[{ "text": "open aai released a lengthy blog post", "start": 0.04, "duration": 5.799 }, { "text": "going over their new ideas about AI", "start": 2.84, "duration": 5.36 }, { "text": "Safety and Security and a lot of it has", "start": 5.839, "duration": 4.521 }, { "text": "me scratching my head some of it makes", "start": 8.2, "duration": 4.04 }, { "text": "sense but other parts of it make it", "start": 10.36, "duration": 4.199 }, { "text": "clear that they are going all in on the", "start": 12.24, "duration": 4.6 }, { "text": "Clos sourced architecture and it makes", "start": 14.559, "duration": 5.121 }, { "text": "me really thankful that meta a company", "start": 16.84, "duration": 5.84 }, { "text": "the size of meta is going all in on the", "start": 19.68, "duration": 5.12 }, { "text": "open source model so we're going to look", "start": 22.68, "duration": 3.8 }, { "text": "at this blog post today and I'm going to", "start": 24.8, "duration": 3.16 }, { "text": "share my thoughts and go through it", "start": 26.48, "duration": 3.48 }, { "text": "together with you so let's get into it", "start": 27.96, "duration": 3.88 }, { "text": "so here's the blog post reimagining", "start": 29.96, "duration": 4.279 }, { "text": "secure infrastructure for advanced Ai", "start": 31.84, "duration": 4.52 }, { "text": "and open AI calls for an evolution in", "start": 34.239, "duration": 4.121 }, { "text": "infrastructure security to protect", "start": 36.36, "duration": 4.92 }, { "text": "Advanced AI so here they say we're", "start": 38.36, "duration": 4.76 }, { "text": "sharing six security measures that we", "start": 41.28, "duration": 3.439 }, { "text": "believe will complement the security", "start": 43.12, "duration": 3.959 }, { "text": "controls of today and contribute to the", "start": 44.719, "duration": 4.761 }, { "text": "protection of advanced AI here they talk", "start": 47.079, "duration": 4.761 }, { "text": "about their mission that's fine first", "start": 49.48, "duration": 4.8 }, { "text": "the threat model AI is the most", "start": 51.84, "duration": 4.16 }, { "text": "strategic and sought-after Technology of", "start": 54.28, "duration": 4.2 }, { "text": "our time it is pursued with Vigor by", "start": 56.0, "duration": 4.8 }, { "text": "sophisticated cyber threat factors with", "start": 58.48, "duration": 4.64 }, { "text": "strategic aims and then at open AI we", "start": 60.8, "duration": 4.2 }, { "text": "want to defend against it now", "start": 63.12, "duration": 4.84 }, { "text": "immediately this is where I diverge from", "start": 65.0, "duration": 5.68 }, { "text": "open ai's opinion on Safety and Security", "start": 67.96, "duration": 5.32 }, { "text": "and really the entire approach to AI", "start": 70.68, "duration": 4.759 }, { "text": "protecting model weights is an important", "start": 73.28, "duration": 4.56 }, { "text": "priority for many AI developers model", "start": 75.439, "duration": 4.521 }, { "text": "weights are the output of the model", "start": 77.84, "duration": 4.56 }, { "text": "training process so immediately they are", "start": 79.96, "duration": 5.6 }, { "text": "saying protecting model weights not open", "start": 82.4, "duration": 5.44 }, { "text": "source not open weights so this is", "start": 85.56, "duration": 3.64 }, { "text": "already very different from what I", "start": 87.84, "duration": 3.2 }, { "text": "believe the future future of artificial", "start": 89.2, "duration": 4.08 }, { "text": "intelligence should look like I am a big", "start": 91.04, "duration": 5.399 }, { "text": "proponent of open-source AI but right at", "start": 93.28, "duration": 5.199 }, { "text": "the very top of this blog post they are", "start": 96.439, "duration": 3.801 }, { "text": "already saying they don't believe that", "start": 98.479, "duration": 3.28 }, { "text": "and if you're not familiar with what", "start": 100.24, "duration": 3.0 }, { "text": "model weights are they're actually going", "start": 101.759, "duration": 3.281 }, { "text": "to describe what they are in detail so", "start": 103.24, "duration": 3.4 }, { "text": "I'll get to that in a moment model", "start": 105.04, "duration": 3.359 }, { "text": "training combines three essential", "start": 106.64, "duration": 3.88 }, { "text": "ingredients sophisticated algorithms", "start": 108.399, "duration": 4.36 }, { "text": "curated training data sets and vast", "start": 110.52, "duration": 4.879 }, { "text": "amounts of computing resources now two", "start": 112.759, "duration": 4.68 }, { "text": "of the three of those things are very", "start": 115.399, "duration": 3.561 }, { "text": "difficult to get sophisticated", "start": 117.439, "duration": 4.04 }, { "text": "algorithms everybody pretty much has", "start": 118.96, "duration": 4.32 }, { "text": "these ideas already with these", "start": 121.479, "duration": 4.0 }, { "text": "algorithms there isn't some silver", "start": 123.28, "duration": 3.759 }, { "text": "bullet that we're going to get all of a", "start": 125.479, "duration": 3.64 }, { "text": "sudden that leads us to AGI it's going", "start": 127.039, "duration": 4.441 }, { "text": "to be very incremental as many AI", "start": 129.119, "duration": 4.881 }, { "text": "leaders have said now curated training", "start": 131.48, "duration": 5.08 }, { "text": "data sets for the most part these data", "start": 134.0, "duration": 4.76 }, { "text": "sets are actually publicly available", "start": 136.56, "duration": 3.8 }, { "text": "making them high quality on the other", "start": 138.76, "duration": 3.64 }, { "text": "hand is very difficult having a very", "start": 140.36, "duration": 3.84 }, { "text": "high quality training data set and", "start": 142.4, "duration": 3.88 }, { "text": "especially getting data sets that are", "start": 144.2, "duration": 4.36 }, { "text": "not publicly available are very unique", "start": 146.28, "duration": 3.84 }, { "text": "is actually very difficult and very", "start": 148.56, "duration": 3.759 }, { "text": "expensive that is why Elon Musk shut", "start": 150.12, "duration": 5.6 }, { "text": "down the X API that is why Reddit shut", "start": 152.319, "duration": 6.161 }, { "text": "down their API essentially all of these", "start": 155.72, "duration": 5.879 }, { "text": "companies that have immense data sets", "start": 158.48, "duration": 5.56 }, { "text": "that are not public that are really", "start": 161.599, "duration": 5.161 }, { "text": "owned by these individual companies are", "start": 164.04, "duration": 5.8 }, { "text": "protecting them more and more and last", "start": 166.76, "duration": 5.72 }, { "text": "vast amounts of computing resources this", "start": 169.84, "duration": 5.44 }, { "text": "is the most costly element of the three", "start": 172.48, "duration": 4.8 }, { "text": "ingredients necessary to train a model", "start": 175.28, "duration": 4.56 }, { "text": "now you can train small models and find", "start": 177.28, "duration": 5.44 }, { "text": "fune smaller models on pretty mediocre", "start": 179.84, "duration": 4.479 }, { "text": "Hardware but if you want to train", "start": 182.72, "duration": 4.12 }, { "text": "Frontier models like llama 3 you have to", "start": 184.319, "duration": 4.961 }, { "text": "spend a lot of money getting gpus all", "start": 186.84, "duration": 4.88 }, { "text": "right so what are model weights the", "start": 189.28, "duration": 4.599 }, { "text": "resulting model weights are sequences of", "start": 191.72, "duration": 4.72 }, { "text": "numbers stored in a file or series of", "start": 193.879, "duration": 4.601 }, { "text": "files so basically the model weights are", "start": 196.44, "duration": 4.28 }, { "text": "the output of the training process and", "start": 198.48, "duration": 4.399 }, { "text": "the model weights inform the model on", "start": 200.72, "duration": 4.879 }, { "text": "how to process the prompts essentially", "start": 202.879, "duration": 4.601 }, { "text": "AI developers may wish to protect these", "start": 205.599, "duration": 3.881 }, { "text": "files because they embody the power and", "start": 207.48, "duration": 3.839 }, { "text": "potential of the algorithms training", "start": 209.48, "duration": 3.759 }, { "text": "data and Computing resources that went", "start": 211.319, "duration": 4.161 }, { "text": "into them here they go on to talk about", "start": 213.239, "duration": 4.08 }, { "text": "how large language models are actually", "start": 215.48, "duration": 4.0 }, { "text": "being used and where the utility is", "start": 217.319, "duration": 4.84 }, { "text": "being found and they say from online use", "start": 219.48, "duration": 4.6 }, { "text": "that makes sense in order to power tools", "start": 222.159, "duration": 4.16 }, { "text": "like chat GPT users must be able to send", "start": 224.08, "duration": 5.159 }, { "text": "API requests in order to develop new AI", "start": 226.319, "duration": 4.881 }, { "text": "models model weights must be deployed to", "start": 229.239, "duration": 4.0 }, { "text": "research infrastructure so researchers", "start": 231.2, "duration": 4.48 }, { "text": "can perform model training and they go", "start": 233.239, "duration": 4.2 }, { "text": "on to say while this enables the", "start": 235.68, "duration": 4.36 }, { "text": "exploration of new scientific Frontiers", "start": 237.439, "duration": 4.321 }, { "text": "research infrastructure and credentials", "start": 240.04, "duration": 4.52 }, { "text": "that provide access to it also represent", "start": 241.76, "duration": 5.679 }, { "text": "potential attack surface this is true", "start": 244.56, "duration": 6.56 }, { "text": "now their conclusion from this fact is", "start": 247.439, "duration": 6.121 }, { "text": "something I disagree with they say well", "start": 251.12, "duration": 4.119 }, { "text": "if that's a potential attack surface we", "start": 253.56, "duration": 3.16 }, { "text": "should just shut down the model weights", "start": 255.239, "duration": 3.28 }, { "text": "we should close it up and not allow", "start": 256.72, "duration": 3.759 }, { "text": "other people to get access to it and", "start": 258.519, "duration": 3.361 }, { "text": "obviously I've mentioned it already in", "start": 260.479, "duration": 2.801 }, { "text": "this video and many other videos that", "start": 261.88, "duration": 3.319 }, { "text": "I've made I don't believe that I think", "start": 263.28, "duration": 4.0 }, { "text": "model weight should be freely accessible", "start": 265.199, "duration": 3.881 }, { "text": "and that is the way to harden the", "start": 267.28, "duration": 3.919 }, { "text": "infrastructure model weights are merely", "start": 269.08, "duration": 3.72 }, { "text": "files that must be decrypted and", "start": 271.199, "duration": 3.401 }, { "text": "deployed in order to be used and if the", "start": 272.8, "duration": 3.679 }, { "text": "infrastructure and operations providing", "start": 274.6, "duration": 3.52 }, { "text": "their availability are compromise the", "start": 276.479, "duration": 3.961 }, { "text": "model weights are liable to be stolen", "start": 278.12, "duration": 3.96 }, { "text": "again a big assumption that closed", "start": 280.44, "duration": 3.72 }, { "text": "source is the way to go thanks to the", "start": 282.08, "duration": 5.08 }, { "text": "sponsor of this video Domo AI if you're", "start": 284.16, "duration": 4.64 }, { "text": "ready to take your creativity to the", "start": 287.16, "duration": 4.72 }, { "text": "next level Domo AI is for you it is your", "start": 288.8, "duration": 5.76 }, { "text": "ultimate AI companion for transforming", "start": 291.88, "duration": 5.44 }, { "text": "ordinary content into extraordinary", "start": 294.56, "duration": 5.16 }, { "text": "masterpieces and Domo is more than just", "start": 297.32, "duration":

4.719 }, { "text": "just an AI tool it is your gateway to a", "start": 299.72, "duration": 5.479 }, { "text": "world of endless creativity right from", "start": 302.039, "duration": 5.401 }, { "text": "Discord with Domo AI you can breathe", "start": 305.199, "duration": 4.84 }, { "text": "life into your videos and images turning", "start": 307.44, "duration": 5.36 }, { "text": "them into captivating works of art so", "start": 310.039, "duration": 4.361 }, { "text": "let me just talk about a couple features", "start": 312.8, "duration": 4.16 }, { "text": "that Domo has so if you simply type", "start": 314.4, "duration": 5.32 }, { "text": "slide you can turn your videos into", "start": 316.96, "duration": 5.0 }, { "text": "endless different styles from", "start": 319.72, "duration": 5.36 }, { "text": "mesmerizing anime Aesthetics to vibrant", "start": 321.96, "duration": 6.44 }, { "text": "3D cartoons and so much more then", "start": 325.08, "duration": 5.679 }, { "text": "there's slash MO move so if you've ever", "start": 328.4, "duration": 4.12 }, { "text": "wanted to make one of your characters", "start": 330.759, "duration": 4.481 }, { "text": "dance or jump or walk around and", "start": 332.52, "duration": 4.76 }, { "text": "interact with surroundings this is the", "start": 335.24, "duration": 4.36 }, { "text": "command for you this uses Domo ai's", "start": 337.28, "duration": 4.52 }, { "text": "motion capture technology which will", "start": 339.6, "duration": 4.12 }, { "text": "bring your characters to life like", "start": 341.8, "duration": 4.839 }, { "text": "you've never seen and then they have SLG", "start": 343.72, "duration": 4.52 }, { "text": "which allows you to create stunning", "start": 346.639, "duration": 3.84 }, { "text": "images just from a simple text", "start": 348.24, "duration": 4.28 }, { "text": "description then you can type slash", "start": 350.479, "duration": 4.321 }, { "text": "animate and take those static images or", "start": 352.52, "duration": 4.799 }, { "text": "really any image and bring them to life", "start": 354.8, "duration": 5.6 }, { "text": "in video which will add movement flare", "start": 357.319, "duration": 5.44 }, { "text": "and make it look really awesome Domo AI", "start": 360.4, "duration": 4.4 }, { "text": "has flexible subscription plans so you", "start": 362.759, "duration": 4.201 }, { "text": "can find which one is right for you and", "start": 364.8, "duration": 4.44 }, { "text": "they also have standard and pro plans", "start": 366.96, "duration": 5.16 }, { "text": "which include unlimited credits so check", "start": 369.24, "duration": 5.519 }, { "text": "out Domo AI join the Domo AI server", "start": 372.12, "duration": 5.32 }, { "text": "today and unlock your creativity join", "start": 374.759, "duration": 5.801 }, { "text": "today and get 10% off with Domo AI I'll", "start": 377.44, "duration": 4.879 }, { "text": "drop all of the information in the", "start": 380.56, "duration": 4.079 }, { "text": "description below now back to the video", "start": 382.319, "duration": 4.121 }, { "text": "so here they start to describe their new", "start": 384.639, "duration": 3.881 }, { "text": "thinking about the infrastructure and", "start": 386.44, "duration": 4.52 }, { "text": "how to secure their infastructure and", "start": 388.52, "duration": 4.679 }, { "text": "here's something that looks really nice", "start": 390.96, "duration": 4.239 }, { "text": "on the surface but if you think about it", "start": 393.199, "duration": 3.84 }, { "text": "for more than 2 seconds it's obvious", "start": 395.199, "duration": 3.84 }, { "text": "what they're trying to do our security", "start": 397.039, "duration": 3.88 }, { "text": "program has sought to Manifest this", "start": 399.039, "duration": 3.801 }, { "text": "principle via voluntary security", "start": 400.919, "duration": 4.081 }, { "text": "commitments provided to the White House", "start": 402.84, "duration": 4.04 }, { "text": "now that sounds all well and good", "start": 405.0, "duration": 3.84 }, { "text": "they're voluntarily saying hey this is", "start": 406.88, "duration": 5.24 }, { "text": "what we're going to do to secure our AI", "start": 408.84, "duration": 5.88 }, { "text": "however they are likely also going to be", "start": 412.12, "duration": 5.16 }, { "text": "pushing to make that the standard and", "start": 414.72, "duration": 4.879 }, { "text": "this is also known as regulatory C", "start": 417.28, "duration": 4.759 }, { "text": "capture if their approach is the", "start": 419.599, "duration": 4.961 }, { "text": "standard and then you have to go through", "start": 422.039, "duration": 5.72 }, { "text": "governmental approval to apply to the", "start": 424.56, "duration": 5.639 }, { "text": "standard and to obey the standard then", "start": 427.759, "duration": 5.321 }, { "text": "all of a sudden small companies have a", "start": 430.199, "duration": 5.0 }, { "text": "much bigger hurdle to deploy Cutting", "start": 433.08, "duration": 4.16 }, { "text": "Edge artificial intelligence and that", "start": 435.199, "duration": 5.201 }, { "text": "makes competition much less for open AI", "start": 437.24, "duration": 4.679 }, { "text": "so in the spirit of shared work and", "start": 440.4, "duration": 3.44 }, { "text": "shared responsibility that bonds all", "start": 441.919, "duration": 3.761 }, { "text": "security teams today we are sharing six", "start": 443.84, "duration": 3.68 }, { "text": "security measures for advanced AI", "start": 445.68, "duration": 3.56 }, { "text": "infrastructure that's so nice that", "start": 447.52, "duration": 3.6 }, { "text": "they're sharing the security measures", "start": 449.24, "duration": 3.6 }, { "text": "but not sharing the model weights all", "start": 451.12, "duration": 3.4 }, { "text": "right so here are the six I'm not going", "start": 452.84, "duration": 2.759 }, { "text": "to read them we're going to go through", "start": 454.52, "duration": 4.239 }, { "text": "them one by one in detail first trusted", "start": 455.599, "duration": 6.0 }, { "text": "Computing for AI accelerators emerging", "start": 458.759, "duration": 4.401 }, { "text": "encryption and Hardware security", "start": 461.599, "duration": 3.16 }, { "text": "technology like confidential Computing", "start": 463.16, "duration": 3.52 }, { "text": "offer the promise of protecting model", "start": 464.759, "duration": 4.481 }, { "text": "weights and inference data by extending", "start": 466.68, "duration": 4.6 }, { "text": "trusted Computing Primitives beyond the", "start": 469.24, "duration": 4.919 }, { "text": "CPU host and into AI accelerators", "start": 471.28, "duration": 5.24 }, { "text": "themselves and AI accelerators they're", "start": 474.159, "duration": 4.241 }, { "text": "really talking about gpus for the most", "start": 476.52, "duration": 4.359 }, { "text": "part Maybe Ipus in the future from Gro", "start": 478.4, "duration": 4.519 }, { "text": "but they're really just talking about", "start": 480.879, "duration": 4.801 }, { "text": "gpus right now extending cryptographic", "start": 482.919, "duration": 4.801 }, { "text": "protection to the hardware layer has the", "start": 485.68, "duration": 3.479 }, { "text": "potential to achieve the following", "start": 487.72, "duration": 3.68 }, { "text": "properties and this is really scary to", "start": 489.159, "duration": 4.44 }, { "text": "me and hopefully I'm misreading it but I", "start": 491.4, "duration": 4.56 }, { "text": "don't think I am gpus can be", "start": 493.599, "duration": 4.201 }, { "text": "cryptographically attested for", "start": 495.96, "duration": 4.56 }, { "text": "authenticity and integrity what does", "start": 497.8, "duration": 5.399 }, { "text": "that actually mean that means if you buy", "start": 500.52, "duration": 5.359 }, { "text": "a piece of Hardware from Nvidia that it", "start": 503.199, "duration": 6.44 }, { "text": "is going to be signed like DRM meaning", "start": 505.879, "duration": 6.96 }, { "text": "that is approved to run AI models to", "start": 509.639, "duration": 5.52 }, { "text": "accelerate AI models so who gets to", "start": 512.839, "duration": 4.361 }, { "text": "authorize that piece of hardware and if", "start": 515.159, "duration": 3.601 }, { "text": "you're a small company building your own", "start": 517.2, "duration": 3.719 }, { "text": "Hardware now you have this additional", "start": 518.76, "duration": 4.959 }, { "text": "layer of approvals to go through to get", "start": 520.919, "duration": 4.92 }, { "text": "your Hardware to Market and yeah this is", "start": 523.719, "duration": 4.321 }, { "text": "really scary I don't really want my GPU", "start": 525.839, "duration": 5.521 }, { "text": "to be signed I want my GPU to be", "start": 528.04, "duration": 5.88 }, { "text": "anonymous so gpus having cryptographic", "start": 531.36, "duration": 4.32 }, { "text": "Primitives can enable model weights to", "start": 533.92, "duration": 3.76 }, { "text": "remain encrypted until they are staged", "start": 535.68, "duration": 4.88 }, { "text": "and loaded on the GPU so am I misreading", "start": 537.68, "duration": 5.279 }, { "text": "this tell me if I'm wrong I am not an", "start": 540.56, "duration": 5.279 }, { "text": "expert in cryptography so maybe I am", "start": 542.959, "duration": 4.081 }, { "text": "misunderstanding what they're trying to", "start": 545.839, "duration": 2.841 }, { "text": "get at here but it pretty much sounds", "start": 547.04, "duration": 3.2 }, { "text": "like there's going to be some kind of", "start": 548.68, "duration": 3.399 }, { "text": "signature on each piece of Hardware that", "start": 550.24, "duration": 3.68 }, { "text": "allows you to run Ai and that sounds", "start": 552.079, "duration": 4.0 }, { "text": "absurd because if there's a signature on", "start": 553.92, "duration": 4.359 }, { "text": "it that also means they can revoke the", "start": 556.079, "duration": 4.601 }, { "text": "signature and who gets to decide that so", "start": 558.279, "duration": 4.24 }, { "text": "gpus having unique cryptographic", "start": 560.68, "duration": 3.32 }, { "text": "identity can enable model weights and", "start": 562.519, "duration": 3.241 }, { "text": "inference data to be encrypted for", "start": 564.0, "duration": 4.68 }, { "text": "specific gpus or groups of gpus yeah I", "start": 565.76, "duration": 4.519 }, { "text": "don't think I'm Mr reading this this is", "start": 568.68, "duration": 3.76 }, { "text": "exactly what it means fully realized", "start": 570.279, "duration": 3.521 }, { "text": "this can enable model weights to be", "start": 572.44, "duration": 3.519 }, { "text": "decryptable only by gpus belonging to", "start": 573.8, "duration": 5.36 }, { "text": "authorized parties oh my God this is so", "start": 575.959, "duration": 6.081 }, { "text": "crazy to me this is absurd I could not", "start": 579.16, "duration": 5.16 }, { "text": "disagree more with this approach because", "start": 582.04, "duration": 5.2 }, { "text": "again who gets to decide all right next", "start": 584.32, "duration": 5.519 }, { "text": "Network and tenant isolation guarantees", "start": 587.24, "duration": 6.24 }, { "text": "air gaps are often cited as an essential", "start": 589.839, "duration": 5.44 }, { "text": "security mechanism and that is not", "start": 593.48, "duration": 3.96 }, { "text": "unfounded Network segmentation is a", "start": 595.279, "duration": 3.68 }, { "text": "powerful control used to protect", "start": 597.44, "duration": 3.12 }, { "text": "sensitive workloads like the control", "start": 598.959, "duration": 3.641 }, { "text": "systems for critical infrastructure this", "start": 600.56, "duration": 4.92 }, {

"text": "is completely true air gaps is a", "start": 602.6, "duration": 4.679 }, { "text": "practice that has been around for a long", "start": 605.48, "duration": 3.64 }, { "text": "time and that essentially means let's", "start": 607.279, "duration": 4.081 }, { "text": "say you have a laptop it does not have a", "start": 609.12, "duration": 4.0 }, { "text": "network connection it does not have", "start": 611.36, "duration": 4.88 }, { "text": "Bluetooth it has no way to interact with", "start": 613.12, "duration": 6.2 }, { "text": "the outside world or if it does it can", "start": 616.24, "duration": 4.96 }, { "text": "only interact with a certain set of", "start": 619.32, "duration": 3.84 }, { "text": "computers it's really cut off from the", "start": 621.2, "duration": 3.96 }, { "text": "broader internet so instead we", "start": 623.16, "duration": 4.239 }, { "text": "prioritize flexible Network isolation", "start": 625.16, "duration": 4.239 }, { "text": "that allows AI systems to work offline", "start": 627.399, "duration": 4.481 }, { "text": "line separated from untrusted networks", "start": 629.399, "duration": 5.201 }, { "text": "including the internet so I guess that's", "start": 631.88, "duration": 5.72 }, { "text": "fine as long as it's optional and I of", "start": 634.6, "duration": 5.16 }, { "text": "course love the idea of AI systems being", "start": 637.6, "duration": 4.479 }, { "text": "able to work offline and so really what", "start": 639.76, "duration": 3.879 }, { "text": "they're talking about is designing", "start": 642.079, "duration": 3.841 }, { "text": "networks that are very isolated in", "start": 643.639, "duration": 4.721 }, { "text": "nature and that's fine for really", "start": 645.92, "duration": 4.479 }, { "text": "sensitive workloads but I don't believe", "start": 648.36, "duration": 4.08 }, { "text": "models and model weights should be", "start": 650.399, "duration": 4.68 }, { "text": "treated as extremely sensitive workloads", "start": 652.44, "duration": 5.12 }, { "text": "and here they go on again this is all", "start": 655.079, "duration": 4.801 }, { "text": "describing very close Source system for", "start": 657.56, "duration": 4.44 }, { "text": "example their architecture so the", "start": 659.88, "duration": 4.079 }, { "text": "networks that they're describing must", "start": 662.0, "duration": 3.959 }, { "text": "eliminate classes of vulnerabilities", "start": 663.959, "duration": 4.0 }, { "text": "that could allow a threat actor with", "start": 665.959, "duration": 4.401 }, { "text": "access to one tenant to compromise model", "start": 667.959, "duration": 4.841 }, { "text": "weights stored in another tenant again", "start": 670.36, "duration": 3.88 }, { "text": "the model weights can't get out all", "start": 672.8, "duration": 3.36 }, { "text": "right three innovation in operational", "start": 674.24, "duration": 4.039 }, { "text": "and physical security for data centers", "start": 676.16, "duration": 4.52 }, { "text": "so operations and physical security", "start": 678.279, "duration": 4.281 }, { "text": "measures for AI data centers are", "start": 680.68, "duration": 3.959 }, { "text": "necessary to ensure resilience against", "start": 682.56, "duration": 3.88 }, { "text": "Insider threats that can compromise the", "start": 684.639, "duration": 3.241 }, { "text": "confidentiality integrity and", "start": 686.44, "duration": 3.36 }, { "text": "availability of the data Center and its", "start": 687.88, "duration": 5.04 }, { "text": "workloads so technically I agree that's", "start": 689.8, "duration": 5.88 }, { "text": "great we should have Security in the", "start": 692.92, "duration": 4.12 }, { "text": "data centers we should have", "start": 695.68, "duration": 3.36 }, { "text": "confidentiality we should be able to", "start": 697.04, "duration": 4.359 }, { "text": "protect sensitive data but again it goes", "start": 699.04, "duration": 4.08 }, { "text": "back to whether or not you believe model", "start": 701.399, "duration": 4.0 }, { "text": "weights should be closed Source or not", "start": 703.12, "duration": 4.279 }, { "text": "if they're open source none of this", "start": 705.399, "duration": 3.281 }, { "text": "security really matters because", "start": 707.399, "duration": 2.601 }, { "text": "everybody's going to have access to it", "start": 708.68, "duration": 3.44 }, { "text": "anyways and here they go on to describe", "start": 710.0, "duration": 4.2 }, { "text": "some common data center security", "start": 712.12, "duration": 4.76 }, { "text": "measures next AI specific audit and", "start": 714.2, "duration": 5.199 }, { "text": "compliance programs since AI Developers", "start": 716.88, "duration": 4.199 }, { "text": "need assurance that their intellectual", "start": 719.399, "duration": 3.521 }, { "text": "property is protected when working with", "start": 721.079, "duration": 3.681 }, { "text": "infrastructure providers AI", "start": 722.92, "duration": 4.039 }, { "text": "infrastructure must be audited for and", "start": 724.76, "duration": 4.44 }, { "text": "compliant with applicable security", "start": 726.959, "duration": 4.12 }, { "text": "standards and so we have existing", "start": 729.2, "duration": 5.439 }, { "text": "standards like sock 2 ISO IEC and nist", "start": 731.079, "duration": 5.281 }, { "text": "families will still apply we expect the", "start": 734.639, "duration": 3.921 }, { "text": "list will grow to include AI specific", "start": 736.36, "duration": 3.96 }, { "text": "security and Regulatory standards that", "start": 738.56, "duration": 3.24 }, { "text": "address the unique challenges of", "start": 740.32, "duration": 4.8 }, { "text": "securing AI systems now again I believe", "start": 741.8, "duration": 6.56 }, { "text": "in securing systems but not necessarily", "start": 745.12, "duration": 5.24 }, { "text": "closed source model weights sorry I keep", "start": 748.36, "duration": 4.64 }, { "text": "repeating myself but I can't stress that", "start": 750.36, "duration": 5.279 }, { "text": "enough security is great model weights", "start": 753.0, "duration": 5.519 }, { "text": "should be open so next AI for cyber", "start": 755.639, "duration": 5.361 }, { "text": "defense We Believe AI will be", "start": 758.519, "duration": 4.44 }, { "text": "transformative for cyber defense and has", "start": 761.0, "duration": 3.72 }, { "text": "the potential to level the playing field", "start": 762.959, "duration": 3.801 }, { "text": "between attackers and Defenders", "start": 764.72, "duration": 3.76 }, { "text": "Defenders across the globe struggle to", "start": 766.76, "duration": 3.4 }, { "text": "ingest and analyze signals needed to", "start": 768.48, "duration": 3.32 }, { "text": "detect and respond to threats to their", "start": 770.16, "duration": 4.039 }, { "text": "networks additionally the resources", "start": 771.8, "duration": 4.08 }, { "text": "required to build a sophisticated", "start": 774.199, "duration": 3.721 }, { "text": "security program are significant placing", "start": 775.88, "duration": 4.199 }, { "text": "meaningful cyber defense Out Of Reach", "start": 777.92, "duration": 4.96 }, { "text": "for many and uh I wonder who the many is", "start": 780.079, "duration": 4.88 }, { "text": "that they're talking about probably the", "start": 782.88, "duration": 4.04 }, { "text": "small companies that they are going to", "start": 784.959, "duration": 4.601 }, { "text": "be competing with in the future all of", "start": 786.92, "duration": 4.76 }, { "text": "this all of it really sounds like", "start": 789.56, "duration": 4.92 }, { "text": "regulatory capture to me and if you", "start": 791.68, "duration": 6.0 }, { "text": "haven't seen this talk by Bill Gurley at", "start": 794.48, "duration": 5.56 }, { "text": "the all-in summit about regulatory", "start": 797.68, "duration": 5.719 }, { "text": "capture I cannot emphasize enough how", "start": 800.04, "duration": 6.68 }, { "text": "good this video is this talk it's 36", "start": 803.399, "duration": 5.321 }, { "text": "minutes and he goes through end to", "start": 806.72, "duration": 5.0 }, { "text": "endend an experience that he had and how", "start": 808.72, "duration": 5.359 }, { "text": "that can extrapolate to the", "start": 811.72, "duration": 4.64 }, { "text": "understanding of regulatory capture so", "start": 814.079, "duration": 5.161 }, { "text": "please watch this bill Gurley is a goat", "start": 816.36, "duration": 5.159 }, { "text": "and this talk is amazing I'll drop a", "start": 819.24, "duration": 4.48 }, { "text": "link to it in the description below so", "start": 821.519, "duration": 4.041 }, { "text": "AI presents an opportunity to enable", "start": 823.72, "duration": 4.0 }, { "text": "cyber Defenders and improve security AI", "start": 825.56, "duration": 3.839 }, { "text": "can be incorporated into security", "start": 827.72, "duration": 3.16 }, { "text": "workflows to accelerate security", "start": 829.399, "duration": 3.56 }, { "text": "engineers and reduce the toil in their", "start": 830.88, "duration": 5.319 }, { "text": "work completely agree I have no caveats", "start": 832.959, "duration": 5.56 }, { "text": "to that we should and we will be", "start": 836.199, "duration": 5.121 }, { "text": "integrating AI into every layer of", "start": 838.519, "duration": 4.921 }, { "text": "security and then it's really about who", "start": 841.32, "duration": 5.28 }, { "text": "is going to have the best AI model and", "start": 843.44, "duration": 5.0 }, { "text": "here's the thing if everything's open", "start": 846.6, "duration": 3.599 }, { "text": "source everybody is going to have the", "start": 848.44, "duration": 3.48 }, { "text": "best model and it kind of will cancel", "start": 850.199, "duration": 3.281 }, { "text": "each other out so attackers and", "start": 851.92, "duration": 4.8 }, { "text": "Defenders both have the exact amount of", "start": 853.48, "duration": 6.0 }, { "text": "AI quote unquote power and here's the", "start": 856.72, "duration": 5.16 }, { "text": "thing I believe the world has more good", "start": 859.48, "duration": 4.44 }, { "text": "actors than Bad actors I also believe", "start": 861.88, "duration": 3.92 }, { "text": "there are more resources for the good", "start": 863.92, "duration": 3.839 }, { "text": "actors than Bad actors and that's why", "start": 865.8, "duration": 4.039 }, { "text": "I'm not worried about open source and", "start": 867.759, "duration": 4.921 }, { "text": "open weights for AI because ultimately", "start": 869.839, "duration": 5.201 }, { "text": "we're not going to have this huge", "start": 872.68, "duration": 5.599 }, { "text": "overnight jump in technology or", "start": 875.04, "duration": 6.359 }, { "text": "capabilities for AI and especially not", "start": 878.279, "duration": 5.24 }, { "text": "for the Bad actors I've heard this again", "start": 881.399, "duration": 4.521 }, { "text": "and again from AI thought leaders there", "start": 883.519, "duration": 6.041 }, { "text": "is no overnight huge leap in technology", "start": 885.92, "duration": 5.64 }, { "text": "for AI it is incremental and it is going", "start": 889.56, "duration": 4.12 }, { "text": "to be overtime so that means let's say", "start": 891.56, "duration": 4.959 }, { "text": "just for example the best AI model might", "start": 893.68, "duration": 5.839 }, { "text": "only be 5 10% better than the the second", "start": 896.519, "duration": 5.56 }, { "text": "best AI model and then they go on to say", "start": 899.519, "duration": 4.68 }, { "text": "at open AI we use our models to analyze", "start": 902.079, "duration": 3.721 }, { "text": "high volume and sensitive security", "start": 904.199, "duration": 3.401 }, { "text": "Telemetry that would otherwise be Out Of", "start":

905.8, "duration": 4.12 }, { "text": "Reach for teams of human analysts they", "start": 907.6, "duration": 5.679 }, { "text": "keep using that term Out Of Reach and", "start": 909.92, "duration": 4.8 }, { "text": "again they're really setting themselves", "start": 913.279, "duration": 3.721 }, { "text": "up to say this is the standard and if", "start": 914.72, "duration": 4.44 }, { "text": "you don't have the resources to have", "start": 917.0, "duration": 3.839 }, { "text": "this standard maybe you shouldn't have", "start": 919.16, "duration": 4.28 }, { "text": "ai and that's absurd all right number", "start": 920.839, "duration": 5.041 }, { "text": "six last resilience redundancy and", "start": 923.44, "duration": 4.44 }, { "text": "research we need to test these measures", "start": 925.88, "duration": 3.72 }, { "text": "and appreciate that these concepts are", "start": 927.88, "duration": 3.8 }, { "text": "likely just the beginning continuous", "start": 929.6, "duration": 3.919 }, { "text": "security research is required given the", "start": 931.68, "duration": 3.44 }, { "text": "Green Field and swiftly evolving state", "start": 933.519, "duration": 3.641 }, { "text": "of AI security I agree with everything", "start": 935.12, "duration": 3.719 }, { "text": "they said there this includes research", "start": 937.16, "duration": 3.119 }, { "text": "on how to circumvent the measures", "start": 938.839, "duration": 3.761 }, { "text": "outlined above as well as to close the", "start": 940.279, "duration": 4.961 }, { "text": "gaps that will inevitably be revealed", "start": 942.6, "duration": 5.64 }, { "text": "lastly these controls must provide", "start": 945.24, "duration": 5.64 }, { "text": "defense in depth there are no Flawless", "start": 948.24, "duration": 5.68 }, { "text": "systems and there is no perfect security", "start": 950.88, "duration": 4.399 }, { "text": "okay so they're just talking about", "start": 953.92, "duration": 3.52 }, { "text": "defense redundancy now which yeah okay I", "start": 955.279, "duration": 4.281 }, { "text": "agree with and so that's it those are", "start": 957.44, "duration": 5.04 }, { "text": "their ideas on AI Safety and Security", "start": 959.56, "duration": 5.88 }, { "text": "and I want to know what you think I am a", "start": 962.48, "duration": 5.64 }, { "text": "staunch supporter of open weights open", "start": 965.44, "duration": 6.36 }, { "text": "source I am super appreciative of the", "start": 968.12, "duration": 6.279 }, { "text": "meta AI team Mark Zuckerberg really he's", "start": 971.8, "duration": 5.519 }, { "text": "the decision maker at meta and his Allin", "start": 974.399, "duration": 6.521 }, { "text": "attitude on open source is vastly needed", "start": 977.319, "duration": 5.801 }, { "text": "because if meta weren't doing it", "start": 980.92, "duration": 4.919 }, { "text": "Google's certainly not doing it and open", "start": 983.12, "duration": 6.079 }, { "text": "AI is a proponent of completely close", "start": 985.839, "duration": 5.8 }, { "text": "Source models well we would be in a very", "start": 989.199, "duration": 4.241 }, { "text": "different state today if llama did not", "start": 991.639, "duration": 4.44 }, { "text": "exist so again very thankful to The Meta", "start": 993.44, "duration": 5.8 }, { "text": "AI team and their positioning in the AI", "start": 996.079, "duration": 4.88 }, { "text": "landscape if you enjoyed this video", "start": 999.24, "duration": 3.039 }, { "text": "please consider giving a like And", "start": 1000.959, "duration": 2.961 }, { "text": "subscribe and I'll see you in the next", "start": 1002.279, "duration": 3.92 }, { "text": "one", "start": 1003.92, "duration": 2.279 }]