

801.7 --> 802.9: Okay.
802.9 --> 803.6: Okay.
806.7 --> 808.1: Okay.
808.1 --> 809.7: Okay.
822.7 --> 824.1: Okay.
829.0 --> 830.4: Okay.
830.5 --> 831.0: Okay.
832.1 --> 833.5: Okay.
833.5 --> 835.2: Okay.
837.8 --> 839.2: Okay.
848.6 --> 849.2: Okay.
860.1 --> 861.5: Okay.
863.9 --> 865.3: Okay.
875.1 --> 876.5: Okay.
876.5 --> 877.5: Okay.
886.1 --> 887.5: Okay.
889.6 --> 891.0: Okay.
891.2 --> 893.6: Okay.
904.6 --> 906.0: Okay.
909.4 --> 909.8: Okay.
909.9 --> 910.2: Okay.
915.3 --> 916.7: Okay.
916.7 --> 918.9: Okay.
919.0 --> 919.7: Okay.
919.7 --> 920.1: Okay.
925.6 --> 927.0: Okay.
928.6 --> 930.0: Okay.
937.0 --> 937.2: Okay.
939.0 --> 940.4: Okay.
940.9 --> 941.2: Okay.
942.4 --> 943.4: Okay.
949.0 --> 950.4: Okay.
961.4 --> 962.8: Okay.
964.1 --> 964.6: Okay.
964.6 --> 965.4: Okay.
965.8 --> 966.0: Okay.
966.0 --> 966.1: Okay.
966.3 --> 966.7: Okay.
966.7 --> 966.8: Okay.
967.2 --> 967.9: Okay.
969.6 --> 971.0: Okay.
971.3 --> 972.7: Okay.
972.7 --> 974.5: Okay.
978.4 --> 979.8: Okay.
979.8 --> 980.9: Okay.
984.4 --> 985.8: Okay.
985.8 --> 988.6: Okay.

995.9 --> 997.3: Okay.
997.3 --> 999.8: Okay.
1001.9 --> 1003.3: Okay.
1003.3 --> 1003.6: Okay.
1004.1 --> 1005.0: Okay.
1005.0 --> 1005.4: Okay.
1005.8 --> 1006.5: Okay.
1008.1 --> 1009.5: Okay.
1009.5 --> 1009.9: Okay.
1010.2 --> 1010.4: Okay.
1011.5 --> 1012.9: Okay.
1014.8 --> 1016.2: Okay.
1016.2 --> 1016.9: Okay.
1016.9 --> 1018.9: Okay.
1019.6 --> 1021.0: Okay.
1027.3 --> 1028.7: Okay.
1036.6 --> 1038.0: Okay.
1040.2 --> 1041.6: Okay.
1049.1 --> 1050.5: Okay.
1106.0 --> 1107.4: Okay.
1109.3 --> 1110.7: Okay.
1143.7 --> 1144.8: If you don't mind, everyone.
1145.8 --> 1147.1: And we'll start with a.
1148.1 --> 1149.4: An overview from.
1149.7 --> 1150.7: On the.
1152.3 --> 1152.9: Initiatives.
1153.1 --> 1153.6: A few ones.
1158.0 --> 1158.6: Hello.
1159.1 --> 1159.8: All right.
1159.8 --> 1160.8: So.
1166.4 --> 1167.0: Yeah.
1167.5 --> 1168.3: All right.
1168.4 --> 1173.3: So for this one, I'll just spend probably 10 to 20 minutes to kind of go through.
1173.9 --> 1175.3: Three knowledge.
1175.8 --> 1178.0: In terms of attack and defend.
1178.6 --> 1182.5: That can be leveraged for this type of standards and discussion.
1183.1 --> 1183.2: So.
1184.2 --> 1185.4: So the first one is.
1185.7 --> 1186.4: This is a.
1186.5 --> 1188.5: A recently released.
1189.2 --> 1190.4: Knowledge base.
1190.9 --> 1193.0: That is in terms of.
1193.1 --> 1193.5: Attack.
1194.4 --> 1196.2: Tactics techniques and procedure.
1196.8 --> 1198.4: That has been released by MITRE.

1199.0 --> 1201.6: That is geared toward digital payment.
1202.2 --> 1202.8: Technologies.
1205.4 --> 1207.4: So I think there was a.
1208.2 --> 1210.9: A requirement or a.
1211.0 --> 1211.9: As regarding.
1212.2 --> 1214.9: You know, understanding a lot of the attacks out there.
1215.0 --> 1217.3: And this type of roll up.
1217.4 --> 1218.4: Or taxonomy.
1219.0 --> 1221.2: Is something that may be useful to the group.
1221.8 --> 1222.0: So.
1223.5 --> 1224.8: As you can see.
1225.3 --> 1226.1: The actual adapt.
1226.8 --> 1227.1: Is.
1228.3 --> 1229.9: Is split up into.
1230.7 --> 1232.8: The same tactics as MITRE tech.
1233.2 --> 1234.4: Which is reconnaissance.
1234.9 --> 1235.9: Resource development.
1235.9 --> 1237.5: Initial access.
1238.2 --> 1239.1: Execution.
1239.7 --> 1241.1: Privilege escalation.
1241.7 --> 1242.8: Defense evasion.
1243.5 --> 1243.9: Credential access.
1244.9 --> 1245.7: Lateral movement.
1246.4 --> 1246.8: Collection.
1247.4 --> 1247.9: Impact.
1248.2 --> 1248.6: And fraud.
1250.1 --> 1251.7: In each one.
1252.2 --> 1253.6: Has techniques already there.
1254.1 --> 1256.1: Based on what is either.
1256.5 --> 1257.0: Available.
1259.4 --> 1260.8: Reports online.
1261.6 --> 1262.5: And then.
1263.0 --> 1264.8: It also has a link.
1264.8 --> 1265.4: So.
1266.8 --> 1267.5: So.
1268.2 --> 1269.6: The goal of this adapt.
1270.5 --> 1271.6: Knowledge base.
1272.3 --> 1273.7: Is actually to extend.
1274.6 --> 1275.1: The MITRE.
1275.6 --> 1277.2: The like original MITRE tech.
1277.8 --> 1278.9: Since a lot of the.
1279.7 --> 1281.7: If you take a look at a lot of the.
1282.7 --> 1284.0: By bit hack.
1284.1 --> 1286.3: Or any of those type of like hacks.
1286.8 --> 1287.7: A lot of the.
1288.9 --> 1289.8: I guess.

1290.2 --> 1291.6: Vectors of attacks.
1291.8 --> 1293.9: Is actually more at an enterprise level.
1293.9 --> 1295.0: Than.
1295.9 --> 1297.6: At the adapt level.
1301.3 --> 1302.0: Okay.
1303.4 --> 1304.8: So the way.
1305.0 --> 1305.3: You know.
1305.7 --> 1307.1: One would use adapt.
1307.7 --> 1309.4: Is to actually use it.
1309.6 --> 1311.6: With also MITRE attack.
1312.2 --> 1313.9: So within MITRE attack.
1314.2 --> 1315.9: There's actually different categories.
1317.0 --> 1318.0: Of knowledge base.
1318.1 --> 1319.4: So you have your enterprises.
1319.9 --> 1321.0: Mobile and ICS.
1321.0 --> 1322.9: Since a lot of the.
1324.6 --> 1325.1: Payment.
1325.3 --> 1326.1: Type of technology.
1326.7 --> 1328.7: Is going to probably leverage.
1329.2 --> 1330.6: These types of platforms.
1331.2 --> 1332.8: Enterprise and mobile and so on like that.
1333.2 --> 1334.6: And then if you take a look at it.
1334.9 --> 1335.7: A lot of this.
1337.3 --> 1338.5: Tactics and techniques.
1338.7 --> 1340.4: That was captured in this knowledge base.
1341.5 --> 1342.5: Actually applies.
1343.2 --> 1344.0: Can be mapped.
1344.4 --> 1345.1: And you know apply.
1345.6 --> 1347.3: To any of the current.
1348.1 --> 1348.7: Hack.
1349.1 --> 1350.8: In terms of the crypto.
1351.1 --> 1353.1: You know exchanges so.
1353.9 --> 1355.2: And then so.
1355.9 --> 1357.7: The thing that's MITRE attack.
1357.9 --> 1359.7: Did that folks may be.
1359.8 --> 1361.1: Interested in is that.
1361.5 --> 1363.4: If a particular type of techniques.
1363.9 --> 1365.0: You know is you know.
1365.1 --> 1367.1: Interested in once you click.
1367.1 --> 1369.1: On each one it will actually.
1369.7 --> 1370.2: Show you.
1372.1 --> 1373.6: Some of the mitigations.
1374.9 --> 1375.8: Some of the.
1375.8 --> 1377.1: Detection strategy.
1377.5 --> 1378.5: In terms of monitoring.
1379.4 --> 1381.1: And the actual reference.
1381.6 --> 1383.6: Where this information came from.

1388.2 --> 1389.5: And then MITRE.
1389.9 --> 1391.4: Also recently released.
1392.1 --> 1393.3: MITRE defend.
1394.4 --> 1394.9: So.
1395.7 --> 1396.9: The goal of MITRE defend.
1397.3 --> 1399.1: Is to actually try to capture.
1399.8 --> 1401.2: You know how one.
1401.5 --> 1403.7: Would defend a lot of this.
1403.7 --> 1405.8: MITRE attack TTP.
1406.1 --> 1406.8: That was captured.
1407.6 --> 1409.3: And then the categories here.
1409.8 --> 1411.4: Or the way it is categorized.
1411.8 --> 1412.9: In terms of tactics.
1413.0 --> 1414.0: Is actually different.
1414.4 --> 1416.4: It's more from a defender point of view.
1417.2 --> 1418.7: So as you can see.
1419.6 --> 1421.1: You have hardening.
1421.4 --> 1423.1: Which is typically the like initial.
1423.3 --> 1425.1: Cyber hygiene you want to do.
1425.5 --> 1427.4: And these are all the like techniques.
1427.5 --> 1428.2: That a company.
1428.8 --> 1430.1: Could actually apply.
1430.1 --> 1431.3: And leverage.
1432.0 --> 1433.1: And a lot of them are more.
1433.7 --> 1434.3: Engineer.
1435.1 --> 1437.3: Or a system admin can actually consume.
1438.1 --> 1438.8: And implement.
1439.7 --> 1440.9: And the next layer.
1441.3 --> 1442.3: Is actually the tech.
1442.7 --> 1444.6: How would one monitor.
1445.1 --> 1446.1: Some of this attack.
1446.5 --> 1448.1: And here are some of the techniques.
1448.5 --> 1449.7: That have been captured.
1450.7 --> 1452.6: From a defensive point of view.
1453.6 --> 1455.3: And then let me go to the other categories.
1456.8 --> 1457.4: So.
1457.4 --> 1458.2: Sorry.
1459.9 --> 1459.9: Okay.
1464.0 --> 1464.6: So.
1465.8 --> 1467.1: Besides detection.
1467.5 --> 1468.1: And hardening.
1468.7 --> 1471.2: The next defend.
1471.5 --> 1473.1: Tactic is called isolate.
1473.5 --> 1474.5: Which is basically.
1474.9 --> 1476.4: If one is compromised.
1476.8 --> 1477.7: What can you do?
1478.3 --> 1480.1: And these are some of the techniques.

1480.3 --> 1482.0: That have been aggregated and captured.
1482.3 --> 1483.8: That should help corporation.
1483.8 --> 1484.9: And companies.
1485.7 --> 1485.8: You know.
1486.4 --> 1488.1: On a specific.
1489.6 --> 1490.7: Use cases.
1491.7 --> 1493.9: The next category is deceive.
1494.4 --> 1495.6: So this is actually.
1495.8 --> 1497.8: More like a next level.
1498.0 --> 1498.6: To detection.
1499.3 --> 1501.2: So that's one of the techniques.
1501.5 --> 1502.3: That's captured there.
1502.6 --> 1503.2: I mean tactics.
1503.6 --> 1505.3: And the last one is evict.
1505.7 --> 1507.7: So now if I'm compromised.
1508.3 --> 1510.3: What are some techniques that I can use.
1510.3 --> 1511.7: To actually either.
1511.9 --> 1514.0: Do incident handling and response.
1516.3 --> 1516.6: Okay.
1517.4 --> 1517.8: And.
1518.7 --> 1519.4: In this.
1521.2 --> 1522.4: Knowledge base.
1523.3 --> 1523.8: There's actually.
1524.3 --> 1525.2: A very cool.
1526.6 --> 1527.4: Tool.
1527.8 --> 1530.1: That people may found.
1530.4 --> 1531.1: Interested in.
1532.3 --> 1532.8: It's hard to click.
1533.0 --> 1533.2: So.
1537.2 --> 1538.5: If you take a look.
1538.5 --> 1539.3: Over here.
1539.4 --> 1541.2: If you actually click MITRE ATT&CK.
1541.8 --> 1542.3: And then.
1543.1 --> 1545.7: If I'm interested in credential dumping.
1546.1 --> 1548.2: It will actually show you.
1548.4 --> 1550.1: A graph right away.
1550.6 --> 1551.8: So if you go down.
1552.0 --> 1552.4: If I go down.
1553.5 --> 1554.1: So.
1555.2 --> 1557.6: For a credential dumping.
1557.8 --> 1558.7: Within MITRE ATT&CK.
1559.0 --> 1560.5: These are the sub techniques.
1561.4 --> 1563.3: And then here's the definition of it.
1563.8 --> 1564.5: And from there.
1564.5 --> 1566.5: There's actually like a model.
1568.1 --> 1569.7: That will show you.
1569.8 --> 1571.1: That for this type of.

1571.2 --> 1572.6: ATT&CK TTPs.
1573.0 --> 1574.8: Here are some mitigation.
1576.0 --> 1577.0: That a company.
1577.3 --> 1578.5: Can actually leverage.
1579.6 --> 1580.2: To kind of.
1581.6 --> 1583.2: Lower their risk.
1586.9 --> 1588.5: And finally.
1590.9 --> 1591.6: If you.
1592.0 --> 1594.1: In the domain section.
1595.3 --> 1596.2: There's actually.
1596.6 --> 1597.1: Some model.
1597.7 --> 1599.4: That was created.
1600.7 --> 1602.5: So in the OT space.
1603.8 --> 1605.2: So as you can see.
1605.8 --> 1606.6: There's a model.
1606.7 --> 1607.3: That was created.
1607.6 --> 1609.8: For the ransomware ATT&CK.
1610.4 --> 1612.3: So in terms of the ATT&CKPAT.
1613.5 --> 1614.6: Let me just zoom in.
1614.7 --> 1615.1: A little bit.
1615.6 --> 1616.5: So people can see.
1619.3 --> 1619.8: So.
1624.8 --> 1627.0: I think it's still hard to see.
1627.1 --> 1628.2: But let me zoom in.
1629.0 --> 1629.8: This is my last.
1630.7 --> 1631.8: I guess discussion.
1632.3 --> 1633.8: On these tools.
1634.5 --> 1635.0: So.
1637.4 --> 1638.0: Okay.
1638.1 --> 1638.7: So.
1643.4 --> 1644.0: Okay.
1646.7 --> 1647.9: So as you can see.
1648.2 --> 1650.3: The red graph is actually showing you.
1650.5 --> 1651.6: The actual ATT&CK itself.
1651.6 --> 1653.1: And then the blue graph.
1653.3 --> 1655.4: Are actually the mitigation.
1657.5 --> 1658.5: You see the bottom.
1659.7 --> 1660.6: Then if you go.
1660.8 --> 1661.6: Let me pull up the graph.
1665.2 --> 1665.7: So.
1666.1 --> 1667.2: Here's the graph model.
1667.3 --> 1668.6: Of the not pecky ATT&CK.
1668.6 --> 1670.0: Along with some countermeasure.
1671.7 --> 1673.8: For that type of ransomware ATT&CK.
1674.7 --> 1675.3: And then.
1675.6 --> 1677.0: This tool.
1677.5 --> 1679.4: If a company wants to create.

1679.4 --> 1680.8: They can actually create it.
1681.1 --> 1682.1: If they actually.
1683.4 --> 1684.8: Go back to.
1685.6 --> 1686.5: The original website.
1687.5 --> 1687.9: So.
1701.1 --> 1709.3: So if you go over here.
1709.7 --> 1710.6: If you go to the cat section.
1710.6 --> 1712.6: You can actually create your own graph.
1712.7 --> 1713.7: Depending on.
1714.0 --> 1715.4: What you're taking a look at.
1715.6 --> 1717.3: And from there you can actually leverage.
1717.5 --> 1719.7: The actual knowledge base itself.
1720.4 --> 1721.6: So as you can see.
1721.8 --> 1723.3: This type of intelligence.
1723.8 --> 1724.9: Is a more higher level.
1725.4 --> 1727.2: But it can actually reach to.
1727.4 --> 1730.2: Different type of more users.
1731.0 --> 1731.0: So.
1731.6 --> 1732.4: But within there.
1732.7 --> 1734.8: We try to also give information.
1735.2 --> 1737.2: So with that lower level.
1737.2 --> 1738.9: Engineers can actually.
1739.7 --> 1740.6: Act on it.
1742.2 --> 1744.1: That was my quick discussion.
1744.4 --> 1746.4: On each of these three tools.
1746.5 --> 1748.1: It's probably the fastest I ever did.
1748.6 --> 1750.1: It's probably each one I could talk.
1750.5 --> 1751.9: An hour each.
1753.6 --> 1754.7: Any questions.
1755.0 --> 1755.5: Comments.
1755.8 --> 1756.4: Suggestions.
1757.8 --> 1760.2: Yeah this is really brilliant.
1760.5 --> 1761.7: I like the look of this.
1761.8 --> 1763.4: And it's almost like we're circling.
1763.4 --> 1764.7: The same problem.
1765.6 --> 1767.7: And just from different approaches.
1768.3 --> 1768.9: Which is neat.
1769.5 --> 1771.6: One question is the edges.
1771.9 --> 1773.1: On the.
1774.6 --> 1775.7: The example.
1775.9 --> 1776.8: The last example.
1777.3 --> 1779.5: Are those edges like standardized.
1779.8 --> 1781.9: Across all of the.
1782.1 --> 1783.9: Graphs or are they dependent on the person.
1784.0 --> 1785.5: Who created it if that makes sense.
1785.6 --> 1787.7: So if we go to the last.
1787.8 --> 1789.1: Example that we had.

1789.4 --> 1791.5: Zooming in thing going on.
1791.5 --> 1792.8: Let me go back.
1793.4 --> 1795.5: So there's three examples here.
1795.6 --> 1796.3: So let's go to.
1796.8 --> 1797.4: Yeah.
1800.0 --> 1800.7: Cool.
1802.3 --> 1803.5: Here's the full graph.
1803.6 --> 1803.8: Sorry.
1804.4 --> 1806.8: So these.
1807.4 --> 1808.8: Tags on the lines.
1809.2 --> 1810.7: One is like verifies.
1811.0 --> 1811.9: One is encrypts.
1812.4 --> 1813.7: Those edges there.
1814.4 --> 1815.9: They're what gives meaning.
1816.6 --> 1818.4: To the thing that is in the.
1819.0 --> 1819.9: The boxes.
1821.0 --> 1822.0: Are those edges.
1822.1 --> 1824.2: Like a standard framework that you guys.
1824.4 --> 1824.6: Okay.
1825.0 --> 1825.1: Yeah.
1825.2 --> 1826.8: So we could very easily.
1827.0 --> 1829.1: Like I could just consume this.
1829.2 --> 1830.2: And then turn it into.
1831.5 --> 1832.5: A spell web.
1832.8 --> 1834.4: Like I showed in the previous one.
1834.6 --> 1834.7: Yeah.
1834.9 --> 1836.2: You can just use this tool.
1836.3 --> 1837.7: And then create your own attack graph.
1837.9 --> 1839.3: Attack model and everything else like that.
1839.3 --> 1840.9: And then that would mean that.
1841.1 --> 1842.7: Someone could then navigate.
1843.0 --> 1845.5: Their own way through those dots.
1846.1 --> 1847.4: And create their own.
1847.6 --> 1848.6: Reconstruction of that.
1848.9 --> 1849.1: Yes.
1849.2 --> 1850.0: If they wanted to.
1850.1 --> 1851.3: They can modify it.
1851.5 --> 1851.6: Yeah.
1851.7 --> 1853.0: That's something we should do.
1853.4 --> 1853.6: Yeah.
1853.8 --> 1854.0: Yeah.
1854.3 --> 1857.5: And the other thing that I was thinking about is.
1858.7 --> 1859.8: I like this.
1859.8 --> 1860.9: Like three.
1862.1 --> 1863.9: Tier where you have attack.
1864.1 --> 1865.1: Adversary defend.
1865.7 --> 1867.3: What would happen if we train.

1867.4 --> 1869.2: Specific agents on these.
1870.0 --> 1871.0: Specific categories.
1872.0 --> 1873.5: And another thing that I liked about.
1873.6 --> 1874.9: The first slide that you had is.
1875.0 --> 1876.3: You've already done the compression.
1876.7 --> 1879.3: Like detect plus application.
1879.9 --> 1881.7: Plus the users context.
1882.4 --> 1882.9: Would be the.
1883.3 --> 1885.4: Yeah if we go to the table.
1885.7 --> 1886.3: Of terms.
1887.0 --> 1887.6: Yeah.
1888.9 --> 1890.4: Maybe back one.
1890.7 --> 1891.6: Because this is the.
1892.5 --> 1893.5: Expansion of that.
1894.5 --> 1895.8: Yeah this one.
1896.0 --> 1897.5: This is the.
1898.9 --> 1899.8: The meat.
1900.0 --> 1900.6: It's really good.
1901.2 --> 1902.1: So you can see.
1904.6 --> 1905.7: These columns.
1906.9 --> 1908.2: Is one part.
1909.0 --> 1909.8: The context.
1910.0 --> 1911.0: That the person comes to.
1911.6 --> 1912.3: Is another part.
1912.3 --> 1913.4: And then where.
1913.9 --> 1914.9: That context hits.
1915.3 --> 1917.6: So whether or not it's gather victim host information.
1917.9 --> 1919.0: Or command and scripting.
1919.5 --> 1920.9: That is the third part.
1921.1 --> 1921.9: And if you could imagine.
1922.2 --> 1924.3: Those three attributes.
1924.7 --> 1926.5: Being compressed into a proverb.
1926.8 --> 1928.5: That connects it to the users context.
1929.5 --> 1932.0: Then they can share that proverb.
1932.4 --> 1933.8: As a key.
1934.4 --> 1935.6: To follow the same path.
1935.8 --> 1936.8: Through this knowledge base.
1937.1 --> 1937.8: That's a good one yes.
1937.8 --> 1939.7: Yeah and then.
1940.4 --> 1941.3: If we.
1942.4 --> 1943.6: Backtrack to the.
1943.8 --> 1945.2: Previous thing that I said we should do.
1945.9 --> 1947.4: That's how we create those.
1947.6 --> 1948.7: Template pathways right.
1949.2 --> 1950.0: That's a good point yes.
1950.4 --> 1951.9: So that.
1953.2 --> 1954.1: Yeah it's.

1954.6 --> 1956.3: I wasn't aware of.
1956.6 --> 1959.3: How well defined.
1959.7 --> 1961.0: This work is.
1961.3 --> 1962.8: I think that realistically.
1963.2 --> 1965.1: We could consume this information.
1965.1 --> 1965.6: And create.
1966.3 --> 1968.4: A knowledge graph similar to the one that I showed.
1968.7 --> 1969.7: Within like a few days.
1970.2 --> 1972.3: As like the begin expression of.
1972.8 --> 1974.0: Either attack defend.
1974.7 --> 1975.6: Or adversary.
1976.7 --> 1978.1: And then the follow on to that.
1978.3 --> 1980.4: The experiment is what happens when those agents.
1980.5 --> 1981.4: Talk to each other and.
1982.2 --> 1983.5: You give one of them a red team.
1983.6 --> 1984.6: And one of them a blue team.
1986.7 --> 1988.0: Instruction or intent.
1989.2 --> 1989.9: So for the red.
1990.2 --> 1991.9: So for this type of knowledge base.
1991.9 --> 1993.1: We try to kind of.
1993.4 --> 1995.7: Just create it more like a dictionary than anything else.
1995.8 --> 1997.3: But people has applied it for.
1997.9 --> 1998.6: Different use cases.
1999.3 --> 2001.7: But it's more specific to that type of activities.
2002.1 --> 2003.7: So and then we see it a lot.
2004.1 --> 2004.8: How people use it.
2005.4 --> 2007.5: And also either merge it into.
2007.6 --> 2009.1: Their process their toolings or.
2009.8 --> 2011.0: You know technology.
2016.3 --> 2016.5: Yeah.
2017.2 --> 2017.5: At the end.
2017.7 --> 2018.9: This is a kind of ontology.
2018.9 --> 2020.3: That can be used to describe.
2021.4 --> 2022.0: Precisely.
2022.9 --> 2024.9: The process kind of attacks.
2025.0 --> 2025.5: And of course.
2025.9 --> 2027.9: I like the approach of the.
2028.5 --> 2030.0: Being able to also.
2031.1 --> 2031.7: To.
2031.9 --> 2033.5: To draw.
2034.2 --> 2035.8: Or to describe the attack path.
2036.0 --> 2037.1: Through the graph approach.
2037.3 --> 2037.8: I think it's.
2038.6 --> 2040.0: It's very helpful.
2040.2 --> 2041.0: Then to visualize.
2042.3 --> 2044.3: The process of a specific attack.

2044.3 --> 2045.4: And the different countermeasures.
2045.6 --> 2046.8: Whether they play a role or not.
2048.4 --> 2049.8: I wonder if this is something.
2050.0 --> 2050.7: That can be helpful.
2050.8 --> 2053.0: Also for guys.
2053.2 --> 2055.3: At SEAL for instance.
2055.4 --> 2056.9: To have a way to describe.
2057.6 --> 2058.4: In a standard.
2058.8 --> 2060.4: Standard way.
2061.7 --> 2062.6: The attack path.
2062.9 --> 2064.2: When investigating.
2065.7 --> 2066.6: Specific cases.
2068.3 --> 2069.7: I don't know if you have an opinion.
2075.0 --> 2075.7: SEAL.
2080.3 --> 2082.2: Saying it differently.
2083.9 --> 2084.9: Do you.
2085.4 --> 2086.0: From time to time.
2086.2 --> 2087.9: Refer to the vocabulary.
2088.2 --> 2089.3: From MITRE.
2090.3 --> 2091.3: On attack paths.
2091.7 --> 2093.0: Or on countermeasure path.
2093.1 --> 2094.0: In order to describe.
2094.7 --> 2095.5: What happens.
2096.1 --> 2097.8: And also to.
2098.8 --> 2100.7: Maybe not to recommend.
2100.7 --> 2101.8: But to understand.
2102.3 --> 2103.4: Which countermeasures didn't work.
2105.9 --> 2106.5: Historically.
2106.8 --> 2108.3: We've not used attack.
2108.5 --> 2109.0: Mainly because.
2109.6 --> 2111.8: We've never really needed to map.
2111.9 --> 2113.0: The web 3 attacks.
2113.6 --> 2116.6: To this terminology.
2117.5 --> 2118.3: But as.
2118.6 --> 2119.6: Crypto attacks move.
2120.3 --> 2120.9: More into web 2.
2121.1 --> 2122.7: This becomes a lot more applicable.
2124.7 --> 2125.6: Truth be told.
2125.7 --> 2127.1: Usually we leave it to.
2128.3 --> 2128.9: Entities like.
2129.3 --> 2130.6: Crowd strike.
2131.0 --> 2132.8: To perform the actual.
2135.6 --> 2136.1: Postmortem.
2136.3 --> 2137.1: On the web 2 side.
2138.4 --> 2138.9: They usually have better.
2139.3 --> 2140.2: Capabilities than we do.
2140.7 --> 2142.2: I suspect they're going to be using.

2142.5 --> 2143.2: Terminology like this.
2144.7 --> 2146.3: But we haven't natively adopted.
2146.5 --> 2147.2: This ourselves yet.
2149.4 --> 2151.0: And follow up to that question.
2151.1 --> 2152.0: I think that was really good.
2152.2 --> 2152.5: And pointed.
2152.5 --> 2154.5: And recognized.
2154.7 --> 2155.8: That some of this is based on.
2156.1 --> 2157.1: Where seal is currently.
2157.3 --> 2158.5: Like pointing most of your efforts.
2158.7 --> 2160.6: Because I let me know if I'm wrong.
2160.6 --> 2162.0: But I think most of your efforts.
2162.0 --> 2163.9: Are focused on recovery of assets.
2163.9 --> 2165.5: But you do do some work on.
2165.7 --> 2166.9: Patching the vulnerabilities.
2167.1 --> 2168.6: Also in the exploits right.
2170.0 --> 2171.0: Based on that.
2171.1 --> 2173.0: I know adapt here was.
2173.1 --> 2174.5: Is the like you know.
2174.6 --> 2175.8: Like living framework.
2175.8 --> 2177.5: That MITRE is has built.
2177.6 --> 2179.5: To kind of adapt and evolve.
2179.9 --> 2181.4: Attack into the web 3.
2181.7 --> 2182.5: Domain and ecosystem.
2183.4 --> 2185.0: So I think it's really interesting.
2185.3 --> 2186.8: For like MITRE to think about.
2187.0 --> 2188.2: And know like how does.
2188.4 --> 2190.3: Thinking about this kind of terminology.
2190.5 --> 2193.1: And like in exploitations.
2193.8 --> 2194.5: And then thinking about.
2194.6 --> 2195.9: How that would map to controls.
2196.3 --> 2197.6: How is that valuable to like.
2197.6 --> 2198.8: An organization like yours.
2198.9 --> 2200.8: Versus maybe something like CCSS.
2200.8 --> 2203.1: So we'll turn to Mark.
2203.3 --> 2203.6: After that.
2203.8 --> 2205.5: But I'm curious like how like.
2205.6 --> 2206.8: Do you feel like this sort of thing.
2207.4 --> 2208.3: That's done some adaptation.
2208.6 --> 2209.8: Into the web 3 world.
2210.4 --> 2211.4: Is that useful for you.
2211.5 --> 2213.7: Is that like more useful.
2213.8 --> 2214.9: For something that's thinking more.
2215.0 --> 2215.8: On the cybery.
2215.9 --> 2217.0: And like fixing the underlying.
2217.1 --> 2218.5: Code side or it's like.
2218.7 --> 2220.0: Because you do some work on both.

2220.1 --> 2221.1: Like recovery of assets.
2221.1 --> 2223.1: And fixing the like underlying tech.
2223.6 --> 2224.8: In some of the compromises right.
2225.5 --> 2227.0: Yeah this is actually really interesting.
2227.2 --> 2228.4: I wasn't aware this.
2229.4 --> 2230.1: Adaptation existed.
2230.8 --> 2232.0: I think this is.
2232.1 --> 2233.4: I mean looking at it over a glance.
2233.6 --> 2234.9: It looks pretty comprehensive.
2236.0 --> 2237.3: I think there might be one or two things.
2237.5 --> 2238.2: That we could add to it.
2238.3 --> 2240.4: But overall this is like a really solid framework.
2240.9 --> 2244.1: And I think the question mark for us.
2244.3 --> 2245.6: As to you know.
2246.4 --> 2248.0: When or why we would adopt it.
2248.0 --> 2249.8: Is I think it comes down to.
2250.4 --> 2252.2: Whether our stakeholders would use it.
2253.2 --> 2254.4: I think right now.
2254.5 --> 2255.6: Our stakeholders are primarily.
2256.2 --> 2257.2: Other crypto you know.
2257.4 --> 2258.3: Crypto developers who.
2259.0 --> 2260.8: They just want to get to the root cause.
2260.9 --> 2261.8: They want to fix the issue.
2261.9 --> 2262.7: They want to put out the tweet.
2263.7 --> 2265.4: I think we're you know.
2265.5 --> 2267.6: Coming to 2026 we're seeing more.
2268.1 --> 2269.1: Involvement from institutions.
2270.2 --> 2271.7: We're finding a lot more.
2272.2 --> 2273.8: Legacy partners want to.
2273.8 --> 2275.1: Work with CEO and figure out.
2275.4 --> 2276.3: How they can get more involved.
2277.3 --> 2279.6: I suspect their security.
2279.8 --> 2281.6: Teams would be interested in.
2282.2 --> 2283.5: You know using this existing terminology.
2283.8 --> 2284.9: That they're familiar with.
2285.6 --> 2286.5: With ATT&CK.
2287.0 --> 2288.9: So I think that could be an impetus.
2288.9 --> 2290.5: For why we would adopt this.
2291.0 --> 2292.4: But I think it sort of comes down to.
2292.7 --> 2294.9: Do our stakeholders want to see.
2295.1 --> 2296.8: Structured data using this format.
2297.3 --> 2299.0: Can they actually get leverage out of it.
2299.2 --> 2300.2: And then if so I think we would.
2300.2 --> 2301.3: Happily adopt it.
2302.8 --> 2304.4: I love that framing.
2304.6 --> 2305.7: I think that really points to.
2306.0 --> 2308.4: What elements of these frameworks are useful.

2308.6 --> 2310.4: To the different participants in the ecosystem.
2311.7 --> 2312.2: So one of my.
2312.5 --> 2314.3: Based on that comment of the idea.
2314.5 --> 2316.4: That like thinking about what the.
2316.5 --> 2318.5: Exploits and TTPs look like.
2318.8 --> 2320.6: Versus what the controls are.
2320.8 --> 2323.0: That developers and engineers want to build in.
2323.2 --> 2324.8: To prevent stuff like this.
2326.0 --> 2326.6: That like.
2326.8 --> 2328.7: That specific thing is useful to.
2328.7 --> 2329.8: Standards orgs.
2330.0 --> 2331.8: Regulators when thinking about what those controls are.
2332.0 --> 2334.1: And developers and engineers that want to build in the controls.
2335.0 --> 2336.4: Knowing the TTPs.
2336.5 --> 2337.8: And agreeing around this.
2337.8 --> 2339.9: Is helpful for folks that care about.
2340.6 --> 2342.7: Understanding the nature of like.
2342.9 --> 2343.6: Of the ATT&CK.
2343.6 --> 2345.5: So I guess those that are interested in like a heatmap.
2345.7 --> 2348.0: Of where threats sort of exist.
2348.1 --> 2349.7: And like which things are the most common.
2350.8 --> 2352.5: So again useful to security professionals.
2352.8 --> 2354.5: But are these mapped specifically.
2354.7 --> 2357.0: To controls that would defend against the TTPs too.
2357.0 --> 2359.2: Or is that like a next phase of evolution?
2362.7 --> 2364.1: Let me just quickly take a look.
2364.5 --> 2366.2: I think we may have you know.
2366.5 --> 2367.5: Let me just take a look but I don't want to.
2368.4 --> 2369.1: Let me just.
2369.1 --> 2369.5: No worries.
2370.1 --> 2372.4: And then I guess on deck like Mark.
2372.5 --> 2374.0: I'm curious if you have thoughts about.
2374.4 --> 2376.8: How or if this kind of framing.
2377.3 --> 2379.0: That like where MITRE has adapted.
2379.6 --> 2381.4: Their ATT&CK framework into ADAPT.
2381.5 --> 2382.7: Which is like a crypto focus.
2382.7 --> 2384.7: Like what those ATT&CK vectors look like.
2385.2 --> 2387.0: For like an entity like yours.
2387.1 --> 2388.7: That is creating very like.
2388.9 --> 2390.6: Specific and exquisite standards.
2391.0 --> 2391.9: Around like controls.
2392.8 --> 2394.6: Useful for the crypto community.
2394.8 --> 2396.7: To defend against those TTPs.
2397.2 --> 2398.6: How or is.

2398.9 --> 2400.6: Like this kind of structure.
2400.9 --> 2402.8: Useful to an organization like yours.
2403.4 --> 2404.6: We may need to get Mark.
2404.9 --> 2406.2: A microphone.
2407.3 --> 2407.8: If you guys.
2407.9 --> 2408.7: He's coming up behind you.
2409.6 --> 2410.7: Over there.
2417.6 --> 2418.4: Yeah I mean.
2418.5 --> 2420.1: We're very much aware of MITRE.
2420.8 --> 2421.6: The CCSS.
2422.6 --> 2424.4: It's one of the ones that we actually.
2424.6 --> 2426.0: Look at quite a bit.
2426.7 --> 2428.3: In terms of when we're mapping out.
2428.4 --> 2429.0: Requirements.
2430.0 --> 2432.3: And it is very effective as well.
2434.9 --> 2436.7: Specifically what we do generally.
2436.7 --> 2438.8: When we're looking for the requirements for us.
2439.1 --> 2440.5: The standard is we look at.
2440.6 --> 2442.6: You know how the ATT&CK occurred.
2443.0 --> 2444.6: And then framing it around.
2444.9 --> 2445.9: MITRE as well.
2446.4 --> 2446.9: So it is.
2447.5 --> 2449.4: We basically look at this as well.
2450.0 --> 2450.7: It's really good.
2451.4 --> 2453.0: And the ADAPT ones.
2453.3 --> 2455.5: Is really really good.
2455.9 --> 2457.3: And on the auditing side of.
2457.6 --> 2458.6: My profession.
2459.2 --> 2461.3: We also recommend it to clients as well.
2461.8 --> 2462.9: It's something to look at.
2467.0 --> 2468.9: In terms of MITRE ATT&CK itself.
2469.0 --> 2470.5: We do have the mitigation for enterprise.
2470.8 --> 2471.4: For each ATT&CK.
2472.3 --> 2473.9: The actual ADAPT doesn't have that yet.
2475.3 --> 2476.9: But there's also MITRE DEFEND.
2477.1 --> 2478.5: Which is a lot of your controls into.
2478.6 --> 2480.2: But on a different type of information.
2480.8 --> 2481.4: But it's more.
2481.8 --> 2483.7: If you take a look at the defense stuff.
2484.0 --> 2486.0: A lot of engineers can probably resonate to that.
2486.1 --> 2487.0: Because they do the harden.
2488.1 --> 2489.6: And those type of steps.
2489.7 --> 2491.1: Because that's what they do as a defender.
2491.5 --> 2492.1: So over.
2494.7 --> 2495.8: One of the.
2496.7 --> 2498.2: Additional value I see.
2498.5 --> 2500.0: With a work like ADAPT.

2500.5 --> 2501.4: Is that.
2502.0 --> 2503.3: Maybe it will resonate for.
2503.8 --> 2504.4: But with.
2505.3 --> 2506.4: With a trend of having.
2507.4 --> 2509.0: More let's say classical players.
2509.1 --> 2510.4: Involved also in web 3.
2511.2 --> 2512.4: You need to.
2512.7 --> 2513.7: Speak the same language.
2514.5 --> 2516.4: So something that is defined.
2517.3 --> 2518.4: Following MITRE.
2519.1 --> 2520.1: Perspective and MITRE.
2521.7 --> 2523.4: Habits of defining attacks.
2523.9 --> 2525.4: Might not be the same way as.
2525.5 --> 2526.3: Web 3 developers.
2527.8 --> 2529.2: Engineers are defining.
2529.6 --> 2530.8: Some of the ATT&CK paths.
2531.0 --> 2533.4: So having a common vocabulary.
2533.7 --> 2534.8: At least a way.
2535.1 --> 2536.4: To refer to a common one.
2536.9 --> 2538.1: Can be a way to.
2539.1 --> 2539.6: Well.
2540.6 --> 2542.6: More quickly explain an ATT&CK.
2542.8 --> 2544.7: More quickly launch an investigation.
2544.9 --> 2546.8: Because when you discuss with some stakeholders.
2547.0 --> 2548.2: That are not speaking the same language.
2548.2 --> 2549.3: Of course investigating.
2549.7 --> 2550.6: Specific ATT&CK paths.
2550.9 --> 2552.7: Can be a nightmare.
2553.1 --> 2554.2: Just because you don't.
2554.3 --> 2555.1: Understand each other.
2555.2 --> 2556.6: So I guess at some point.
2556.7 --> 2557.3: It would be useful.
2557.7 --> 2558.8: Yeah I totally agree.
2559.0 --> 2560.4: I think you know.
2560.4 --> 2561.4: ATT&CK and ADAPT.
2561.9 --> 2564.4: This is sort of standard terminology.
2565.6 --> 2568.5: I think it's.
2568.9 --> 2570.2: I mean I'm personally.
2570.2 --> 2571.8: Very excited to see.
2571.8 --> 2573.6: What I would view as.
2574.1 --> 2575.6: The crypto security community.
2575.7 --> 2577.4: Leveling up by adopting this framework.
2578.7 --> 2579.8: I think today it's.
2580.1 --> 2581.0: I mean you know.
2581.1 --> 2582.5: People are resistant to change.
2583.0 --> 2585.2: And people love their workflows right.
2585.2 --> 2586.3: It's like you broke the space bar.

2586.4 --> 2587.4: Now it doesn't overheat my CPU.
2587.8 --> 2589.2: So that's broken workflow.
2589.9 --> 2592.3: And I think getting adoption on this.
2592.5 --> 2594.4: At least within the CEO community.
2595.3 --> 2596.6: Over the years that I've understood.
2596.9 --> 2598.8: It's you know people value.
2598.8 --> 2600.9: You know like.
2601.2 --> 2603.2: Does their work and does their effort.
2603.4 --> 2605.5: Actually translate into some you know.
2605.9 --> 2606.9: Some additional leverage.
2607.0 --> 2608.2: Like moving the needle in some form.
2608.7 --> 2611.1: And so I think if there was some way.
2611.6 --> 2613.5: The people in this room or on the call.
2613.7 --> 2615.7: Or maybe we expand the scope somewhat.
2616.0 --> 2617.7: But if there's a way that we could actually.
2619.1 --> 2620.1: Construct a scenario.
2620.5 --> 2621.7: In which you know.
2621.9 --> 2623.2: By utilizing this framework.
2623.6 --> 2625.0: We can show that there's actually.
2625.3 --> 2627.4: Increased efficiency or some upside.
2627.9 --> 2629.4: I think we might have to basically.
2630.2 --> 2631.9: Put in the effort to create that scenario.
2632.3 --> 2633.4: Before we can then get adoption.
2634.6 --> 2636.0: Because otherwise you know.
2636.1 --> 2637.8: There's just no upside to trying to convince.
2637.9 --> 2640.3: A bunch of people to figure out how to do this thing.
2640.3 --> 2641.3: So then they can use the new thing.
2641.4 --> 2642.4: So they can learn a new thing.
2642.4 --> 2644.6: And we might have to do that work ourselves first.
2648.1 --> 2649.2: Very good point yeah.
2649.5 --> 2651.7: It's a good idea to try to work out.
2651.8 --> 2652.7: A scenario like this yeah.
2653.3 --> 2655.3: So I just quickly googled.
2655.3 --> 2657.5: So if you googled actually attack flow.
2657.7 --> 2659.0: There is now an attack flow.
2659.4 --> 2660.1: It's over.
2661.8 --> 2662.7: So actually.
2663.3 --> 2664.4: Tying the.
2665.2 --> 2667.4: Before coffee to after coffee session.
2668.6 --> 2669.6: On the one hand.
2669.7 --> 2670.5: You know LLMs are great.
2670.7 --> 2672.3: You just spit.
2673.5 --> 2675.0: Random words at it.
2675.0 --> 2676.4: And it understands it and all that.
2676.5 --> 2678.2: But you know those things work a lot better.
2678.7 --> 2680.9: When you're using a common language.
2681.6 --> 2683.1: So is there.

2683.1 --> 2684.7: An interest.
2685.3 --> 2685.7: In.
2687.1 --> 2688.4: Not reinventing the wheel.
2688.6 --> 2690.1: We've got a common language.
2690.8 --> 2692.8: And would then people be willing.
2693.6 --> 2694.7: To put stuff in.
2694.8 --> 2695.8: Because in fact right now.
2696.9 --> 2697.8: It's pretty dumb.
2698.0 --> 2698.8: It doesn't know anything.
2699.6 --> 2701.8: So we need to get a lot of data into.
2703.1 --> 2703.5: The.
2704.5 --> 2706.7: AI tool to make it worthwhile.
2707.6 --> 2709.0: Do you would you would you say.
2709.2 --> 2709.9: Oh yeah you know.
2710.6 --> 2711.8: This will help me out.
2712.0 --> 2713.5: Because it's going to give me a corpus.
2713.7 --> 2714.9: Of stuff that I don't already had.
2715.0 --> 2715.7: Are you just like.
2716.1 --> 2717.3: We already have a big corpus.
2717.4 --> 2719.3: We don't need to go outside.
2720.4 --> 2722.3: I think being able to categorize.
2722.6 --> 2724.3: The data through.
2725.1 --> 2726.5: You know classifications like this.
2726.7 --> 2728.1: Makes retrieval a lot easier.
2728.8 --> 2730.6: So that that is a huge upside for me.
2732.1 --> 2733.0: I think.
2733.3 --> 2735.2: Absent the manpower to.
2735.8 --> 2737.0: To do that internally.
2737.0 --> 2738.1: Which we don't have that.
2738.3 --> 2739.2: We don't have at the moment.
2739.6 --> 2740.3: But also absent.
2740.8 --> 2741.9: Like private inference.
2742.2 --> 2743.9: Because I think most people.
2744.2 --> 2744.8: Ourselves included.
2744.9 --> 2746.5: Would be very reluctant to dump.
2746.7 --> 2747.5: All of our TLP red data.
2747.6 --> 2749.4: Into like cloud or chat GPT or whatever.
2750.2 --> 2751.4: It does feel like a bit of.
2752.0 --> 2753.2: You know like being stuck.
2753.2 --> 2754.2: Between a rock and a hard place.
2754.6 --> 2755.5: But it would be great.
2755.5 --> 2756.5: To get to a point where.
2757.2 --> 2758.6: You know as part of the.
2758.8 --> 2759.5: Instant response workflow.
2760.6 --> 2761.4: You know people.
2761.8 --> 2762.8: Were able to take.
2763.0 --> 2763.7: I'm not actually sure.

2763.8 --> 2765.6: Maybe it only takes like five minutes right.
2765.9 --> 2767.0: Maybe it's really quick and simple.
2767.1 --> 2767.6: Maybe it's not.
2768.0 --> 2769.3: But for people to be able to take the time.
2769.4 --> 2770.7: And like categorize it.
2771.2 --> 2771.8: According to this.
2771.9 --> 2772.8: And then you know over time.
2773.0 --> 2774.1: Possibly even expand it to.
2774.6 --> 2776.7: Cover other missing techniques.
2779.3 --> 2779.8: Yeah.
2780.3 --> 2781.6: I know that this is.
2781.8 --> 2783.0: Something that I've said it.
2783.3 --> 2784.6: For the last three years.
2785.1 --> 2787.1: But I will still like.
2787.4 --> 2788.2: I think that.
2789.6 --> 2791.6: One of the ways to help meet this need.
2791.9 --> 2793.6: That I really appreciate.
2793.7 --> 2795.2: Sam highlighting for us.
2795.3 --> 2796.8: Is like when trying to think about.
2796.9 --> 2798.7: What is the scenario in which this is useful.
2799.1 --> 2800.9: Like I think about the things.
2801.2 --> 2803.4: Every ISAC that Eric helped stand up.
2803.5 --> 2804.7: In the OG days of ISACs.
2806.1 --> 2807.3: Because for those that.
2807.4 --> 2808.2: If you don't know Eric Berger.
2808.4 --> 2810.1: He did stand up like most of the ISACs.
2810.7 --> 2811.8: Back like in the.
2812.0 --> 2812.9: Like starting in the 90s.
2814.7 --> 2815.8: Trying to help highlight.
2816.1 --> 2817.2: Like the context of.
2817.3 --> 2819.4: Like the sticks and taxi for crypto.
2819.5 --> 2820.5: That does not exist.
2820.7 --> 2821.5: Which of course.
2822.0 --> 2823.8: Can mean going to Oasis.
2824.1 --> 2825.3: And adapting sticks and taxi.
2825.5 --> 2828.9: To include this in the fields about vectors of attack.
2829.5 --> 2831.2: If we don't want it to be sticks and taxi.
2831.2 --> 2832.1: I don't care.
2832.2 --> 2833.6: Whatever industry wants and likes.
2833.7 --> 2834.7: Is like the specific standard.
2834.7 --> 2836.4: For how they want to be able to share the information.
2836.4 --> 2837.1: Is fine with me.
2837.5 --> 2838.3: But you know.
2838.5 --> 2840.0: Since taxi clients already exist.
2840.1 --> 2841.2: And you already have that like.
2841.3 --> 2843.4: The protocol for the exchange of information.
2843.8 --> 2845.4: This would mean changing sticks.

2845.5 --> 2847.3: The language for IOCs.
2847.4 --> 2849.0: To include stuff like this.
2849.8 --> 2851.2: I'm sure that there's pros and cons.
2851.4 --> 2852.0: On like.
2852.0 --> 2855.0: On leveraging the exact same.
2855.9 --> 2857.0: Standard and methodology.
2857.3 --> 2858.4: For how we already share.
2858.5 --> 2860.3: Machine readable IOCs with each other.
2860.7 --> 2861.4: But thinking about.
2861.5 --> 2862.9: Some of that also points to.
2863.3 --> 2864.4: Some stuff that I wanted to highlight.
2864.8 --> 2865.6: Like there's.
2866.6 --> 2868.2: At the very beginning when we talked about.
2868.4 --> 2870.3: The state of threat information sharing.
2870.7 --> 2872.2: There's a lot of different partnerships.
2872.5 --> 2873.6: That are happening right now.
2874.8 --> 2876.8: So besides the ones that are crypto specific.
2877.4 --> 2877.8: There's.
2878.9 --> 2881.0: There's a lot of fraud information sharing.
2881.3 --> 2882.6: There's things like.
2882.8 --> 2883.2: The NICMIC.
2883.4 --> 2885.2: Which is sharing information around CSAM.
2885.2 --> 2886.5: Child and sexual abuse material.
2887.0 --> 2888.5: Obviously we know that there's touch points.
2888.6 --> 2889.8: With crypto flows sometimes.
2890.3 --> 2891.9: The global signals exchange.
2892.3 --> 2895.3: Is an example of where the main tech platforms.
2895.5 --> 2896.9: So think web 2 and social media.
2897.2 --> 2899.4: Are sharing technical indicators.
2899.4 --> 2900.3: Around fraud.
2900.7 --> 2901.2: Not crypto.
2901.3 --> 2902.8: Crypto is not involved in GSE.
2903.4 --> 2904.1: Yet ever.
2904.3 --> 2904.7: I don't know.
2905.0 --> 2906.6: How cool would it be if some of this.
2906.6 --> 2909.2: Became like the crypto partners to GSE.
2909.5 --> 2911.2: To kind of create the.
2911.5 --> 2913.4: To fill the gaps on the flows.
2913.4 --> 2914.8: Of like where crypto is certainly.
2914.9 --> 2916.0: Playing a role in all this.
2916.8 --> 2918.0: I bring up those things.
2918.2 --> 2920.2: Because they're like more to just highlight.
2920.3 --> 2921.4: That some of the broader issues.
2921.4 --> 2922.2: That have come up around.
2922.4 --> 2923.8: What the policy enablers are.
2923.9 --> 2925.1: To allow this to be shared.
2925.1 --> 2926.9: But then also thinking about okay.

2927.1 --> 2929.5: How do we want to distill down.
2929.6 --> 2930.7: Exactly what Sam said.
2930.8 --> 2932.3: Of like the practical use case.
2932.3 --> 2933.9: That will make it really attractive.
2933.9 --> 2935.4: To get the security professionals.
2935.7 --> 2936.8: To know why it's valuable.
2937.5 --> 2939.4: And maybe that's where like.
2940.0 --> 2941.2: Some of the work that.
2941.6 --> 2944.5: There's an international US UK treasury.
2944.5 --> 2946.7: Co-chaired fraud task force right now.
2947.7 --> 2949.7: I'm part of the secretariat on it.
2949.7 --> 2951.0: And like some of the work that we're doing.
2951.1 --> 2952.2: Is around information sharing.
2952.2 --> 2953.8: And like we're looking very hard.
2953.9 --> 2956.3: At stuff like trying to identify.
2956.4 --> 2958.9: The very specific pieces of information.
2959.2 --> 2960.2: That are the most valuable.
2960.4 --> 2961.8: To share in the near term.
2962.2 --> 2962.8: Like that basically.
2963.0 --> 2964.2: Like I have no idea of seal 911.
2964.4 --> 2965.8: If you guys already have a structure.
2966.1 --> 2967.5: For your requests.
2967.6 --> 2968.9: Or if basically that's something.
2969.0 --> 2969.9: That you're working to create.
2970.7 --> 2971.9: It's the kind of thing.
2972.1 --> 2973.2: That like in the army.
2973.3 --> 2975.2: We had what was called a nine line.
2975.2 --> 2977.3: I know I've used this talking point before.
2977.4 --> 2978.6: So I apologize for those of you.
2978.7 --> 2979.5: That have been here to hear it.
2980.1 --> 2981.8: Like it was the army's standard.
2982.1 --> 2983.2: For the military standard.
2983.4 --> 2985.2: For like if you are hurt.
2985.5 --> 2986.8: This information needs to be called.
2986.9 --> 2987.9: Over the radio and then we know.
2988.1 --> 2989.2: How to come and insert help.
2989.5 --> 2991.2: That's the same kind of like.
2992.4 --> 2993.7: Assistance that's needed here.
2993.7 --> 2994.6: It's just not a medevac.
2994.7 --> 2995.4: It's to help a victim.
2995.4 --> 2996.4: That has been defrauded.
2996.4 --> 2999.0: Or an exchange that needs to recoup its funds.
2999.4 --> 3001.6: There's a specific discrete set of information.
3001.6 --> 3003.0: That is the most valuable.
3003.1 --> 3004.3: To be shared in the near term.
3004.7 --> 3006.0: Then there's like sticks and taxi.
3006.2 --> 3007.9: Which is the whole ecosystem.

3008.3 --> 3010.3: Of the whole scope of every bit of information.
3010.3 --> 3011.3: That could be shared.
3011.8 --> 3013.5: We could start by just identifying.
3013.8 --> 3016.2: Those very specific most valuable.
3016.4 --> 3017.5: But the highest value.
3017.8 --> 3019.6: Use cases of information.
3020.3 --> 3022.2: Create the scenario that Sam has talked about.
3022.4 --> 3024.7: Paint the value of mapping it to this.
3025.3 --> 3026.3: Maybe that's the moment.
3026.4 --> 3027.6: I know I was giving a lot of context.
3027.8 --> 3029.4: Behind why that's my recommendation.
3029.8 --> 3031.6: But I do think there's an opportunity.
3031.6 --> 3034.4: For us to create the nine line.
3034.6 --> 3036.9: The emergency hotline call for help.
3037.2 --> 3038.8: To work with the major stakeholders.
3038.8 --> 3040.2: That are actually helping victims.
3040.4 --> 3041.9: We could define that.
3042.0 --> 3043.6: That could be something that would be helpful.
3043.6 --> 3044.8: It would also be helpful to a chat bot.
3044.9 --> 3046.5: That wants to think about what information.
3046.5 --> 3048.5: Would be shared up front.
3048.6 --> 3050.8: To help support specific use cases.
3050.8 --> 3053.7: Is it to help fix vulnerability in a smart contract.
3053.8 --> 3055.6: Or is it to help go recover funds.
3055.9 --> 3056.9: For a victim.
3057.4 --> 3057.7: Sorry Sam.
3059.0 --> 3061.3: Okay I have a few varying thoughts.
3061.4 --> 3062.2: The first one really quickly.
3062.4 --> 3064.0: I notice we have nine chat messages.
3064.2 --> 3065.4: I don't know if people.
3067.1 --> 3068.0: Okay I just want to make sure.
3068.2 --> 3070.0: We aren't neglecting the remote.
3070.6 --> 3072.2: Okay so on the nine line.
3072.3 --> 3073.9: We've actually experimented with.
3074.2 --> 3076.7: Trying to distill down the core set of information.
3076.9 --> 3078.2: That from our perspective.
3078.2 --> 3080.4: When we want to liaise.
3080.6 --> 3081.5: With particularly exchanges.
3083.1 --> 3084.0: Anyone who.
3084.2 --> 3085.3: Any centralized entity.
3085.8 --> 3086.8: Who might have information.
3087.4 --> 3089.9: That we need as part of an investigation.
3091.9 --> 3093.0: We have a pretty.
3093.8 --> 3095.2: Good idea of what information.
3095.9 --> 3097.2: Is required from them at this point.
3097.6 --> 3098.7: Or by them at this point.
3099.0 --> 3100.1: The actual harder problem.

3100.2 --> 3101.4: Is not necessarily defining the schema.
3101.7 --> 3104.1: It's getting past all the legal and compliance hurdles.
3104.3 --> 3105.7: That all these exchanges put up.
3105.7 --> 3107.3: I think we can definitely.
3107.6 --> 3109.2: I think we can knock this out in a day.
3109.3 --> 3110.9: We can figure out exactly the schema that we need.
3111.0 --> 3112.6: And then we can spend the next four months.
3113.1 --> 3116.3: On solving the information sharing problem.
3117.9 --> 3120.1: I was thinking about.
3120.7 --> 3121.8: The scenario again.
3122.0 --> 3123.0: As we were talking.
3125.9 --> 3127.4: I'm not sure if this is a hot take or not.
3128.5 --> 3129.6: One thought was like.
3130.2 --> 3131.7: Part of the value of.
3131.9 --> 3133.6: A framework like attack or adapt.
3133.6 --> 3134.7: Is that you know.
3135.2 --> 3137.4: You need these increasing layers of abstractions.
3137.5 --> 3139.1: As the community.
3139.1 --> 3140.4: And the audience grows bigger.
3140.7 --> 3142.7: Because the ability to like transmit.
3142.9 --> 3144.1: Information across audiences.
3144.5 --> 3146.7: Just like diminishes with the size.
3147.1 --> 3149.2: And so part of the reason.
3149.3 --> 3150.7: Why crypto hasn't adopted this.
3150.8 --> 3153.0: Could be like a very very reasonable.
3153.3 --> 3154.7: The community is just small enough.
3154.8 --> 3156.0: That like you can actually communicate.
3156.5 --> 3158.4: Information within the web three circles.
3158.5 --> 3159.6: Properly and effectively.
3159.6 --> 3161.8: Without needing to rely on abstractions.
3163.5 --> 3164.6: But at the same time.
3164.7 --> 3165.7: I think it's a fact that like.
3165.9 --> 3168.0: The web two security community has grown.
3168.4 --> 3169.9: It's massive at this point.
3170.0 --> 3171.2: And like you need things like this.
3172.2 --> 3173.0: And from.
3174.0 --> 3175.8: I think one thing that.
3176.3 --> 3176.4: You know.
3177.2 --> 3179.2: One way I could imagine this working out is like.
3179.9 --> 3181.5: At the end of the day we want to stop hacks.
3182.2 --> 3183.8: A lot of these hacks are now impacting.
3184.4 --> 3185.4: Either web two organizations.
3185.6 --> 3187.4: Or organizations in like a very web two way.
3187.4 --> 3190.2: If we want to.
3190.3 --> 3192.0: Demonstrate that you know.
3192.4 --> 3193.8: Some change in process.

3193.9 --> 3195.4: Has resulted in less hacks.
3195.9 --> 3197.4: Absent you know proving the negative.
3197.7 --> 3199.8: The next best thing we can do is like demonstrate that.
3200.3 --> 3201.8: By providing this structured information.
3202.2 --> 3204.5: To teams that primarily.
3204.8 --> 3205.9: Speak this language.
3206.6 --> 3208.7: They were able to actually act on it.
3209.0 --> 3209.7: In some way that was like.
3209.9 --> 3212.3: That action or the results of that action.
3212.5 --> 3215.1: Were visible to the people supplying it.
3215.3 --> 3217.0: You know us at the table.
3217.8 --> 3219.5: What does that look like in practice?
3219.9 --> 3221.0: Like perhaps it's.
3222.2 --> 3224.3: You know after two months of coordination.
3225.2 --> 3225.8: We can.
3226.8 --> 3228.0: Run some sort of exercise.
3228.4 --> 3229.4: With major exchanges.
3230.1 --> 3232.3: Or with you know like major protocols.
3233.0 --> 3234.4: With banks whoever.
3234.6 --> 3235.0: But like.
3235.9 --> 3238.5: Some security training.
3238.8 --> 3240.6: Session where we.
3241.1 --> 3242.4: Leverage this framework.
3242.8 --> 3244.7: Maybe by providing like a simulation of sorts.
3244.9 --> 3246.3: Or maybe by running through.
3246.3 --> 3247.2: Like past examples.
3247.5 --> 3249.6: Or like you know whatever it could be.
3249.9 --> 3250.7: Using this.
3251.2 --> 3253.4: But crucially like I think we need to show that.
3253.9 --> 3255.9: That exercise that work produced.
3256.0 --> 3256.7: Results right.
3257.2 --> 3258.7: If it just goes in the black hole of like.
3259.1 --> 3260.6: We prepared a bunch of structured data for you.
3260.6 --> 3263.3: It took us like 5, 10, 20 hours to do this.
3263.8 --> 3264.7: Throw it into the black hole.
3265.1 --> 3265.8: Nothing happens.
3266.3 --> 3268.3: Like I think that is then like very demoralizing.
3268.4 --> 3270.1: At least from my perspective.
3270.3 --> 3272.1: Like I think it would be a very hard sell.
3272.1 --> 3274.7: To convince the CL community to do that.
3275.0 --> 3275.9: On the flip side.
3276.5 --> 3278.6: If it was a collaborative process.
3278.7 --> 3280.5: Where we prepared all this data.
3280.8 --> 3281.7: The data was used.
3281.9 --> 3283.2: Consumed in a way that was visible.
3284.2 --> 3286.4: You know like everyone felt really good about.

3286.8 --> 3288.0: The time being spent.
3288.2 --> 3289.8: Not only on the preparation but the implementation.
3290.6 --> 3292.2: And then perhaps like.
3292.8 --> 3294.3: Six months down the line.
3294.8 --> 3295.7: That organization says hey.
3295.8 --> 3297.3: We totally prevented a hack.
3297.5 --> 3298.6: That's like the cherry on top.
3298.6 --> 3300.3: But I think that visibility is.
3300.4 --> 3302.1: You know is going to be a key component.
3302.5 --> 3304.3: Of how we structured this process.
3307.0 --> 3308.6: Also just want to add too.
3309.2 --> 3310.6: From a regular.
3310.8 --> 3312.7: Policy regulation point of view.
3313.7 --> 3314.8: From my point of view.
3315.3 --> 3316.7: The actual mitigation.
3317.2 --> 3318.9: Is actually something that I found.
3319.3 --> 3319.7: Useful.
3320.2 --> 3321.9: Because that will actually tell you.
3322.3 --> 3324.4: Some of the actual mitigation.
3324.7 --> 3325.6: For specific attack.
3325.6 --> 3328.0: But if you actually go to the defend itself.
3328.7 --> 3330.0: If you go to the actual.
3331.7 --> 3332.6: Graph of it.
3332.9 --> 3333.6: So if I go back.
3333.8 --> 3333.9: Sorry.
3335.6 --> 3337.5: If you take a look at it right.
3337.9 --> 3339.3: Based on these type of.
3339.8 --> 3341.8: Categorization from a defend point of view.
3342.2 --> 3343.6: There's actually something now.
3343.8 --> 3345.2: When you create your policy.
3345.4 --> 3346.7: Within an institution or whatever.
3348.0 --> 3350.0: You're now able to communicate.
3350.2 --> 3351.4: With different type of users.
3352.6 --> 3353.5: Right so hardening.
3353.5 --> 3356.1: So now from a higher level.
3356.9 --> 3357.9: When you say yes.
3358.1 --> 3359.3: I am hardening.
3359.8 --> 3361.0: But an actual engineer now.
3361.2 --> 3362.1: Can I just say yes.
3362.3 --> 3364.8: I am doing biometric authentication.
3365.0 --> 3365.6: I'm doing this.
3365.7 --> 3366.3: I'm doing that.
3366.7 --> 3369.5: So now when a higher level.
3369.8 --> 3371.6: Non cyber folks now.
3372.1 --> 3373.5: Seize that type of information.
3374.2 --> 3375.8: They now know exactly how.
3377.5 --> 3378.7: Translate from a.

3379.3 --> 3380.3: Defending point of view.
3380.3 --> 3382.1: So yeah.
3383.5 --> 3384.2: And I.
3385.3 --> 3386.8: Again building on both.
3386.9 --> 3388.3: Both of the last two comments.
3388.5 --> 3388.8: Like the.
3390.4 --> 3392.1: Layers of like.
3392.9 --> 3394.4: The of the value chain.
3394.6 --> 3396.2: And the utility for folks to different.
3396.2 --> 3397.6: Kinds of stakeholders I think.
3398.2 --> 3399.8: Like when you have something like.
3400.0 --> 3401.3: Adapt like an understanding.
3401.6 --> 3402.9: The threat TTPs.
3404.3 --> 3405.9: It's useful that like.
3406.2 --> 3407.4: Basically if you have that understanding.
3407.4 --> 3408.3: As one layer.
3408.9 --> 3410.0: An overlay on top of that.
3410.2 --> 3412.1: Would be the actual threat picture.
3412.4 --> 3413.6: Like where the threat firms come in.
3413.7 --> 3415.2: And they overlay it with like the actual.
3415.8 --> 3417.2: Situation and environment.
3417.8 --> 3419.3: Where they're racking and stacking.
3419.7 --> 3420.8: All of those different TTPs.
3420.9 --> 3423.1: And saying which ones are present.
3423.4 --> 3425.1: Most commonly.
3425.8 --> 3426.7: Across you know.
3426.8 --> 3428.3: And targeting the crypto ecosystem.
3428.9 --> 3431.4: And then underneath the TTPs.
3431.4 --> 3432.5: Comes pointing to.
3432.5 --> 3435.0: What are the controls that defend against.
3435.4 --> 3436.1: Each of those things.
3436.2 --> 3438.8: And that's where this kind of stuff mapped.
3439.1 --> 3441.5: Where some of it we know is very OG.
3441.7 --> 3442.1: Web 2.
3442.7 --> 3443.2: Traditional techie.
3443.6 --> 3445.4: And some of it's pretty bespoke crypto-y.
3445.7 --> 3447.4: And stuff like what CCSS has been building.
3447.9 --> 3449.8: And other things that like.
3449.9 --> 3451.2: That Begin has published around.
3451.5 --> 3453.8: Around secure wallet and key manager practices.
3455.1 --> 3457.0: Basically that inside of all of that.
3457.2 --> 3458.8: It hearkens to the work.
3458.9 --> 3460.8: That JFSA has been working on.
3460.8 --> 3463.2: Where you guys have been specifically looking at.
3463.5 --> 3465.5: Like the actual threat picture.
3465.7 --> 3467.4: Like very specific attacks that occurred.
3467.7 --> 3468.8: Looking at the TTPs.

3469.7 --> 3471.3: Mapping that to the actual controls.
3471.7 --> 3473.2: And then policy makers use that.
3473.5 --> 3474.8: In for them prioritizing.
3475.6 --> 3477.6: Which controls that they want to consider implementin
g.
3477.9 --> 3479.2: In a rules-based way.
3479.4 --> 3481.4: If they want to do rules-based requirements.
3481.6 --> 3482.4: In their regulations.
3483.1 --> 3484.8: Or in a risk-based approach.
3485.4 --> 3487.6: Risk means needing to understand the threat picture.
3487.7 --> 3488.8: Threat is like the first component.
3489.0 --> 3490.6: Of a risk equation.
3492.2 --> 3493.4: Is understanding that.
3493.8 --> 3495.2: And then the mitigations.
3495.2 --> 3496.2: Also that are in place.
3496.4 --> 3497.0: But I feel like.
3498.2 --> 3499.9: Those layers of understanding.
3500.8 --> 3502.1: So the threat picture.
3502.3 --> 3503.8: Which we know that there's tons of threat firms.
3504.3 --> 3505.8: To what extent that there is.
3506.6 --> 3507.9: I'm sure that Fireblocks.
3508.0 --> 3509.8: Or one of the cyber firms.
3509.8 --> 3510.7: Is probably looking at.
3511.1 --> 3512.8: It would be interesting for them to help.
3512.9 --> 3515.4: Overlay on top of MITRE's ADAPT framework.
3516.2 --> 3517.2: How common.
3517.6 --> 3519.2: Which things are red, yellow, green.
3519.3 --> 3521.1: On the level of commonality.
3521.3 --> 3523.2: That those attacks are occurring in.
3524.3 --> 3525.2: I realize that frequency.
3525.4 --> 3527.3: Is not the only component of threat.
3527.4 --> 3529.9: But at least that kind of archetype.
3530.1 --> 3531.2: For then each institution.
3531.5 --> 3533.0: To apply it to their unique implementation.
3533.8 --> 3535.1: Then if you get the controls.
3535.3 --> 3537.4: Then that gives the north star.
3537.5 --> 3538.8: To the developers and the engineers.
3538.8 --> 3540.0: That Sam was talking about.
3541.2 --> 3542.4: And to policy makers.
3542.4 --> 3544.0: On what to be looking for.
3544.3 --> 3545.1: In their supervision.
3545.9 --> 3548.0: I think it really points to.
3548.3 --> 3549.9: Each of those pieces.
3550.5 --> 3551.9: And then based on each of those use cases.
3552.2 --> 3553.4: For information sharing.
3553.8 --> 3556.3: We just think about the specific use case.
3556.6 --> 3557.8: Of is the information sharing.

3557.9 --> 3559.7: For the purpose of asset recovery.
3559.8 --> 3561.3: For the purpose of alert everybody.
3561.3 --> 3562.9: That there's a critical vulnerability.
3564.0 --> 3566.3: Which means if there's a critical vulnerability.
3566.4 --> 3567.2: Then we start with the TTP.
3567.8 --> 3569.3: But then we have to map that.
3569.3 --> 3570.7: To the specific vulnerability.
3570.7 --> 3572.3: That was exploited via the TTP.
3572.6 --> 3574.5: And then with the fixes to that vulnerability.
3575.7 --> 3577.0: Do we feel like.
3577.3 --> 3579.1: I guess maybe that's an interesting question.
3579.2 --> 3581.5: For begin on how much additional work.
3581.7 --> 3582.4: Needs to happen.
3583.1 --> 3584.6: Probably not above on the threat picture.
3584.8 --> 3586.3: I feel like that probably sits somewhere else.
3586.3 --> 3588.2: In the ecosystem with the threat firms.
3588.7 --> 3590.7: But underneath something like adapt.
3590.9 --> 3593.3: On mapping to specific vulnerabilities.
3593.8 --> 3594.3: And controls.
3595.1 --> 3596.3: Is that a place that we want to be?
3596.3 --> 3598.1: Is that a place that plenty of other organizations.
3598.1 --> 3599.1: Already exist at.
3599.4 --> 3600.4: So we don't really need it.
3600.9 --> 3603.6: I don't know is that a good area of work.
3603.7 --> 3605.4: To build on what's here.
3607.0 --> 3608.4: If you take a look at it right now.
3608.5 --> 3610.1: I just clicked one of the mitigation.
3610.7 --> 3611.2: As you can see.
3611.4 --> 3613.0: We actually help the community.
3613.6 --> 3615.8: By mapping it to the actual attack techniques.
3615.9 --> 3617.3: That will actually mitigate it.
3617.7 --> 3618.8: So that will help everybody out.
3618.9 --> 3621.1: And then we try to go as low as possible.
3621.7 --> 3623.5: To kind of help different type of users.
3623.5 --> 3625.8: So now if you look at the like defend itself.
3625.9 --> 3627.7: It will actually help communicate.
3627.7 --> 3629.8: From different levels of users.
3630.2 --> 3630.9: And people.
3631.4 --> 3633.4: And then now it's also both actionable.
3633.7 --> 3635.2: So we try to kind of help as much as possible.
3635.4 --> 3635.7: The community.
3638.0 --> 3638.8: I'm so sorry.
3640.1 --> 3640.9: It's quite funny.
3641.4 --> 3642.6: I was leading.
3642.9 --> 3643.8: Going to lead with a joke.
3643.8 --> 3646.8: We should call our defend AI agent metapod.
3647.2 --> 3648.2: Because it casts harden.

3651.6 --> 3652.1: Okay.
3653.3 --> 3654.9: A couple things that I've been thinking about.
3655.1 --> 3655.8: While everyone's been talking.
3656.1 --> 3657.7: And the discussion has been really, really good.
3658.1 --> 3661.2: Based on a lot of the research around knowledge graphs.
3661.3 --> 3662.0: That I've been doing.
3663.4 --> 3665.2: It's pretty well known.
3665.4 --> 3667.8: That what gives weight to the words.
3667.8 --> 3669.4: Is actually the edges.
3669.8 --> 3670.9: Not the nodes.
3671.0 --> 3673.1: Or the vertices of the information.
3673.7 --> 3675.6: So the nodes and the vertices of the information.
3675.6 --> 3676.4: Is the context.
3676.6 --> 3677.7: But what gives weight.
3677.7 --> 3679.2: Is the edges.
3679.4 --> 3681.0: That's why my first question was.
3681.2 --> 3682.0: Are the edges defined?
3682.6 --> 3685.5: And I think that's actually also the lowest common denominator.
3685.6 --> 3686.9: That we could work on.
3687.1 --> 3689.9: Is defining the edges of the common graph.
3690.1 --> 3691.1: That we're all going to share.
3691.8 --> 3693.2: And that is literally.
3693.6 --> 3695.3: Often six terms.
3696.0 --> 3697.4: Depending on context.
3698.2 --> 3699.9: And the edge could be.
3700.1 --> 3701.2: The use case as well.
3701.5 --> 3704.3: Where this defines this.
3704.7 --> 3705.9: This attacks this.
3705.9 --> 3707.2: This defends this.
3707.7 --> 3708.2: For example.
3708.4 --> 3711.6: And then once we've defined the edges.
3711.8 --> 3712.9: It doesn't really matter.
3713.0 --> 3714.5: What people put in the nodes.
3715.6 --> 3717.2: The graphs will overlap.
3718.7 --> 3720.3: And magic happens.
3721.1 --> 3723.1: So let's think about the edges.
3723.4 --> 3724.2: And the other way.
3724.3 --> 3725.5: That you add weight to words.
3726.1 --> 3729.5: Is the discrete information path.
3729.7 --> 3730.6: And how you do that.
3730.7 --> 3731.8: Is you build a codex.
3732.1 --> 3733.4: Or a pirate language.
3733.4 --> 3735.4: A secret language among you.
3735.6 --> 3737.6: And that's kind of like what a standard is.
3737.7 --> 3740.2: It is like a secret language.

3740.7 --> 3742.8: But within that secret language.
3743.0 --> 3744.6: You can actually create another layer.
3744.9 --> 3747.2: Where within this ecosystem.
3747.2 --> 3748.3: For example crypto.
3749.0 --> 3750.8: We use attack.
3750.8 --> 3752.0: And defend terms.
3752.1 --> 3752.7: And terminology.
3753.6 --> 3755.3: But we then.
3755.8 --> 3756.8: Because we're expanding.
3757.2 --> 3758.9: And need to add an abstraction layer.
3759.2 --> 3761.7: Which I thought was like a brilliant point.
3761.7 --> 3764.4: The larger the industry gets.
3764.6 --> 3766.5: The more abstraction needs to happen.
3767.1 --> 3769.7: You get these like subset codexes.
3770.3 --> 3773.6: Of this is what this word means.
3773.8 --> 3776.7: In the crypto specific context.
3776.7 --> 3777.3: For example.
3778.1 --> 3781.2: And then anyone within that ecosystem.
3781.4 --> 3782.0: And community.
3782.4 --> 3783.8: Has their own abstraction layer.
3783.8 --> 3785.1: To this abstraction layer.
3785.3 --> 3787.9: Which then adds that discrete weight.
3788.8 --> 3790.2: To the words.
3790.7 --> 3791.7: And we can compress the words.
3791.7 --> 3793.1: As much as possible that way.
3794.1 --> 3795.3: And yeah.
3795.4 --> 3796.9: I think that they were the points.
3797.2 --> 3799.1: That I wanted to bring up.
3805.4 --> 3806.9: A question I have.
3807.9 --> 3808.8: Well a couple.
3809.9 --> 3811.0: One is generally.
3811.3 --> 3813.4: Unlike mapping to.
3815.1 --> 3815.6: Vulnerabilities.
3815.9 --> 3816.5: And controls.
3817.0 --> 3818.2: That map to adapt.
3818.2 --> 3819.4: So basically.
3819.8 --> 3821.1: The work that you guys have done.
3821.2 --> 3822.4: With defend and attack.
3822.9 --> 3824.7: But like are you with adapt.
3825.2 --> 3826.6: Working on like another iteration.
3826.9 --> 3828.8: That sort of does what you've done with attack.
3828.9 --> 3830.5: Which is the like the next step down.
3830.6 --> 3832.2: Of like with the TTP.
3833.5 --> 3834.3: Here's like.
3834.7 --> 3836.5: Here's what the controls are.
3836.6 --> 3837.8: That sort of map against that.
3838.0 --> 3840.0: Or is that something that MITRE is working on.

3840.2 --> 3841.9: Are you able or willing to share that.
3842.4 --> 3843.6: If not we could ask.
3843.6 --> 3844.9: Is anybody working on it.
3845.4 --> 3846.6: Seeing this on the line.
3847.3 --> 3849.7: Curious if that or that anybody else is.
3850.0 --> 3851.6: Is that a valuable place to go.
3851.7 --> 3853.6: And then maybe in an even more.
3853.6 --> 3854.8: Tangible near term thing.
3855.2 --> 3856.4: What Sam mentioned of that like.
3856.9 --> 3858.5: We could in a day identify.
3859.3 --> 3860.1: The crypto nine line.
3861.3 --> 3862.8: Now I think that then we'd like.
3863.3 --> 3864.5: There would be some discussions around.
3864.6 --> 3865.6: Specific use case right.
3865.7 --> 3867.1: Like the information that needs to get shared.
3867.3 --> 3869.5: For law enforcement and attribution purposes.
3869.5 --> 3870.3: Is very different.
3870.4 --> 3872.5: Is not necessarily the same information that's needed.
3872.6 --> 3874.1: For a bunch of private investigators.
3874.1 --> 3875.3: In partnership with industry.
3875.4 --> 3877.1: To just go say stop this money.
3877.2 --> 3878.1: Don't let it go anywhere.
3878.2 --> 3878.6: Freeze it.
3878.9 --> 3879.4: Hold it.
3880.2 --> 3881.8: Like so we could map that out.
3881.9 --> 3883.2: But we could do that day.
3883.6 --> 3885.4: Like and I like candidly.
3885.4 --> 3887.8: Like I'm trying to like push.
3888.1 --> 3890.1: Every other fraud information sharing.
3890.2 --> 3891.3: Organization that I'm a part of.
3891.3 --> 3893.4: Trying to push them exactly towards that.
3893.4 --> 3894.9: Because I think that his point is.
3895.2 --> 3896.6: Entirely prescient and right.
3896.7 --> 3898.8: That this could be done literally in a day.
3899.0 --> 3900.5: To at least create V1.
3900.7 --> 3902.5: And then socialize it with industry.
3902.8 --> 3904.0: With government stakeholders.
3904.3 --> 3906.2: On specifically the use cases that are relevant for them.
3906.5 --> 3907.7: But especially with industry.
3907.8 --> 3909.4: Because we know that most of this information sharing.
3909.6 --> 3911.0: That happens timely and machine readable.
3911.4 --> 3912.3: Is industry.
3912.6 --> 3913.3: It's not government.
3913.5 --> 3914.8: Like there is government.
3914.8 --> 3916.5: Certainly on the hard cyber side.
3917.2 --> 3918.0: Of that but we know.

3918.7 --> 3919.8: You know with the.
3920.5 --> 3922.6: Level of maturity of many governments.
3922.8 --> 3924.7: Like this is going to start.
3924.8 --> 3926.1: With scaling from the industry side.
3926.3 --> 3928.7: Like is begin interested in.
3928.9 --> 3930.3: Do people think that begin should.
3931.0 --> 3932.8: Help be a host or a participant.
3933.1 --> 3934.2: Of this discussion.
3934.6 --> 3935.7: And then what other organizations.
3936.0 --> 3937.0: Do we want to loop in.
3937.4 --> 3939.4: Is that the right next near term thing.
3940.6 --> 3942.6: Like I like the idea of doing that.
3942.6 --> 3944.2: Because it creates a very tangible thing.
3944.3 --> 3946.2: To then go and engage with a lot of.
3946.4 --> 3947.5: Entities across crypto.
3947.7 --> 3948.8: To go like say.
3948.9 --> 3949.7: But so I'm curious.
3949.9 --> 3950.3: Yeah you're right.
3950.3 --> 3951.4: Sorry did you raise your hand.
3951.5 --> 3952.0: Because you want to talk.
3952.7 --> 3953.8: Great we can give it to Japan.
3954.0 --> 3954.6: Crypto ISAC.
3959.5 --> 3961.2: So we are really interested.
3961.4 --> 3962.0: In this information.
3962.6 --> 3963.5: But also because.
3963.7 --> 3965.0: The information is really huge.
3965.0 --> 3966.3: So if begin.
3966.9 --> 3968.4: Helps this information to.
3968.7 --> 3970.2: Crypto ISAC it's helpful for us.
3970.8 --> 3972.1: So because.
3973.1 --> 3974.3: The incident.
3975.2 --> 3975.9: Happens.
3976.2 --> 3977.3: So real time.
3977.7 --> 3979.7: So we would like to know.
3980.1 --> 3982.1: So we cannot gather by ourselves.
3982.4 --> 3984.4: So if begin can help this.
3984.7 --> 3985.7: It's important thing.
3990.2 --> 3992.3: Welcome to this kind of framework.
3992.3 --> 3994.4: Because this is a really well organized.
3994.8 --> 3995.7: So I think it's also.
3996.4 --> 3998.8: This kind of map.
3999.3 --> 4000.5: Should be the API.
4000.8 --> 4001.3: Or other.
4001.8 --> 4004.2: But I think that this is the machine readable.
4004.4 --> 4005.2: And the AI friendly.
4005.5 --> 4007.7: So I think that we can utilize this.
4008.0 --> 4008.8: Framework to the AI.

4010.4 --> 4010.9: Framework.
4012.7 --> 4013.2: Also.
4014.2 --> 4015.2: Connecting the data.
4015.3 --> 4016.8: And the incident is really important.
4017.1 --> 4018.4: Because it's visually.
4019.9 --> 4020.7: Understandable.
4021.3 --> 4022.7: Thank you.
4023.1 --> 4024.7: Coming back to Carol.
4024.9 --> 4025.8: Carol's point.
4026.9 --> 4027.8: I like the idea of.
4028.3 --> 4029.8: Defining achievable.
4030.5 --> 4031.6: Step in.
4033.2 --> 4034.3: Let's say.
4034.7 --> 4036.7: That we can.
4037.2 --> 4038.5: Show as a tangible.
4039.2 --> 4040.2: Achievement in order.
4040.3 --> 4041.6: To bring additional.
4042.3 --> 4043.8: Experts additional stakeholders.
4045.4 --> 4046.6: In the group.
4046.6 --> 4048.1: In order to build the next.
4048.4 --> 4049.5: The first coming steps.
4050.2 --> 4052.8: I like the idea of trying to define.
4053.3 --> 4054.4: Guidelines templates.
4054.6 --> 4055.9: Whatever we name it.
4056.3 --> 4057.6: For kind of emergency.
4059.8 --> 4060.9: Scorecard principle.
4061.2 --> 4062.3: What needs to be shared.
4062.4 --> 4064.3: What are the maybe also the.
4064.8 --> 4066.6: Guidelines on the first.
4066.8 --> 4068.3: Actions depending on the use cases.
4068.5 --> 4069.4: That you should take etc.
4069.6 --> 4070.8: What you should be checked.
4071.2 --> 4072.3: So that at least there is something.
4072.3 --> 4074.3: That can be shared quickly.
4074.6 --> 4076.2: With everyone and probably with.
4076.4 --> 4077.9: Different ways to interpret it.
4078.4 --> 4079.4: With a layer of abstraction.
4079.7 --> 4080.9: Depending on the kind of stakeholders.
4081.2 --> 4082.9: That are involved.
4083.2 --> 4084.8: But I really like the idea.
4086.1 --> 4087.9: And I think it'll be valuable.
4088.1 --> 4088.8: Whether you're doing.
4089.6 --> 4091.0: Manual information sharing.
4091.2 --> 4092.5: Or if you're doing agentic.
4092.5 --> 4093.8: Based information sharing.
4093.9 --> 4094.8: Like these data elements.
4095.2 --> 4097.4: I know I'm continuing this.

4097.4 --> 4098.5: This sales pitch.
4098.7 --> 4099.9: For this particular initiative.
4100.2 --> 4101.3: I think we should do it.
4101.8 --> 4104.4: Adding to that.
4104.9 --> 4107.9: If we have a template.
4108.2 --> 4109.6: Of which information.
4110.1 --> 4111.1: Shall be shared.
4111.7 --> 4112.6: In case of.
4113.1 --> 4114.6: In case of something happened.
4115.2 --> 4116.8: Depending on the different use cases.
4116.9 --> 4118.1: Then we can also ask.
4118.9 --> 4120.6: For the legal entities.
4120.9 --> 4122.4: For instance to define already.
4122.8 --> 4124.1: An emergency process to get.
4124.1 --> 4126.3: Those information sharing approved.
4127.5 --> 4128.1: Quickly.
4128.5 --> 4129.4: In case there is a request.
4129.5 --> 4130.7: Because this is also about.
4131.0 --> 4132.6: Having processes internally ready.
4133.4 --> 4134.5: For such requests.
4135.2 --> 4136.9: When some describe that.
4137.6 --> 4137.8: Well.
4139.8 --> 4140.9: Defining asking.
4141.4 --> 4142.5: What is needed is quick.
4142.6 --> 4144.3: But then getting the approval.
4144.4 --> 4145.6: To get information from.
4146.0 --> 4148.3: Of course I feel the pain.
4148.7 --> 4151.6: It shows that it's going to be.
4151.6 --> 4153.1: To be long if they never.
4153.8 --> 4155.3: Add the case.
4155.4 --> 4156.2: This kind of request.
4156.4 --> 4159.0: If they already thought about internal processes.
4159.2 --> 4160.1: In order to.
4161.2 --> 4162.4: Approve such requests.
4162.5 --> 4163.4: Then it's a different story.
4163.6 --> 4164.8: We can probably.
4165.6 --> 4167.4: Enter into interesting discussion.
4167.7 --> 4168.7: Once we have defined.
4169.9 --> 4172.3: Content of a request like this.
4176.9 --> 4178.2: I would echo.
4178.2 --> 4180.4: Let's create something.
4181.2 --> 4182.4: For someone else to name.
4183.0 --> 4183.8: After they observe it.
4184.3 --> 4185.7: And then go from there.
4186.4 --> 4188.0: I think that that's been.
4188.4 --> 4189.1: Something that.
4190.1 --> 4192.1: I've realized over recent history.

4192.4 --> 4194.3: That it's easier.
4194.5 --> 4196.3: To socialize or express something.
4196.8 --> 4198.2: In lots and lots and lots.
4198.3 --> 4199.2: Of different ways.
4199.8 --> 4201.8: And for other people to name the thing.
4201.9 --> 4202.4: That you're building.
4202.9 --> 4204.6: Then to try and explain it to everyone.
4204.6 --> 4205.1: Every time.
4206.1 --> 4208.5: If we follow that path here.
4209.1 --> 4210.4: I'm really excited.
4210.8 --> 4212.4: For the first thing that we put on the ground.
4212.6 --> 4214.6: To be this interactive.
4215.2 --> 4216.4: Let's build the simulation.
4216.8 --> 4217.7: First version.
4218.4 --> 4220.1: Have someone observe that.
4220.3 --> 4220.8: And name it.
4221.3 --> 4222.6: And say wow that's really neat.
4223.3 --> 4224.6: With this new name.
4224.8 --> 4225.6: And our perspective.
4226.0 --> 4227.4: Let's do our version of it.
4227.9 --> 4229.3: And then we go from there.
4229.3 --> 4230.0: And we improve.
4235.9 --> 4237.1: I'm so sorry.
4237.2 --> 4239.5: I know it's the NSC mind in me.
4239.6 --> 4242.0: Of how to help achieve that.
4242.1 --> 4243.5: Because it will be such a valuable input.
4243.7 --> 4245.1: Into what you guys are building.
4246.3 --> 4247.2: On identifying.
4247.5 --> 4248.9: These high value data elements.
4249.1 --> 4251.0: Because I'm sure we'll start from thinking about.
4251.1 --> 4252.3: Just what is the information.
4252.8 --> 4254.2: Then getting into breaking out.
4254.2 --> 4255.4: What the specific elements are.
4255.4 --> 4257.0: A lot of those will end up pointing to.
4257.3 --> 4258.3: Long existing standards.
4258.8 --> 4261.1: That exist in Sticks and Taxi or ISO.
4262.2 --> 4263.4: And then also standards that exist.
4263.6 --> 4264.3: On different blockchains.
4264.6 --> 4268.3: It will naturally take form that way.
4269.3 --> 4270.8: Who do we need.
4271.3 --> 4272.4: To invite.
4272.7 --> 4273.3: In that session.
4273.6 --> 4274.7: Who should be involved.
4275.3 --> 4276.9: I was texting GBBC.
4277.2 --> 4278.2: Where are you Sandra.
4278.8 --> 4281.0: I know they're doing stuff on cyber.
4281.1 --> 4283.4: I don't know what they're doing.

4283.4 --> 4285.0: I'm looking forward to asking them.
4286.6 --> 4288.5: If there is anything they're doing.
4288.6 --> 4289.2: Related to this.
4289.4 --> 4291.2: They've got a huge member base.
4291.4 --> 4292.8: That would be really valuable.
4292.9 --> 4293.6: To get input on.
4294.0 --> 4295.6: We definitely know the ISACs.
4296.0 --> 4297.8: The information sharing groups.
4298.1 --> 4301.3: What are the other stakeholders.
4301.8 --> 4302.9: That are not present here.
4303.5 --> 4304.5: I guess mapping.
4304.8 --> 4306.0: The information sharing organizations.
4306.3 --> 4307.4: The standards organizations.
4308.8 --> 4310.4: I assume it's exchanges.
4311.3 --> 4312.4: Some bridges.
4313.1 --> 4313.8: I don't know.
4314.0 --> 4315.4: I think that list.
4316.7 --> 4318.2: Stoking some ideas.
4318.6 --> 4321.4: Who the participants could be.
4321.6 --> 4322.6: For that working session.
4323.4 --> 4325.2: Curious if anybody has thoughts.
4325.5 --> 4326.8: On some really good folks.
4326.9 --> 4328.1: For us to have.
4328.2 --> 4329.1: On a very targeted.
4331.8 --> 4332.5: Workshop.
4332.9 --> 4333.5: Or series.
4333.8 --> 4335.9: Of very pointed workshops.
4336.7 --> 4337.9: My first thought.
4337.9 --> 4340.2: Is split the stakeholders.
4340.5 --> 4341.2: Into two groups.
4341.6 --> 4343.0: Victims and solvers.
4344.5 --> 4345.9: Then we can map.
4346.8 --> 4348.2: The organizations.
4349.2 --> 4350.9: And give them a character.
4351.1 --> 4352.2: Before they join the session.
4353.2 --> 4353.5: In a way.
4353.9 --> 4355.1: Here is your persona.
4355.5 --> 4356.3: For the day.
4357.9 --> 4359.0: They will match the persona.
4359.3 --> 4360.4: Of the organization.
4360.9 --> 4361.6: They are coming to.
4362.1 --> 4363.9: The good thing about that.
4363.9 --> 4365.4: Is that you create this.
4365.8 --> 4367.4: Group duality.
4367.4 --> 4368.2: Within the room.
4368.9 --> 4371.4: Where the victims are all.
4371.7 --> 4372.5: Working together.

4372.7 --> 4374.1: To work out the victims perspective.
4374.3 --> 4375.2: Of this tool.
4375.9 --> 4378.4: The solvers are working together.
4378.6 --> 4379.2: To work out.
4379.4 --> 4380.9: It's like doing blue team.
4380.9 --> 4381.3: Red team.
4381.5 --> 4382.6: You are doing a tabletop exercise.
4382.9 --> 4383.3: I like it.
4384.2 --> 4385.9: I think the first meeting.
4385.9 --> 4386.8: Being a tabletop.
4387.5 --> 4387.9: Is cool.
4388.7 --> 4390.5: You come up with different.
4390.6 --> 4391.1: Archetypes.
4391.4 --> 4395.3: For the participants.
4395.5 --> 4396.0: In the ecosystem.
4396.6 --> 4399.9: The industry participants.
4400.4 --> 4400.7: The victim.
4401.1 --> 4402.5: They are a source of information.
4403.7 --> 4404.4: In most cases.
4404.5 --> 4405.4: We are talking about exchanges.
4405.9 --> 4407.3: The actual person.
4408.7 --> 4409.4: Responders.
4409.7 --> 4411.8: People like Sam.
4411.8 --> 4413.7: Law enforcement.
4414.0 --> 4414.5: Regulators.
4415.2 --> 4416.0: We can walk through that.
4416.1 --> 4418.4: It gets away from people.
4419.2 --> 4420.4: That I sometimes find.
4420.9 --> 4422.6: When you host these sorts of things.
4423.2 --> 4425.7: They put the perspective.
4425.7 --> 4427.2: Of the company they are representing.
4427.5 --> 4428.4: Into the conversation.
4429.1 --> 4431.3: It restricts the information.
4431.5 --> 4432.3: And the knowledge sharing.
4432.9 --> 4433.9: Give them a character.
4434.5 --> 4435.7: Tell them to be that thing.
4436.4 --> 4437.4: More often than not.
4437.4 --> 4438.6: You get the right information.
4438.9 --> 4439.6: In a roundabout way.
4440.2 --> 4442.0: Make DeFi play law enforcement?
4442.3 --> 4442.6: I love it.
4443.2 --> 4446.4: I think that's what you want.
4446.4 --> 4448.1: You want discovery from other perspectives.
4448.6 --> 4450.2: Because we already know the things we know.
4451.0 --> 4451.9: I think that's great.
4452.1 --> 4454.8: I don't know if it can all work in one day.
4454.9 --> 4456.0: Or if it will have to be multiple ones.

4456.0 --> 4457.9: I realize that some of the technical work.
4458.0 --> 4460.2: Of mapping very specific standards.
4460.4 --> 4460.9: To data elements.
4461.4 --> 4462.4: The law enforcement guys.
4462.4 --> 4463.4: To talk about what's useful.
4463.6 --> 4464.6: To go after a guy.
4464.7 --> 4468.1: Who may not be aware of what standards are there.
4468.6 --> 4470.6: I think that tabletop.
4470.8 --> 4472.2: Would be a valuable way.
4472.2 --> 4473.1: To set the stage.
4473.3 --> 4474.7: For more technical standards.
4474.8 --> 4476.0: That feels more like beginning.
4476.6 --> 4479.2: Some work we can bounce back and forth.
4479.4 --> 4481.0: With the security teams.
4481.5 --> 4484.2: You could try crystal intelligence.
4484.8 --> 4486.1: We have worked with them.
4486.7 --> 4487.9: We have worked with them.
4488.2 --> 4490.4: In some of the commonwealth regulators.
4490.6 --> 4494.1: They are helping places like Vanuatu.
4494.4 --> 4494.6: With their supervisors.
4496.2 --> 4498.1: With how to use their tooling.
4498.3 --> 4499.2: The supervision tooling.
4500.2 --> 4501.9: I know crystal intelligence.
4502.1 --> 4505.6: Has some pretty serious skills online.
4505.8 --> 4507.1: Like XMI5.
4507.4 --> 4507.9: CIA.
4508.7 --> 4509.5: A whole group of them.
4509.9 --> 4512.0: I know they also help supervisors.
4513.2 --> 4514.3: Work out.
4514.5 --> 4516.8: How to track down.
4517.5 --> 4518.1: The attackers.
4518.9 --> 4520.5: And also to be part of.
4520.5 --> 4521.1: The response.
4521.2 --> 4524.1: They are very proactive.
4524.5 --> 4525.2: Crystal intelligence.
4538.6 --> 4540.3: What I was thinking.
4540.8 --> 4542.9: While listening to you.
4542.9 --> 4543.8: You guys talking.
4545.1 --> 4546.7: About research.
4547.1 --> 4548.1: The GFSA research.
4548.1 --> 4550.3: I showed it to you all.
4551.1 --> 4551.5: Yesterday.
4558.1 --> 4560.0: We got a lot of perspectives.
4561.0 --> 4561.7: Opinions.
4562.1 --> 4563.2: From you all.
4564.7 --> 4566.2: We realized.
4567.0 --> 4569.2: We have a lot of things to do.

4572.1 --> 4574.4: Looking at the defense.
4574.8 --> 4575.4: Our defense.
4575.4 --> 4576.1: And you know.
4577.6 --> 4579.0: This maps as well.
4580.6 --> 4583.2: I'm a little bit overwhelmed.
4583.6 --> 4584.8: By all of the things.
4585.1 --> 4586.2: I will need to do.
4586.4 --> 4587.8: For this research.
4588.8 --> 4590.6: The contract with Deloitte.
4590.8 --> 4592.5: Will end at the end of next month.
4592.6 --> 4593.5: This month actually.
4593.8 --> 4595.7: I don't think we will have time.
4595.8 --> 4596.6: To do all of them.
4596.9 --> 4598.6: What I am going to do.
4598.7 --> 4599.4: For this research.
4599.4 --> 4600.2: Is going to be.
4602.4 --> 4603.1: Prioritize.
4603.4 --> 4605.5: What we need to do.
4605.7 --> 4606.9: And also summarize.
4607.3 --> 4608.7: All of the points.
4609.4 --> 4610.9: Everybody made yesterday.
4612.8 --> 4614.4: It will be great.
4614.5 --> 4615.5: If there is any.
4616.0 --> 4617.7: Forum or workshop.
4618.3 --> 4619.4: Any place.
4620.4 --> 4622.2: Where we will be able.
4622.3 --> 4623.2: To receive feedback.
4623.6 --> 4624.7: On the research again.
4624.9 --> 4627.3: After we revise the research.
4627.3 --> 4629.5: I don't think.
4629.9 --> 4630.7: We will be able.
4630.9 --> 4632.3: To finish that research.
4632.3 --> 4634.0: By the end of this month.
4634.2 --> 4635.9: Probably I need to do.
4636.5 --> 4638.9: The revision work as well.
4641.3 --> 4642.6: We were looking.
4643.0 --> 4643.5: We were thinking.
4645.1 --> 4646.5: Originally we were thinking.
4646.7 --> 4648.5: Of doing a lot of.
4649.3 --> 4649.4: Hearings.
4651.3 --> 4652.0: To the.
4652.5 --> 4654.2: Crypto asset service providers.
4654.2 --> 4656.1: Crypto exchanges.
4656.5 --> 4657.6: And third party players.
4658.0 --> 4659.0: Wallet providers.
4659.2 --> 4661.1: I think it might be better.
4661.3 --> 4662.5: To have a forum.

4663.3 --> 4665.7: Like what I did.
4668.2 --> 4669.0: I think.
4670.2 --> 4671.6: So that it will be.
4671.8 --> 4672.6: Valuable to you.
4673.1 --> 4674.5: Truly valuable to you.
4674.9 --> 4676.5: All of the stakeholders.
4676.9 --> 4678.3: In this industry.
4679.1 --> 4681.3: I am just.
4682.4 --> 4682.9: Yeah.
4683.2 --> 4684.9: I definitely need to do.
4685.2 --> 4687.2: A lot of things I need to do.
4687.3 --> 4689.1: I was wondering if I could.
4690.0 --> 4691.4: I should actually.
4691.6 --> 4692.8: Spend my time.
4693.3 --> 4694.3: Organizing things.
4694.8 --> 4696.5: During the next week.
4696.6 --> 4697.9: I think I need.
4699.4 --> 4701.3: To spend a lot of time.
4702.2 --> 4703.0: Revising it.
4706.5 --> 4707.5: That's part of.
4707.6 --> 4708.6: What begins trying to create.
4708.6 --> 4709.3: With the chat bot.
4709.6 --> 4710.4: So we'll have a chat bot.
4710.6 --> 4711.4: That is specifically.
4712.6 --> 4715.4: Would be trained on all of this information.
4715.4 --> 4716.6: That's publicly available.
4716.9 --> 4719.1: And then you would just have to put your persona.
4719.3 --> 4720.2: As a regulator in.
4720.6 --> 4722.1: And then you could prompt your way to learning.
4722.7 --> 4724.7: About it within your context.
4725.0 --> 4726.6: So hopefully that will be helpful.
4727.0 --> 4728.4: For that position.
4729.4 --> 4730.1: I'll also say.
4730.8 --> 4732.2: That research was awesome.
4732.7 --> 4734.2: And I know that the research.
4734.2 --> 4736.3: The research train and the expansion pack.
4736.3 --> 4737.8: Because I was on like the panels.
4738.1 --> 4739.8: That JFSA was very generously hosting.
4740.0 --> 4741.6: And we all had ideas.
4741.6 --> 4743.3: Of how to optimize and expand.
4743.6 --> 4744.0: But like.
4746.0 --> 4747.7: The guidance around.
4748.1 --> 4749.4: What security controls are.
4749.5 --> 4751.5: And things is always a living framework and document.
4751.5 --> 4752.9: If you guys publish that tomorrow.
4753.0 --> 4754.8: I think it would already be a massive value.
4754.8 --> 4756.1: Add to industry.

4756.6 --> 4757.6: So I think you like.
4757.9 --> 4759.5: I just encourage you to note.
4759.5 --> 4760.7: That like even though there is like.
4761.0 --> 4761.9: There's so much still.
4762.1 --> 4763.6: That can be done in the space.
4764.3 --> 4765.5: Getting information out.
4765.7 --> 4767.5: And figuring out what will be useful and tangible.
4768.0 --> 4770.3: Now for the next like year.
4770.6 --> 4772.2: Or two years of like.
4772.3 --> 4774.4: And then building out what it is you want to get to.
4775.3 --> 4777.3: I just wanted to reinforce.
4777.7 --> 4778.8: How great.
4779.1 --> 4780.6: That work was that you guys presented.
4780.8 --> 4783.0: I think it'll be super valuable to the industry.
4783.4 --> 4784.6: And to other regulators.
4784.8 --> 4786.0: To be able to understand.
4786.0 --> 4788.5: How they should be thinking about.
4789.1 --> 4790.8: Putting in place very specific.
4790.8 --> 4792.1: Kinds of cyber controls.
4792.7 --> 4794.7: Whether prescriptively in regulation.
4795.4 --> 4796.6: Or in a risk-based way.
4797.0 --> 4799.1: What their examiners should be considering.
4799.3 --> 4799.9: And looking for.
4800.0 --> 4802.2: In the institution's own risk assessments.
4802.6 --> 4804.3: And controls that are in place.
4804.4 --> 4805.3: Either way like.
4805.6 --> 4805.9: I tell you.
4806.0 --> 4808.7: IOSCO and FSB haven't done anything like that.
4808.9 --> 4809.5: Not on cyber.
4810.1 --> 4811.5: I don't even think they've done that.
4811.5 --> 4812.9: I don't know if they've done that in trad5.
4813.1 --> 4814.3: They've definitely not done it in crypto.
4814.5 --> 4816.4: So I think it was incredibly valuable.
4816.7 --> 4818.4: And I'm looking forward to that coming out.
4818.5 --> 4819.1: In a public way.
4819.2 --> 4819.9: It was really great.
4821.6 --> 4822.4: Based on that.
4822.6 --> 4823.5: Like one of the other things.
4823.6 --> 4825.2: So besides the high value data elements.
4825.5 --> 4827.0: I think is super useful.
4827.2 --> 4827.7: And necessary.
4828.0 --> 4828.2: And like.
4828.3 --> 4829.0: And I agree with Sam.
4829.1 --> 4830.6: That I think it can be like identified.
4830.6 --> 4832.8: Like very very speedily.
4833.8 --> 4835.1: That will also highlight.
4835.3 --> 4836.1: Like I could imagine.

4836.1 --> 4837.8: That one of the high value data elements.
4837.9 --> 4838.6: That people would point to.
4838.7 --> 4839.5: Is saying the vulnerability.
4839.7 --> 4840.7: Like that you'd want to share.
4840.8 --> 4842.5: Like we have that in Stix and Taxi.
4843.5 --> 4844.5: I don't think.
4844.8 --> 4845.4: Like we have.
4845.5 --> 4847.7: Like there isn't a common taxonomy yet.
4847.7 --> 4849.5: That I'm aware of necessarily.
4849.6 --> 4851.2: On vulnerabilities.
4851.2 --> 4853.7: Like on what crypto CVEs are.
4853.7 --> 4854.2: Right?
4854.5 --> 4857.1: Like whatever the CVE equivalent is for crypto.
4857.7 --> 4858.9: Like it's kind of this middle ground.
4859.0 --> 4860.4: But also tell me if I'm wrong.
4860.5 --> 4861.6: I really want like.
4861.9 --> 4862.6: I'm looking at MITRE.
4862.7 --> 4864.4: Because you guys help administer the NVD.
4864.7 --> 4866.7: But the National Vulnerability Database.
4867.1 --> 4869.8: Like I know that some of the additional.
4870.3 --> 4873.1: Like longer term standards work.
4873.1 --> 4875.3: Is going to have to involve something like.
4877.0 --> 4878.0: Getting into.
4878.2 --> 4879.9: The like mapping of vulnerabilities.
4879.9 --> 4881.0: And then controls.
4881.0 --> 4883.4: The controls especially are going to point to.
4883.5 --> 4885.3: A lot of the exact same stuff.
4885.4 --> 4886.8: That already we have standards for.
4887.2 --> 4887.8: Which is going to be great.
4887.9 --> 4889.2: I think you'll get an answer for that.
4889.3 --> 4891.6: In like 60, 70 percent of the instances.
4892.2 --> 4894.7: And then it will very explicitly help to identify.
4894.9 --> 4897.1: Ah here's the 30 to 40 percent bespoke.
4897.4 --> 4899.1: You know issues that are unique.
4899.2 --> 4900.0: Because crypto.
4900.4 --> 4901.9: It just has some things about it.
4902.0 --> 4902.5: That are special.
4903.7 --> 4905.4: And maybe that percentage is totally off.
4906.0 --> 4908.3: But like I am curious.
4908.3 --> 4909.8: Like is there.
4910.1 --> 4912.1: Is there work that we think.
4912.4 --> 4914.4: That the people that manage the NVD.
4914.7 --> 4916.3: Should be doing on adapting the NVD.
4916.4 --> 4918.1: To include crypto vulnerabilities.
4918.1 --> 4919.5: And CVEs or.
4919.9 --> 4921.3: I don't know if that's something.
4921.6 --> 4923.6: That NIST and MITRE are thinking about.

4923.6 --> 4924.8: If that's something that instead.
4924.9 --> 4926.6: Another organization should be thinking on.
4927.1 --> 4928.6: I'm not saying it needs to be.
4928.6 --> 4929.9: Like prioritized nearest term.
4930.0 --> 4931.7: I still feel that the high value data elements.
4931.7 --> 4932.4: For info sharing.
4932.4 --> 4934.4: Is like a very near term.
4934.6 --> 4936.1: 25 meter target that we could hit.
4936.8 --> 4938.3: But on a road map.
4938.4 --> 4939.9: That some organization.
4940.5 --> 4942.2: Could be mapping that.
4942.3 --> 4943.7: And that it's going to be necessary.
4944.1 --> 4945.4: Because the vulnerability.
4945.8 --> 4947.3: And then controls is where.
4947.7 --> 4949.9: Like that's going to be what's useful to regulators.
4950.1 --> 4951.4: That's going to be what's useful to.
4951.8 --> 4953.5: Security developers and engineers.
4954.4 --> 4955.5: To what extent.
4956.1 --> 4957.9: Is there work being done on that.
4958.5 --> 4960.6: Like and I guess we've already mapped some of it.
4960.6 --> 4961.9: Like we know that there's a lot of controls.
4962.1 --> 4963.2: That like CCSS has mapped.
4963.7 --> 4965.1: Some of the work that Begin has done.
4965.2 --> 4967.0: But on like creating that like.
4967.4 --> 4968.8: Common repository of like NVD.
4969.0 --> 4971.5: I have no idea if MITRE is thinking about that.
4971.6 --> 4972.5: Or with NIST.
4972.5 --> 4973.0: I don't know.
4973.6 --> 4975.9: Is that something that's on the docket.
4976.3 --> 4977.0: For y'all.
4977.6 --> 4978.5: I'll go find out.
4978.6 --> 4979.6: Because MITRE is pretty big.
4980.2 --> 4981.4: We do like a lot of things.
4982.1 --> 4983.1: But to answer.
4983.1 --> 4985.0: Because I think Tatsuya-san.
4985.2 --> 4986.5: You kind of asked the panel this.
4987.1 --> 4987.7: So one of the things.
4988.0 --> 4989.3: That's why when I mentioned DEFEND.
4989.7 --> 4992.2: Because I know from understanding.
4992.4 --> 4994.3: Your research is trying to map to MITRE ATT&CK.
4994.6 --> 4996.3: So a lot of this stuff.
4996.5 --> 4997.7: We already kind of mapped for you.
4998.1 --> 4999.7: So once you identify a MITRE ATT&CK.
4999.8 --> 5002.4: It will actually map to a DEFEND.
5002.6 --> 5003.2: Or a control.
5003.9 --> 5004.8: And then this may be something.
5005.1 --> 5006.3: For the group to think about.

5006.6 --> 5010.2: From a crypto perspective.
5010.2 --> 5011.3: You may.
5011.8 --> 5012.8: If the goal.
5013.2 --> 5015.2: If one of the activities is to create ATT&CK flows.
5015.7 --> 5017.7: That can be shared around the group.
5018.3 --> 5019.9: Maybe finding a common tool.
5020.0 --> 5020.8: To kind of similar.
5021.5 --> 5023.6: To the examples we did over here.
5023.8 --> 5024.4: For IOT.
5025.1 --> 5026.8: So in the IOT.
5030.0 --> 5032.0: If somebody wants to create.
5032.5 --> 5033.4: ATT&CK flows.
5033.6 --> 5034.6: They can actually create.
5034.8 --> 5037.9: And then upload like a library of cryptos.
5037.9 --> 5040.0: In terms of ATT&CK flows.
5040.1 --> 5040.6: Mitigation.
5041.6 --> 5042.4: And so on like that.
5043.2 --> 5045.0: And that may help the group.
5045.7 --> 5046.9: Let me just go there.
5047.1 --> 5049.1: And that may help the group.
5049.7 --> 5052.1: From a community perspective.
5053.6 --> 5053.7: So.
5054.3 --> 5056.6: Having a database on that.
5060.1 --> 5060.7: Yeah.
5060.8 --> 5061.1: Thank you.
5061.2 --> 5062.3: So a little turn.
5062.4 --> 5065.0: But first I'm glad you have a lot of work to do.
5065.0 --> 5065.3: Not me.
5067.5 --> 5068.8: So if we look at.
5068.9 --> 5069.5: What made.
5070.5 --> 5072.8: The successful information sharing.
5073.0 --> 5074.2: Ecosystem successful.
5075.2 --> 5076.9: It was less about technology.
5077.3 --> 5078.4: And more about.
5078.9 --> 5080.3: Economics and law.
5083.4 --> 5084.6: Because we knew.
5085.2 --> 5086.8: We needed electronic.
5087.5 --> 5089.4: Distribution of cyber threats.
5090.0 --> 5090.7: About five years.
5090.7 --> 5092.3: Before anyone actually did it.
5092.9 --> 5093.9: And it was often.
5094.1 --> 5095.8: Because the lawyers kept saying no.
5096.6 --> 5097.6: So is begin.
5098.1 --> 5099.2: A good venue.
5099.3 --> 5100.8: Because you said the magic words.
5101.0 --> 5102.6: You know maybe you need some more workshops.
5102.8 --> 5103.7: But I'm wondering if it's.

5104.5 --> 5106.4: If it would be worthwhile to convene.
5106.7 --> 5107.7: Workshops with.
5108.6 --> 5109.9: Both the legal people.
5110.1 --> 5112.0: So they have like a standard contract.
5112.4 --> 5114.7: Because frankly no matter how much we hide.
5115.8 --> 5117.3: They're putting stuff in the lawyers.
5117.4 --> 5118.8: Will tell them you're not allowed to touch it.
5119.9 --> 5121.1: However if we can.
5121.2 --> 5122.9: Educate the lawyers and say hey look.
5123.0 --> 5125.0: No really we're not just doing the typical.
5125.4 --> 5126.8: ISAC model.
5127.0 --> 5129.1: Which is we promise not.
5129.8 --> 5130.5: To spill.
5131.4 --> 5132.7: Who gave us the data.
5132.9 --> 5134.0: Except for when we're hacked.
5135.1 --> 5136.6: We can say you know.
5137.5 --> 5138.0: Mathematically.
5138.8 --> 5140.9: We're going to obfuscate.
5141.8 --> 5142.8: You know your data is.
5143.0 --> 5144.6: Actually mathematically safe with us.
5145.5 --> 5146.5: You know is there value.
5146.5 --> 5147.5: In doing that.
5147.7 --> 5150.0: Is there value in working out the economics.
5150.2 --> 5151.3: So that Sam goes.
5151.9 --> 5152.8: Oh yeah the return on.
5152.9 --> 5154.6: It's a positive return on investment.
5154.8 --> 5155.7: Yes I got to spend.
5156.8 --> 5157.9: 20 minutes.
5158.7 --> 5160.6: Entering in the latest thing we solved.
5160.8 --> 5163.3: But that's going to save me hours on the next one.
5164.0 --> 5164.7: You know is it worth.
5165.2 --> 5166.5: This group doing that.
5166.6 --> 5167.7: Should somebody else do it.
5167.8 --> 5168.8: Is anyone doing it.
5169.9 --> 5171.3: Just kind of tossing it out there.
5171.3 --> 5173.3: Are there next steps for us.
5180.1 --> 5181.5: So from my.
5182.3 --> 5183.6: Point of view.
5184.1 --> 5185.8: Based on my experiences.
5186.5 --> 5187.1: As an operator.
5187.5 --> 5189.4: As you know.
5189.8 --> 5191.5: Responsible person of the organization.
5192.2 --> 5193.4: Operations begin.
5194.1 --> 5194.9: I feel like.
5195.2 --> 5196.4: There are a lot of.
5197.3 --> 5198.8: Cyber security related projects.
5198.8 --> 5200.3: Begin already right.

5200.4 --> 5202.2: So maybe like.
5202.8 --> 5204.5: If we're going to add more projects.
5205.1 --> 5206.0: Where you know.
5206.2 --> 5208.4: Begin people needs to actually work on.
5209.1 --> 5210.2: Like doing.
5211.0 --> 5211.9: Like you know.
5212.0 --> 5213.9: Writing standards or like.
5214.5 --> 5216.8: Doing all of the mapping like this.
5217.2 --> 5218.3: Probably it would be.
5218.8 --> 5220.8: Very a lot of burden.
5221.0 --> 5222.6: To begin again.
5223.2 --> 5224.7: But maybe like.
5224.9 --> 5225.4: Let's say.
5225.4 --> 5227.3: Like if it's a.
5228.1 --> 5229.6: For example wants to do.
5229.9 --> 5231.7: Are working on the research already.
5232.4 --> 5233.4: And you know if you know.
5233.7 --> 5235.6: We will be able to receive feedbacks like.
5235.9 --> 5237.5: You know from these stakeholders.
5238.0 --> 5239.2: Right like you all.
5239.7 --> 5241.7: And we will get all of the.
5242.1 --> 5244.0: Opinions and you know revise.
5244.1 --> 5245.5: Themselves ourselves right.
5246.0 --> 5247.0: So that kind of.
5248.0 --> 5249.5: That would be probably.
5250.3 --> 5251.7: Not a lot of burden.
5251.9 --> 5253.6: To begin and also.
5253.6 --> 5255.8: That's very very.
5255.9 --> 5257.0: Beneficial to GFSA.
5257.4 --> 5259.3: So that types of like forums.
5259.3 --> 5260.9: Or workshop might be very.
5261.2 --> 5262.9: You know like.
5263.1 --> 5264.7: Beneficial for it.
5264.9 --> 5266.0: Begin participants.
5266.5 --> 5268.5: So I don't know if I could.
5268.6 --> 5270.3: I answered your questions but.
5276.5 --> 5278.2: I think one benefit.
5278.7 --> 5280.5: Of this path that we're.
5280.5 --> 5282.1: Discussing right now.
5282.2 --> 5283.7: And I'm glad that this.
5284.1 --> 5285.6: Is on the screen.
5286.3 --> 5287.7: Is and it gets to.
5288.0 --> 5289.4: Yeah I'm the guy in the group.
5289.6 --> 5290.7: That always talks about graphs.
5291.0 --> 5292.5: I'm sorry I've become that person.
5293.7 --> 5295.4: It's a recent thing.
5295.5 --> 5296.7: But I'm not stopping.

5297.2 --> 5299.0: If we do get to a point.
5299.0 --> 5301.0: Where we define these edges.
5301.1 --> 5302.1: On the graph.
5302.5 --> 5304.0: And then we host a workshop.
5304.0 --> 5305.5: With lawyers and then we host.
5305.5 --> 5306.3: A different workshop.
5306.7 --> 5307.9: With crypto ISAC people.
5308.1 --> 5309.3: And then we host a different workshop.
5309.7 --> 5312.1: With insert stakeholder community here.
5312.8 --> 5313.9: The workshop transcript.
5314.3 --> 5316.2: Is what creates these nodes.
5316.4 --> 5317.2: These boxes.
5318.4 --> 5320.7: But the lines are defined.
5321.5 --> 5322.3: So an AI.
5322.4 --> 5324.4: Is going to very easily map the lines.
5324.7 --> 5325.6: Which means that.
5326.3 --> 5328.1: The result of that workshop.
5328.6 --> 5329.8: Is something like this.
5330.1 --> 5332.3: With this perspective of like legal.
5332.3 --> 5334.2: And if.
5335.1 --> 5336.3: What emerges from that is.
5336.6 --> 5337.9: Oh my god we need a new edge.
5338.8 --> 5339.9: Then that's really really.
5340.2 --> 5341.1: Like that's the outcome.
5341.3 --> 5343.4: Because you're expanding the potential.
5344.7 --> 5346.2: Of the graph.
5346.3 --> 5347.2: To cover more meaning.
5347.8 --> 5348.8: Like what I was saying before.
5349.0 --> 5351.0: Where the weight of the meaning.
5351.2 --> 5353.6: Is actually in what defines the relationship.
5353.6 --> 5355.2: Between the nodes rather than.
5355.5 --> 5357.4: What the information is within the nodes.
5358.5 --> 5360.5: So yeah and similarly.
5360.5 --> 5362.1: With the tools that we have today.
5362.9 --> 5364.5: The hard part is getting everyone.
5364.6 --> 5365.4: In the room for the workshop.
5365.6 --> 5367.4: The easy part is converting the transcript.
5367.9 --> 5370.6: Into a structured system.
5370.8 --> 5372.8: And model that then just prints it out.
5372.9 --> 5374.1: And sends it the day after.
5374.3 --> 5376.7: And hosts the web page with this website.
5376.8 --> 5378.2: As per the legal.
5378.9 --> 5380.5: Understanding of this particular.
5381.1 --> 5382.4: Thing that we were analyzing.
5385.3 --> 5386.1: Two things.
5386.5 --> 5387.6: Eric to your.
5388.3 --> 5389.1: Question whether.

5389.4 --> 5390.7: Begin is the right place to.
5391.6 --> 5393.2: Do something specific.
5393.6 --> 5395.0: And in particular respect to the topics.
5395.2 --> 5396.7: That we discuss this is where I like.
5397.5 --> 5398.6: Quick action quick win.
5399.0 --> 5399.8: Even if it's slow.
5400.3 --> 5403.3: It could be a way to validate.
5403.8 --> 5405.3: That we are going into the right direction.
5405.4 --> 5406.1: So the quick.
5408.1 --> 5409.1: Establishment definition.
5409.7 --> 5411.2: Of the cheat sheet.
5411.4 --> 5413.4: For information.
5413.7 --> 5414.9: Sharing I think it's a way.
5414.9 --> 5416.6: To kind of validate.
5416.8 --> 5417.6: That there is an interest.
5417.9 --> 5420.7: And that we might be the right forum.
5420.8 --> 5421.2: To do so.
5423.2 --> 5424.8: We need to be careful not to launch.
5425.0 --> 5426.7: Long-term action without really knowing.
5426.8 --> 5427.9: Whether we will have.
5428.5 --> 5430.3: Some impact or whether we are really.
5430.5 --> 5431.3: Legitimate to do so.
5432.7 --> 5434.3: I'm just conscious of the time.
5435.0 --> 5436.4: Normally we have only five minutes.
5436.4 --> 5439.0: Left we.
5439.2 --> 5440.2: For those online.
5440.8 --> 5442.9: We talk a lot in person.
5442.9 --> 5445.0: In the room is there anyone online.
5445.2 --> 5446.7: Willing to say something to contribute.
5446.9 --> 5448.8: To give some thoughts to say that.
5448.9 --> 5450.8: We are going completely wrong.
5451.1 --> 5452.3: With what we just discussed.
5460.5 --> 5460.9: Silence.
5463.9 --> 5464.3: Katya.
5464.5 --> 5466.7: Any thoughts from the NIST side.
5466.8 --> 5469.5: I'm sorry to put you on the spot.
5469.5 --> 5470.6: It was just curious on the.
5470.6 --> 5473.0: The focus on some of the specific.
5473.2 --> 5475.4: Data elements or standards work here.
5475.7 --> 5478.5: Where there is gaps on efforts.
5478.6 --> 5479.9: Just curious if you have any thoughts.
5480.4 --> 5481.4: Especially on.
5482.8 --> 5484.1: What we have been covering.
5484.9 --> 5486.2: I think this has been a really.
5486.6 --> 5487.9: Interesting and helpful conversation.
5488.6 --> 5490.3: We have certainly been trying to scope.
5490.6 --> 5492.3: And get an understanding of where the gaps are.

5492.9 --> 5494.0: In the ecosystem.
5494.3 --> 5495.7: As far as security is concerned.
5496.0 --> 5497.8: Having this conversation with this group.
5497.8 --> 5498.7: Has been really insightful.
5501.2 --> 5502.7: I can say.
5502.8 --> 5503.7: To your earlier question.
5503.9 --> 5504.3: We have not.
5504.9 --> 5506.7: Just in high-level conversations.
5508.3 --> 5509.7: Maybe two or three years ago.
5509.7 --> 5510.5: We talked about.
5511.9 --> 5513.5: Just as a research project.
5513.5 --> 5514.7: Updating the CVEs.
5516.7 --> 5517.8: As you know.
5518.1 --> 5518.7: Our staff.
5519.8 --> 5522.8: Has been kind of redirected.
5522.9 --> 5523.6: Or gone.
5524.3 --> 5524.7: What do you mean?
5524.7 --> 5526.7: Resourcing has been super consistent.
5526.7 --> 5529.0: On the U.S. side right now.
5529.3 --> 5529.5: Right.
5529.9 --> 5532.6: I think all of this sounds like.
5532.7 --> 5534.0: It is heading in the right direction.
5534.4 --> 5536.2: I am keenly aware.
5537.3 --> 5538.5: Not aware.
5539.6 --> 5540.6: The issue.
5540.8 --> 5542.2: The legal challenges have been raised.
5542.3 --> 5542.9: Again and again.
5544.2 --> 5545.8: I agree with Julian.
5546.1 --> 5548.3: At least the quick wins.
5548.5 --> 5549.8: Might be worth pursuing.
5550.9 --> 5551.7: Early on.
5553.7 --> 5554.8: We expect.
5554.8 --> 5556.4: To be hosting a workshop.
5557.1 --> 5558.3: April 16.
5558.6 --> 5560.5: Maybe that will be a forum.
5560.7 --> 5563.7: To discuss ways to motivate.
5564.6 --> 5565.9: The information sharing.
5566.2 --> 5566.7: In a way.
5567.2 --> 5567.9: That sort of.
5568.7 --> 5569.9: Might have.
5571.5 --> 5572.9: A bit more.
5573.4 --> 5573.9: What is the word?
5574.3 --> 5575.3: Heft to it.
5576.7 --> 5577.3: I like it.
5578.4 --> 5579.2: Thank you.
5579.4 --> 5582.4: I am sorry.
5582.4 --> 5583.1: Did I cut you off?

5583.9 --> 5584.0: No.
5584.2 --> 5585.0: Thank you.
5585.1 --> 5587.7: Thank you for highlighting that.
5587.8 --> 5589.2: That will be awesome.
5592.4 --> 5593.6: I share Julian's.
5593.8 --> 5593.9: I know.
5595.2 --> 5597.0: I have so many high horses.
5597.2 --> 5597.8: This is one of them.
5598.8 --> 5600.3: I do think on creating.
5600.5 --> 5601.9: At least V1.
5602.2 --> 5603.9: The high value data elements.
5605.0 --> 5606.6: Private sector driven.
5607.2 --> 5608.7: Agreed upon standards.
5608.7 --> 5610.2: That is the kind of stuff.
5610.3 --> 5612.3: Government likes to point to industry.
5612.5 --> 5614.5: They know what standards they use.
5614.8 --> 5616.0: What information is available.
5616.3 --> 5619.0: If industry agrees.
5619.2 --> 5620.0: To use it.
5620.2 --> 5622.4: Government will figure out a way around it.
5623.7 --> 5625.6: There are interesting.
5625.9 --> 5626.7: Government focused applications.
5627.8 --> 5628.3: For that.
5629.3 --> 5630.5: Identifying of high value.
5630.9 --> 5631.5: Data elements.
5632.0 --> 5633.2: Regulators and law enforcement.
5633.3 --> 5633.9: Will have feelings.
5633.9 --> 5636.1: Those are the highest value data elements.
5636.2 --> 5637.3: For some of your use cases.
5638.3 --> 5639.5: I do think.
5639.6 --> 5640.5: Because of how.
5640.7 --> 5642.0: I think it is tangible.
5642.2 --> 5643.1: Within reach.
5643.6 --> 5645.4: This is something that would be good.
5646.1 --> 5648.3: Even if we co-hosted.
5648.8 --> 5650.4: That targeted discussion.
5650.6 --> 5652.2: To create the first version.
5652.8 --> 5654.1: And socialize it publicly.
5654.3 --> 5656.5: Is this the right version?
5657.0 --> 5660.2: Even before the NIST workshop.
5661.1 --> 5661.8: Potentially.
5661.8 --> 5663.6: To feed into some of the other.
5664.0 --> 5665.2: Efforts that are ongoing.
5665.4 --> 5666.4: Fighting fraud.
5667.0 --> 5668.4: To feed into the FATF.
5668.5 --> 5670.2: Virtual asset contact group.
5671.9 --> 5673.8: I think they would be interested.

5674.0 --> 5674.9: In something tangible.
5675.5 --> 5677.6: To allow for debate and discussion.
5677.8 --> 5679.6: On whether that is the right information.
5680.5 --> 5681.1: I will tell you.
5681.4 --> 5682.6: In illicit finance.
5682.7 --> 5684.8: There is not a stick and taxi.
5685.5 --> 5687.8: Which is something I want to exist.
5688.0 --> 5689.0: In illicit finance.
5689.0 --> 5692.0: I would love to start with crypto.
5692.3 --> 5693.0: Because it is all digital.
5693.4 --> 5694.0: Structured information.
5695.6 --> 5698.1: I will take whatever I can get.
5698.2 --> 5699.0: I will try crypto.
5700.0 --> 5701.8: See who hits first.
5702.9 --> 5703.9: With this one.
5704.0 --> 5705.4: Begin would be great.
5705.8 --> 5707.7: Thinking about who the right partners are.
5707.8 --> 5709.5: To come up with that version 1.
5710.1 --> 5711.4: That targeted.
5711.8 --> 5713.0: Tangible workshop.
5713.3 --> 5715.0: Feels beginning to me.
5715.7 --> 5718.1: Because it feeds into the standard.
5718.1 --> 5721.9: It is all around information sharing.
5722.4 --> 5724.8: We did not identify what that information is.
5725.0 --> 5726.7: That should be flowing through.
5727.1 --> 5727.6: That standard.
5727.8 --> 5728.6: Which we don't have to.
5728.9 --> 5730.4: That is not what that standard was focused on.
5730.7 --> 5734.2: This one is the input and output.
5734.5 --> 5735.4: That would be flowing throughout.
5735.7 --> 5737.0: I think this would be good.
5737.5 --> 5739.1: The ones on the policy issues.
5739.3 --> 5741.0: That Eric brought up.
5741.8 --> 5743.0: To Kaya's point.
5743.3 --> 5745.3: What should JFSA and government authorities.
5745.5 --> 5746.3: Be convening.
5747.2 --> 5748.0: First off.
5748.2 --> 5750.9: If we can develop this version 1.
5751.3 --> 5752.6: That would be a great input.
5752.9 --> 5753.9: For you guys to consider.
5754.1 --> 5756.1: Is this useful for your industry?
5756.6 --> 5758.0: For your government use cases?
5758.2 --> 5759.6: Not to mention all the other topics.
5759.7 --> 5760.8: You will want to cover in a workshop.
5761.7 --> 5764.0: To allow government to focus on the areas.
5764.0 --> 5765.7: Where only you can solve it.
5766.2 --> 5768.0: The information sharing agreements.

5768.1 --> 5769.0: The framework.
5769.6 --> 5770.8: All the different things.
5771.0 --> 5774.5: Government is exclusively positioned.
5774.5 --> 5775.4: To be able to solve.
5777.1 --> 5778.1: Liability protections.
5778.4 --> 5778.6: Pilots.
5781.7 --> 5783.6: Where an organization like BEGIN.
5783.7 --> 5785.0: Can focus on this building block.
5785.4 --> 5789.1: One of the most atomic building blocks.
5789.2 --> 5789.5: That is needed.
5790.3 --> 5791.0: For this system.
5791.2 --> 5793.0: What is the most valuable information.
5793.6 --> 5795.0: To flow through this flowchart.
5795.9 --> 5797.8: I think that would be good.
5798.0 --> 5799.0: For BEGIN to focus on.
5799.1 --> 5800.8: It reinforces what we have done otherwise.
5801.1 --> 5802.6: It will feed into the agent.
5802.6 --> 5803.9: It is literally an input.
5804.7 --> 5806.0: When you use a chatbot.
5806.2 --> 5808.2: It will want to think about what is the information.
5808.8 --> 5810.1: It should be transmitting and sending.
5810.3 --> 5811.9: It is an input into something.
5812.0 --> 5813.0: That BEGIN is already building.
5813.9 --> 5815.1: It is part of the standard.
5815.4 --> 5818.4: It is the right thing for BEGIN to do.
5818.9 --> 5820.3: Organizations like JFSA.
5820.8 --> 5821.8: It would be great.
5821.9 --> 5824.4: To focus on the policy framework.
5824.6 --> 5825.5: And governance models.
5826.2 --> 5827.7: Where only you guys.
5828.1 --> 5829.6: And 200 other nations.
5829.6 --> 5830.6: Have to work together.
5831.5 --> 5832.6: Stuff you could raise.
5832.8 --> 5834.6: Even at FSB and FATF.
5841.7 --> 5842.8: Was it a conclusion?
5847.2 --> 5848.4: We are good?
5849.6 --> 5851.0: Thank you for those online.
5851.8 --> 5853.4: We are going to take a break.
5854.8 --> 5856.1: For about one hour.
5856.6 --> 5857.3: Thank you.
5858.5 --> 5859.2: Thank you all.
5859.4 --> 5859.6: Great.
5887.3 --> 5887.7: Thank you.