WEBVTT

57

00:05:46.470 --> 00:06:03.090

jim.ash: And getting it set up as it will be exchanged a few emails on how we wanted to flow this. My name is Jim ash. I'm the Florida. He RP sales rep for Tyler technologies Tyler technologies does

58

00:06:04.410 --> 00:06:16.650

jim.ash: A lot of different applications beyond cyber security in Florida. You don't have to have our other applications in which to to engage and Tyler detect what we're going to talk about

59

00:06:17.850 --> 00:06:35.670

jim.ash: For the balance of the hour, but you may be familiar. We have financial applications and time and attendance and payroll and analytics analytics facilities management electronic data.

60

00:06:37.110 --> 00:06:39.900

jim.ash: Storage the document storage.

61

00:06:41.550 --> 00:06:50.730

jim.ash: When you look at what Tyler does for schools across the country. There's a little more than 18,000 school districts in the country.

62

00:06:51.780 --> 00:06:52.230

jim.ash: And

63

00:06:53.430 --> 00:06:54.960

jim.ash: When you look at him.

64

00:06:55.170 --> 00:07:02.190

jim.ash: 25% of those school districts have some sort of Tyler software.

65

00:07:03.540 --> 00:07:13.740

jim.ash: In there helping them to administer the districts as they go through their daily operations in the stuff that I talked about before, but just a very broad.

66

00:07:15.450 --> 00:07:27.480

jim.ash: Selection of software you can of course hit our web page at Tyler tech com and get a briefing on that or if if you have needs beyond the cyber security.

67

00:07:28.770 --> 00:07:36.600

jim.ash: Please feel free to contact me or visit with me. We'd love to talk with you about the broader applications that

68

00:07:37.200 --> 00:07:44.490

jim.ash: Tyler delivers that's really all I had. Today, I would just wanted to open it with a minute or two there to

69

00:07:45.150 --> 00:08:00.870

jim.ash: Really just give you the background let you know that Tyler does a lot more than what we're going to show today, and I'll turn over the balance of the time to Karen to talk about the, the subject of the day cyber security. You ready, Karen.

70

00:08:03.690 --> 00:08:05.430

karen.grosset: I am, thank you again.

71

00:08:06.900 --> 00:08:20.670

karen.grosset: Thank you all for joining today. I know it's different times and wish we were all there together, but it is what it is. And I've been doing webinars nonstop, so we can get the point across. No doubt this morning, or this afternoon, I should say.

72

00:08:21.480 --> 00:08:25.590

karen.grosset: The FM was Tyler technologies actually over 20 years now.

73

00:08:26.460 --> 00:08:36.270

karen.grosset: As an account executive before, just making sure our customers, our existing customers schools and municipalities have all the different Tyler applications and Tyler services that they need.

74

00:08:36.600 --> 00:08:47.400

karen.grosset: To be running effectively and efficiently and a couple years ago, the cybersecurity opportunity came up and I was extremely excited about it because I believe it was it was a big hole, unfortunately.

75

00:08:47.760 --> 00:08:58.950

karen.grosset: That I think a lot of our customers are feeling in unfortunately suffering from as well. So I was happy to come on board with this and be able to talk to you about the type of solution that we have today.

76

00:09:00.570 --> 00:09:11.430

karen.grosset: So it's a great story and Tyler has all sorts of great stories and I really like this one as well. So cyber security. It's important for everybody. It's important for Tyler technologies.

77

00:09:12.150 --> 00:09:26.160

karen.grosset: Especially in our data center. That's where we host over 5000 of our Tyler clients we host their data and their applications, whether we're doing their nightly disaster recovery backups or hosting them in a SAS environment.

78

00:09:27.120 --> 00:09:31.380

karen.grosset: So again, we need to make sure we're keeping everything as buttoned up and safe as possible.

79

00:09:31.650 --> 00:09:43.890

karen.grosset: And for those of you that are working with cyber security that are tasked with cyber security you know, there's no one silver bullet that you can put in place and say all protected. It's really about layering.

80

00:09:44.370 --> 00:09:49.710

karen.grosset: So what Tyler did back in 2013 was partner with a company called Safe data security.

81

00:09:50.220 --> 00:09:59.400

karen.grosset: And they provide in what we now call the Tyler detect service. It was log monitoring and it was threat hunting services and they did a great job.

82

00:09:59.970 --> 00:10:05.610

karen.grosset: Making sure on a daily basis that things that our data center. We're working as effectively as possible.

83

00:10:06.090 --> 00:10:11.520

karen.grosset: So we really liked the service and much more. So realize our customers could benefit from the service.

84

00:10:12.030 --> 00:10:25.980

karen.grosset: The very cost effective way to have these resources, doing the necessary work of monitoring network activity that again. Unfortunately, with limited resources. We know that in our school customers. Just don't necessarily have that time.

85

00:10:26.550 --> 00:10:39.510

karen.grosset: Or expertise to do so to Tyler fashion, we went ahead inquired sage data security to little over two years ago now, so that we can provide this service out to our customers.

86

00:10:42.510 --> 00:10:52.290

karen.grosset: So it municipal landscapes, you know, I'm sure if you sitting on any other classes or sessions during the conference, you know that cyber security is

87

00:10:52.770 --> 00:11:01.470

karen.grosset: In cyber activity is unfortunately on the rise. Hopefully none of you have been hit yourself but I'm sure you know every municipality.

88

00:11:01.740 --> 00:11:09.870

karen.grosset: Our school district nearby that has suffered from a cyber attack and it makes a lot of sense. Why they target municipalities and schools.

89

00:11:10.380 --> 00:11:20.190

karen.grosset: There's so much critical data student information including social security numbers, sometimes banking information email addresses physical addresses.

90

00:11:21.030 --> 00:11:27.180

karen.grosset: They want to get their hands on this data, not necessarily to do anything from their side of the house, but they know what they access this data.

91

00:11:27.570 --> 00:11:37.680

karen.grosset: And bring down your networks, then you can't be serving your, you know, your students, effectively, it doesn't matter if your large or small, again, they know that if they've

92

00:11:38.430 --> 00:11:54.420

karen.grosset: They're taking away your ability to access this data, then you can't be effective at your job and the numbers are growing. If you look at the numbers. Last year between that and the year before over 1000 US schools were impacted in

93

00:11:55.920 --> 00:12:06.060

karen.grosset: And that includes the Louisiana attacks that all occurred right at the end of the summer, right before the school session started up again. They had to actually declared state of emergency down there.

94

00:12:06.480 --> 00:12:15.300

karen.grosset: And that was a large increase over 2018 Tyler itself because we do have again so many customers and our disaster recovery.

95

00:12:15.810 --> 00:12:30.570

karen.grosset: Service where we do a nightly backup and, in the event that anything happens, we can still access your applications and your Tyler data. We had a 350% increase in declared disasters due to cyber attacks in 2019 over

96

00:12:32.160 --> 00:12:38.010

karen.grosset: And these numbers are growing, we're seeing them on our end and the experts predict the growth is going to continue as well.

97

00:12:38.670 --> 00:12:47.400

karen.grosset: And especially right now in this you know code 19 world where people are working remotely we're expanding our attack services.

98

00:12:47.790 --> 00:12:57.750

karen.grosset: You might just be trying to make your job easier by flipping a USB into your work computer so that you can take a file and move it over to your home computer or your home laptop.

99

00:12:58.350 --> 00:13:05.370

karen.grosset: Or emailing a file over because you'd rather work on a personal computer than your work computer and then you're sending that information back.

100

00:13:05.850 --> 00:13:14.250

karen.grosset: So by by sending information and sharing information with unsecured devices we again, we're really expanding our attack services.

101

00:13:14.760 --> 00:13:24.990

karen.grosset: Working through VPN, you know, the hackers are well aware that people might not be patching them and putting in the updates as quickly as necessary. And so those are vulnerable area as well.

102

00:13:25.500 --> 00:13:35.940

karen.grosset: So they're taking advantage of it. Unfortunately, and then there's just your typical phishing emails, where they're trying to you know get you to click on a malicious link.

103

00:13:36.420 --> 00:13:45.420

karen.grosset: By us talking about maybe a a coven 19 check government check funding that's coming your way or coven 19 relief.

104

00:13:45.930 --> 00:13:52.470

karen.grosset: Relief, excuse me. So we're in a home rule. Time for sure. It's certainly not a time to let our guard down

105

00:13:53.430 --> 00:14:04.110

karen.grosset: And we're seeing and hearing. Unfortunately, especially in North Carolina and a couple in Florida as well have some municipalities and school districts being hit

106

00:14:04.560 --> 00:14:13.560

karen.grosset: And so again, like I said, those numbers are on the rise. Unfortunately, but I do like to kind of point out two sites that were hit in 2019

107

00:14:14.370 --> 00:14:20.700

karen.grosset: One's a very large city on the East Coast Baltimore, Maryland. Probably everybody has heard about that incident that occurred.

108

00:14:21.300 --> 00:14:37.080

karen.grosset: But the other ones right down in Florida, Revere a beach about 20th, the size of Baltimore, Maryland. But again, that the hackers are looking at larger small they really don't care. They're just trying to get that end result which is money out of these systems.

109

00:14:38.190 --> 00:14:52.620

karen.grosset: So the attacks happened, both within a couple weeks apart in May of 2019 Baltimore, Maryland had a Robin Hood type of virus that infected the city and Revere Beach was again your typical email phishing campaign.

110

00:14:53.760 --> 00:15:02.520

karen.grosset: Emails email phishing is so it's still the number one way that hackers infiltrate systems and it is so successful, I believe, because

111

00:15:03.000 --> 00:15:06.510

karen.grosset: We're so used to the pace and pattern of technology these days.

112

00:15:06.750 --> 00:15:17.370

karen.grosset: That we might run off to a meeting and as soon as we get back to our desk. We want to quickly run through our email and you know get things out of our inbox. I know that's my mo I want to keep my inbox as clean as possible so

113

00:15:17.730 --> 00:15:24.300

karen.grosset: As opposed to taking a step back and pausing and saying, okay, is this email, something that I initiated.

114

00:15:25.140 --> 00:15:31.290

karen.grosset: Is this an email that I'm expecting communication that I'm expecting and do I know where this is coming from.

115

00:15:31.710 --> 00:15:45.180

karen.grosset: Again before taking that time to really vet these emails we kind of just unfortunately click a quick little too quickly. And that's what can get us into trouble. And again, why these phishing emails are so successful for the hackers.

116

00:15:46.200 --> 00:15:59.520

karen.grosset: So Baltimore, they asked $76,000 for the ransom. That was the equivalent of 13 Bitcoin back then in back then. At this time, that was a typical amount for ransom ask

117

00:16:00.330 --> 00:16:06.930

karen.grosset: Before this time it was really just opportunistic attacks that the hackers were doing spray and pray, if you will.

118

00:16:07.560 --> 00:16:16.920

karen.grosset: Seeing is, you know, maybe one out of 10 hits, they could get and maybe some money out of them. They were happy with it. But now they're becoming much more targeted they're doing their research.

119

00:16:17.580 --> 00:16:27.990

karen.grosset: They're sitting laying in wait, if you will, figuring out vulnerabilities in networks and figuring out the best way to infiltrate these networks unseen until they can do.

120

00:16:28.440 --> 00:16:37.020

karen.grosset: Large scale attack and bring everything down and asked for a much higher ransom, which was the case in Revere Beach. It was almost a $600,000 ask

121

00:16:37.980 --> 00:16:44.490

karen.grosset: Again, much larger, we are seeing the ransoms increase as the hackers again are becoming much more targeted.

122

00:16:44.820 --> 00:16:59.460

karen.grosset: We actually had a city in Massachusetts. Last year, towards the end of 2019 got hacked in the hackers asked for 5.3 million for ransom. They did not pay that one. They tried to negotiate once they started negotiating that and a hackers went

123

00:16:59.610 --> 00:17:04.830

karen.grosset: Silent on them. So the site was left to get everything back up and running on their own.

124

00:17:05.730 --> 00:17:10.470

karen.grosset: Which is a large endeavor, because if you look at Baltimore, Maryland. They did not pay the ransom either

125

00:17:11.010 --> 00:17:18.990

karen.grosset: And they have been very public about this. They said, with all the it over time hiring of consultants lost revenue.

126

00:17:19.260 --> 00:17:27.090

karen.grosset: From their side because they actually had to stop real estate sales for over a month after the attack because they couldn't access the data to confirm

127

00:17:27.510 --> 00:17:34.650

karen.grosset: The property owners confirm or whether there are any liens on those properties they couldn't get utility bills out for five months after the attack.

128

00:17:34.980 --> 00:17:42.480

karen.grosset: Again, because they couldn't access systems and access data that was needed for that. So they waive late fees. So a lot of lost revenue there.

129

00:17:42.900 --> 00:17:55.260

karen.grosset: Resulting in almost 18 million loss because of this incident at Baltimore. Now on the other side of the coin Ruby or beach to go ahead and decide to pay the almost 600,000 ransom.

130

00:17:55.950 --> 00:18:00.930

karen.grosset: You know, they took a look and just realize that their backups weren't where they needed to be. It was going to

131

00:18:02.010 --> 00:18:13.080

karen.grosset: Be much more effective effective and efficient for them to just pay the ransom, and hopefully get all their data back we are dealing with criminals. So the odds that you get 100% of your data back are slim to none.

132

00:18:13.440 --> 00:18:24.270

karen.grosset: They say in the best case scenario, you typically get 90% of your data back but again for Revere Beach. That was a better scenario than not working with the hackers.

133

00:18:24.780 --> 00:18:30.780

karen.grosset: So they paid the ransom. They actually spent took 900 and capital funds to go back and upgrade.

134

00:18:31.170 --> 00:18:47.220

karen.grosset: A lot of their infrastructure their hardware because they did realize a lot of their workstations were very old running on old versions of Windows, which was part of why they were so susceptible so conservatively. They're a one and a half million dollar expense for them as well.

135

00:18:48.450 --> 00:18:53.790

karen.grosset: So they had to these two cities had to be reactive because they were hit with

136

00:18:54.210 --> 00:19:03.750

karen.grosset: ransomware and that was their best case scenario and Maryland's case to try and rebuild from scratch, Revere of Revere beaches case to actually pay the ransom.

137

00:19:04.260 --> 00:19:12.990

karen.grosset: And attain that data back. But I think if you know they could go back in time and say, is there a way that as opposed to being reactive. We can be proactive.

138

00:19:13.410 --> 00:19:23.100

karen.grosset: And have a service so that we know what's happening with our network and be aware when anything malicious is occurring so that we can stop it in its tracks before

139

00:19:23.430 --> 00:19:39.210

karen.grosset: It becomes a large scale incident. I think they'd be on board and that's what we want to talk about today is what we have for a service through Tyler technologies is called Tyler detect and it is an advanced threat detection service.

140

00:19:40.260 --> 00:19:51.720

karen.grosset: We are going out in monitoring your network doing that with the log files. We're doing this 24 seven so that it is that proactive support and insurance, if you will.

141

00:19:52.620 --> 00:20:00.840

karen.grosset: As you're working on your day to day activities. We're doing the hard work with our expertise to figure out, figuring out if there's any chinks in your armor of your network.

142

00:20:01.140 --> 00:20:09.180

karen.grosset: And making you aware of that. So we can shore that up as quickly as possible, so it doesn't infiltrate your system and cause any downtime to you.

143

00:20:10.320 --> 00:20:20.580

karen.grosset: So it's managed threat detection is what it really boils down to, we're looking at anything that could possibly put you at risk malware and ransomware are the big

144

00:20:21.150 --> 00:20:25.710

karen.grosset: You know, the big targets these days. We're definitely looking for that type of information.

145

00:20:26.430 --> 00:20:36.060

karen.grosset: But or activity, I should say. But there's other things that can put you at risk as well think about zero day exploits, especially within the schools, you think about all the applications.

146

00:20:36.420 --> 00:20:46.260

karen.grosset: All the upgrades you're continuously doing patches, you're continuously doing hackers definitely know how to take advantage of those upgrades and new code, if you will.

147

00:20:47.040 --> 00:20:59.190

karen.grosset: So we're looking for that type of behavior as well insider threats. I almost prefer to say insider. Oops, if you will. I really find it hard to believe that we have any of our customers, employees.

148

00:20:59.610 --> 00:21:11.310

karen.grosset: Trying to do malicious harm to networks. But again, because we're so used to the pace and pattern and it just takes one click to put your network at risk that one little. Oops.

149

00:21:12.150 --> 00:21:17.430

karen.grosset: You know, oops, maybe I wasn't supposed to click on that, it does it's taking me to a site. I've never seen before.

150

00:21:18.180 --> 00:21:25.500

karen.grosset: Probably shouldn't have done that. I don't know how to backtrack out of that. So it's really those those insider. Oops, that that behavior that

151

00:21:25.890 --> 00:21:31.650

karen.grosset: You know, when we just don't have our thinking caps on we're trying to do things quickly that can put networks at risk.

152

00:21:32.310 --> 00:21:44.670

karen.grosset: But even things like Aaron administrative activity. If someone is creating new users, maybe at a firewall level or a server level or granting excessive permissions at those levels for users.

153

00:21:45.120 --> 00:21:54.780

karen.grosset: That's information, you know, activity that could put you at risk as well. So this is the all all the type of activity that we're looking for anything that could put you at risk.

154

00:21:55.320 --> 00:22:12.600

karen.grosset: We're doing this again 24 seven all hours of the day we're doing it in real time and we don't just have, you know, like your antivirus and anti malware. It's not just automated programs. It's actually human expertise and human analysts doing this investigating

155

00:22:14.550 --> 00:22:15.540

karen.grosset: So what we're doing.

156

00:22:15.660 --> 00:22:26.640

karen.grosset: We're using log files that is the basis like the thumbprint or the DNA, if you will, of what occurs on your network on a daily basis. So that gives us all the information

157

00:22:27.030 --> 00:22:35.250

karen.grosset: That we need to be able to figure out and do our detective work of what's going on. So we transfer these log files over securely.

158

00:22:35.940 --> 00:22:43.620

karen.grosset: 24 seven from your network over to our SoC our security operating center. And that's where our analysts. Do all their work.

159

00:22:44.490 --> 00:22:51.060

karen.grosset: So when we bring these over, we basically put the log files into one of three buckets, if you will, virtual buckets, if you will.

160

00:22:51.630 --> 00:22:57.180

karen.grosset: The first bucket are events that we've seen before. And we know they're not causing any harm.

161

00:22:57.840 --> 00:23:04.140

karen.grosset: When you think about that, that really is the majority of your day to day activity on your network. And it might be that

162

00:23:04.650 --> 00:23:11.970

karen.grosset: We've seen it before on your network or we seen it before. On the hundreds of other networks that were monitoring, I would say their strength in numbers.

163

00:23:12.780 --> 00:23:20.280

karen.grosset: So we're going to look at it as a broad concept across all of our networks. And again, if we've seen it before. We know it's not putting you at harm.

164

00:23:20.640 --> 00:23:28.890

karen.grosset: That's something that we say, okay, it's, it's nothing that requires us to dig into any further and we let that activity go obviously

165

00:23:29.550 --> 00:23:35.100

karen.grosset: Now the second bucket are events that we have seen before as well. But we know they're harmful.

166

00:23:35.730 --> 00:23:43.590

karen.grosset: You know, just like an antivirus that has a dictionary of known bad if you will. And it's going to block in any event that comes through that's in that dictionary.

167

00:23:44.130 --> 00:23:54.660

karen.grosset: We do the same thing, but we have to take a little more time and effort with our side of the house because when it comes to hackers. They aren't just using the same old tricks.

168

00:23:55.050 --> 00:24:02.460

karen.grosset: Time and time again, they need they have many tricks in their bag to infiltrate systems and each infiltration has a different thumbprint.

169

00:24:02.760 --> 00:24:08.430

karen.grosset: Than the other. So it really takes those humanized to be able to pinpoint that type of activity.

170

00:24:09.000 --> 00:24:17.850

karen.grosset: Now if something does happen in the second bucket that we know is that we're going to reach out to you immediately make you aware of what's occurring on the network.

171

00:24:18.630 --> 00:24:29.130

karen.grosset: Where it's infiltrated your network which machines are infected so that we can immediately contain that behavior when it's only on one to two machines as opposed to spreading through your network.

172

00:24:29.610 --> 00:24:38.280

karen.grosset: Because timing is very, very key obviously when it comes to malware undetected malware can sit on networks for months and months.

173

00:24:38.910 --> 00:24:42.810

karen.grosset: Before the hackers decide to, you know, really do anything with it.

174

00:24:43.380 --> 00:24:51.900

karen.grosset: But we want to find things as quickly as possible, so things don't spread through. And when we talk about transferring the files over and our analysts reviewing

175

00:24:52.410 --> 00:25:00.180

karen.grosset: That is literally only about a 20 to 25 minute turnover from maybe the time you click on a link of a malicious email.

176

00:25:00.750 --> 00:25:11.760

karen.grosset: sending that information over to us were alerted that something new is occurring on the network. And we dig in investigate that. And either confirm that it is malicious or not and make you aware of it.

177

00:25:12.270 --> 00:25:21.780

karen.grosset: So within that time period, we're only talking about one to two machines that are possibly infected. So it's very easy to keep that activity mitigated and contained

178

00:25:23.190 --> 00:25:24.600

karen.grosset: So the third bucket.

179

00:25:25.770 --> 00:25:32.070

karen.grosset: events that occur on the network are things that we haven't seen before. They're brand new to us.

180

00:25:32.490 --> 00:25:38.010

karen.grosset: Or we've seen them before. And we just haven't come to an overall conclusion of their risk yet.

181

00:25:38.430 --> 00:25:45.090

karen.grosset: And again, this bucket is where the analysts spend the majority of their time figuring out what the nature of the activity is

182

00:25:45.630 --> 00:25:53.820

karen.grosset: Where it's originating from how it's infiltrated your system and putting it into context as well when I'm talking about context.

183

00:25:54.540 --> 00:26:00.870

karen.grosset: Something might come through on your network. Let's say somebody does a Google search at two in the afternoon.

184

00:26:01.500 --> 00:26:11.610

karen.grosset: From within your network from a device that we've seen within your network and the Google searches. How to disarm a Stanley alarm system Stanley door alarm system.

185

00:26:12.030 --> 00:26:22.200

karen.grosset: Now most schools have these alarm systems on their front doors or doors in general just to you know make sure that only students are getting in and out or parents who are authorized

186

00:26:22.680 --> 00:26:27.300

karen.grosset: Or clicking up other and talking to the secretary and they allow access them.

187

00:26:27.930 --> 00:26:39.150

karen.grosset: So if it's two in the afternoon and somebody's looking up how to disarm of one of these systems. It might be that it's jammed locked in schools, about to be let out from from for the afternoon and

188

00:26:39.420 --> 00:26:50.700

karen.grosset: We want to make sure that the traffic can flow in and out. So we won't think too too much about that scenario. But let's say that same actions that same activity occurs.

189

00:26:51.300 --> 00:26:55.770

karen.grosset: Google search on how to disarm Stanley alarm system at three in the morning.

190

00:26:56.220 --> 00:27:03.480

karen.grosset: And it's occurring from outside your network on a guest wireless network on a device that we've never seen before, within your network.

191

00:27:03.900 --> 00:27:15.570

karen.grosset: That context is much more suspicious to us and the analysts are going to spend much more time on that. Figuring out the nature of that event to see if it is putting you at risk or not.

192

00:27:17.310 --> 00:27:20.940

karen.grosset: So we're gathering all this information, all this log files.

193

00:27:21.660 --> 00:27:36.030

karen.grosset: So that we understand the nature of your network and your daily network activity and have a lot of information to be able to put that into context again for the whole purpose of figuring out if these events are putting you at risk or not.

194

00:27:36.630 --> 00:27:44.760

karen.grosset: And we're monitoring everything. This is not just related to your Tyler applications or the devices that your Tyler apps are running on

195

00:27:45.120 --> 00:27:57.360

karen.grosset: This is across your entire network. So we started the firewall. We're looking at servers and we're going all the way down to end user machines and end user devices. This includes like email gateways.

196

00:27:58.920 --> 00:28:13.230

karen.grosset: Hardware like VPN switches and routers your phones wireless, etc. We want to get information from everywhere. One, because an attack and really occur from any different vector within your network. And like I mentioned VPN.

197

00:28:13.800 --> 00:28:19.710

karen.grosset: Our big area right now have compromised and the hackers are well aware of that as people are working remotely.

198

00:28:20.670 --> 00:28:25.410

karen.grosset: So we can see this type of activity that is out of the ordinary from any level.

199

00:28:26.010 --> 00:28:34.920

karen.grosset: But having all that information as well really helps us put it into context and dig further if needed, we might find something new that comes through on a device.

200

00:28:35.280 --> 00:28:43.680

karen.grosset: And being able to have being able to compare that with the firewall traffic as well really gives us a broad view of what's going on with these events.

201

00:28:45.600 --> 00:28:53.190

karen.grosset: And with the events, what we're really looking for is new persistence mechanism. So not all processes mechanisms or malware.

202

00:28:53.730 --> 00:29:02.730

karen.grosset: Some are most of them are completely fine innocuous. But from our to be effective. It has to create a persistence mechanism within your network.

203

00:29:03.150 --> 00:29:09.420

karen.grosset: So by calling out anything new. Any new processes that occurred mechanism that occurs on your network.

204

00:29:10.050 --> 00:29:16.320

karen.grosset: That's where, again, our analysts focus their time on to figure if this new behavior is putting you at risk.

205

00:29:16.800 --> 00:29:24.750

karen.grosset: Because once we do start up Tyler detect, we're going to get a baseline of what a normal day to day activity network activity looks like.

206

00:29:25.290 --> 00:29:37.410

karen.grosset: For your system so that anything out of the ordinary anything new that comes through really stands out. And again, that's where we want our analysts spending their time to research that activity.

207

00:29:40.200 --> 00:29:46.470

karen.grosset: So when you look at and think of threats on a threat spectrum over on the left.

208

00:29:47.100 --> 00:29:55.530

karen.grosset: You know, you've got things that are easily detectable with your firewalls with your antivirus and anti malware and I'm sure everyone's keeping things up to date.

209

00:29:55.980 --> 00:30:08.010

karen.grosset: And, you know, installing those regularly and that's great. Again, they're good, they do a good job at stopping known bad and they can work on their own. There's, there's no need for human intervention or anything like that.

210

00:30:09.150 --> 00:30:16.680

karen.grosset: But where Tyler detect is really working is the wrong this right hand side of the threat spectrum with the red and the infrared.

211

00:30:17.490 --> 00:30:23.490

karen.grosset: There's one of our customers, said the hackers are using human intelligence to figure out how to infiltrate our systems.

212

00:30:23.880 --> 00:30:37.560

karen.grosset: He's like, I don't know how antivirus and anti malware. They're going to be effective, you really need human intelligence to figure out what the hackers are doing to stop them in their tracks and I couldn't agree more. Because we do think about it.

213

00:30:38.850 --> 00:30:47.700

karen.grosset: All when you know anything, any events that happen whether it's Revere Beach or Baltimore, all these attacks that occurred all the clues were there.

214

00:30:48.090 --> 00:31:00.450

karen.grosset: It's just that nobody necessarily had the resources, the time or the expertise to look through and find those clues to figure out what was occurring and be able to stop it before it became unfortunately a ransomware event.

215

00:31:01.590 --> 00:31:14.790

karen.grosset: And again, that's, that's what our analysts are trained to do 24 seven looking through your data and your logs to see if there's anything out of the ordinary occurring so that we can stop it in its tracks.

216

00:31:16.920 --> 00:31:28.320

karen.grosset: So I'd like to equate the tower detect service, as you know, keeping your networks your users, your guests who come in to the school systems, teachers, students

217

00:31:28.740 --> 00:31:36.810

karen.grosset: keeping them safe by doing a 360 review of all the activity within the network 24 seven around the clock.

218

00:31:37.380 --> 00:31:46.470

karen.grosset: So it'd be nice if when you go home in the evening or just in general, knowing that you had that same kind of comfort and review for your home, somebody looking around it.

219

00:31:46.860 --> 00:31:56.760

karen.grosset: At 360 degree view 24 seven so that maybe before you go to bed at night. It could alert you that you've left the door unlocked, or there's a window ajar.

220

00:31:57.090 --> 00:32:03.690

karen.grosset: Things like typically on the left hand side of the spectrum that aren't too hard to detect. And you can remediate those quickly.

221

00:32:04.200 --> 00:32:09.750

karen.grosset: But what about the things that you can't see in your home, like maybe there's a little hairline fracture.

222

00:32:10.140 --> 00:32:16.200

karen.grosset: In your foundation that's invisible to the naked eye. But if it's left unchecked is going to

223

00:32:16.620 --> 00:32:27.360

karen.grosset: lead to bigger problems down the road. So it'd be nice to have an alert and an update on that as quickly as possible so that he can remediate that situation and get it shored up sooner rather than later.

224

00:32:28.320 --> 00:32:34.380

karen.grosset: Or maybe there's a hornet's nest that has they built that under one of the shingles of your roof.

225

00:32:35.250 --> 00:32:46.170

karen.grosset: You haven't looked up there to notice, maybe time the equivalent of a port being Open All Hours 24 seven as opposed to just one hour on Saturday nights when the bank needs to send that file to you.

226

00:32:46.860 --> 00:32:54.750

karen.grosset: Will give you all those kinds of updates so that you're aware of what's going on and any chinks in the armor of your network or home, if you will.

227

00:32:55.620 --> 00:32:58.590

karen.grosset: Now I mentioned Aaron's administrative activity.

228

00:32:59.190 --> 00:33:11.910

karen.grosset: I have a closet in my home. I have a 13 and 14 year old and they know under no circumstances are they allowed to enter that closet, because that's where I hide all the goodies like their birthday presents and Christmas presents, etc.

229

00:33:12.900 --> 00:33:23.010

karen.grosset: So if I'm at work one day I would be nice to have an alert saying my 13 year old daughter just snuck a peek into that closet and I can deal with her accordingly.

230

00:33:23.970 --> 00:33:36.450

karen.grosset: Again, kind of the same idea of what Tyler detect can do with you as well. Hey, someone has created excessive user permissions for this user at the firewall level something you might want to look into and deal with

231

00:33:37.200 --> 00:33:49.170

karen.grosset: When the timings appropriate at the same time. Maybe somebody is approaching your front door from the sidewalk. They're dressed all in blue, and they're carrying packages.

232

00:33:49.620 --> 00:33:55.860

karen.grosset: That's something that we won't alert on because we know every weekday the mail woman delivers the mail.

233

00:33:56.190 --> 00:34:03.780

karen.grosset: On the same route looking the same in the same outfit carrying packages. So we know that's expected behavior and it's nothing that's putting you at risk.

234

00:34:04.350 --> 00:34:11.760

karen.grosset: But let's say it's two in the morning and someone's approaching your house from the backwoods and no one ever approaches, your house from the backwoods

235

00:34:12.120 --> 00:34:25.050

karen.grosset: It's a person that we've never seen on your property before upon closer look, it looks like they're wearing camouflage with a mask and carrying something that looks suspiciously like a crowbar, and they're headed right for your back door.

236

00:34:26.220 --> 00:34:30.540

karen.grosset: So what detect would do in that case is put on the floodlights on the back.

237

00:34:31.080 --> 00:34:39.150

karen.grosset: Put on your, your alarm system and call the police and make them make him make everybody inside aware that someone's approach from the back door so

238

00:34:39.420 --> 00:34:56.430

karen.grosset: You can safely get out of the house from the front door right now while the police come and deal with the intruder. So again, that's the idea is 360 degree view making you aware of anything that's putting your home at risk or your network at risk at any time.

239

00:34:58.440 --> 00:35:06.810

karen.grosset: So that's what we're doing on the back end of our side to make sure that we're keeping things and monitoring things and keeping things secure

240

00:35:07.350 --> 00:35:17.460

karen.grosset: What you'll see on your side, first and foremost, we published daily reports and these are consolidated views of the previous day's log activity.

241

00:35:18.210 --> 00:35:25.200

karen.grosset: So they're really great to get a real quick feel of what's occurring and our folks typically say you can look at the first three pages.

242

00:35:25.590 --> 00:35:34.770

karen.grosset: And go from there to understand what's happened on your network in the last three days. So we've got some graphics, which are great. And then again, some high level findings.

243

00:35:35.730 --> 00:35:45.510

karen.grosset: That we may eat. We want to point out to you if we haven't already called you if it's something that's putting you at risk. Now a daily reports are great for compliance.

244

00:35:46.290 --> 00:35:52.500

karen.grosset: We do know that a lot of our customers, especially schools are getting written up for data security.

245

00:35:53.340 --> 00:35:59.880

karen.grosset: You know, maybe not having enough of it or not doing due diligence. So the reports are great. You can provide those to auditors.

246

00:36:00.240 --> 00:36:06.180

karen.grosset: Or anybody else you need to, and they can quickly see yes you're doing your due diligence when it comes to data security.

247

00:36:06.570 --> 00:36:19.020

karen.grosset: And we not only offer the daily reports we have monthly reports as well. And we recently also started monthly management reports. So these are less for the IT side of house and more for department has

248

00:36:19.560 --> 00:36:34.320

karen.grosset: To be able to see the benefits of Tyler detect, you know, especially when those budget reviews come up and they say, Okay, what are we getting out of this service. Why are we paying this and you can provide those reports and they can see. Oh gosh. Wow, you know, they've they've helped us

249

00:36:35.340 --> 00:36:43.230

karen.grosset: Avert some maybe some Trojans are some malware and also help us shore up our system as well and button things up to keep it secure.

250

00:36:44.190 --> 00:36:53.310

karen.grosset: And this is a table of contents of the daily reports, just so you can get a good view of how extensive and comprehensive our monitoring is

251

00:36:53.940 --> 00:37:06.720

karen.grosset: Like I said from the firewalls down to the end user machines office 365 now Microsoft 365 we seen a ton of compromised accounts on there lately, and we can quickly detect those

252

00:37:07.530 --> 00:37:14.070

karen.grosset: You know his, his phone. So logging in from Nigeria, because we've just seen that activity and will call the

253

00:37:14.370 --> 00:37:23.220

karen.grosset: Customer and they'll say no, that person sitting right across from me right now. And they'll say, well, the accounts been compromised, you need to shut that down and reinstate it

254

00:37:23.910 --> 00:37:31.350

karen.grosset: So in the feedback we get as well as that folks are really impressed with the comprehensiveness of what we are monitoring, especially for

255

00:37:32.070 --> 00:37:42.660

karen.grosset: The price so good cost effective way to make sure everything's being monitored. Now I mentioned this a little bit before you also have real time alerts with the system.

256

00:37:43.680 --> 00:37:52.680

karen.grosset: So I mentioned, if we find and detect malware we're reaching out by phone and calling you right away to make you aware of what's occurring on your network.

257

00:37:52.980 --> 00:38:00.240

karen.grosset: Because we want to keep that contain as quickly as possible. So we'll have details for you of where the infiltration occurred.

258

00:38:00.780 --> 00:38:04.260

karen.grosset: Which machines are impacted and the best way to remediate that

259

00:38:05.010 --> 00:38:15.180

karen.grosset: If you think to yourself, Well, if it's two in the morning and you're calling me with malware on my system. It's going to take me a while to to wake up and get access to my network and be effective.

260

00:38:15.480 --> 00:38:24.510

karen.grosset: In containing that is that just something Tyler can do automatically. And the answer is yes, you can authorize us to disable infected Windows machines.

261

00:38:25.140 --> 00:38:34.380

karen.grosset: When we do confirm malware. So the we will do that and will still make you aware of what we've done and what's occurred on your network, we can go ahead and

262

00:38:34.980 --> 00:38:43.350

karen.grosset: isolate those infected machines for you at any time of day so that we're keeping things contained as soon as possible.

263

00:38:43.950 --> 00:38:51.210

karen.grosset: But there might be other events that occur on your network that you want to know about before the next day's DAILY Report.

264

00:38:51.660 --> 00:38:58.320

karen.grosset: Maybe if someone's creating new users at a firewall level or if there's excessive account lockout

265

00:38:58.980 --> 00:39:04.740

karen.grosset: You can customize which alerts you want to have and also set thresholds for those as well.

266

00:39:05.400 --> 00:39:15.780

karen.grosset: You know, if it occurred. Once you don't necessarily need to be alerted on that. But if it's occurring 10 times in a row. Yes. I want to be made aware of that behavior. Give me those details as quickly as possible.

267

00:39:16.710 --> 00:39:22.230

karen.grosset: So customizable customizable alerts are really great to be able to manage your network.

268

00:39:22.710 --> 00:39:31.110

karen.grosset: You also get ongoing support with Tyler detect and this is a dedicated support team that just works on the cyber security side.

269

00:39:31.680 --> 00:39:38.070

karen.grosset: Very different than the folks that you reach out to, if you have a question with a Tyler application like a financial application.

270

00:39:38.580 --> 00:39:45.360

karen.grosset: They just work on the cyber, cyber security side and they are available 24 seven 365 days a year.

271

00:39:46.140 --> 00:39:58.260

karen.grosset: hate to say it a little different from the support team that you're you're used to, as well, but they are available around the clock during normal business hours, you will be assigned a technician that you can reach out to directly

272

00:39:59.010 --> 00:40:04.410

karen.grosset: But let's say it's eight o'clock and you're just sitting down to read today's DAILY Report and you have a question on there.

273

00:40:04.740 --> 00:40:13.620

karen.grosset: You can reach even call through on the 800 number and they'll reach right back out and go over that question with you. And we also have a great online portal.

274

00:40:14.550 --> 00:40:24.510

karen.grosset: That I want to bring up and show you how that works. So the portal is a great way. In addition to the reports for us to get information out to you.

275

00:40:24.840 --> 00:40:33.810

karen.grosset: So your understand what's going on with your network and you can manage your network. And it's also a great communication tool as well. So this is the main dashboard.

276

00:40:34.350 --> 00:40:41.520

karen.grosset: Kind of the workflow will go through a peer of again communication back and forth, as well as your reports that you can access

277

00:40:41.940 --> 00:40:53.040

karen.grosset: And anything that we could put into graphical view. We've done that here as well. And you can dig into and click on to find any more any detail on this information.

278

00:40:53.850 --> 00:41:03.540

karen.grosset: So like I said, a great communication tool, especially at the beginning as we are based lining the normal day to day activity of your network will have questions.

279

00:41:04.380 --> 00:41:11.250

karen.grosset: Not necessarily anything we need to call you about and put you on edge. Oh my gosh. Detectives calling me what's wrong with my network.

280

00:41:12.600 --> 00:41:20.190

karen.grosset: We don't want to do that and set off any false alarms. We just want to get some information out to you. So we'll put questions up here within the portal.

281

00:41:20.880 --> 00:41:33.450

karen.grosset: You know, our HTTPS connection from a certain device in San Francisco expected and you can answer back here with all sorts of detailed information so that we understand the nature

282

00:41:33.900 --> 00:41:41.730

karen.grosset: Of that communication and we say, okay, that, you know, it's okay, from your side of the house. We understand that's a Dropbox for banking files.

283

00:41:42.150 --> 00:41:52.860

karen.grosset: And we baseline that behavior and we don't ask you about it again now at the beginning again as we're getting a feel for what's normal on your network, which takes about two weeks for us.

284

00:41:53.280 --> 00:42:06.360

karen.grosset: We'll there'll be quite a few questions here. We try to only post a maximum of 10 a day. And then as we after a couple weeks as we do know. We know what looks normal on your network. These questions will drop down quite a bit.

285

00:42:07.650 --> 00:42:15.720

karen.grosset: Now we'll post the findings from the reports in here as well. If there was malware, we would have already reached out to talk to you about that real time.

286

00:42:16.260 --> 00:42:27.480

karen.grosset: But other things that come up. Maybe we've discovered a new VPN device on your network that we've never seen before. This is a great way for us to put that information out there and again for you to respond back

287

00:42:28.230 --> 00:42:40.920

karen.grosset: We recently outsource one of our applications to be cloud hosted this VPN is for secure communication with that it's going to stay on our network. So again we baseline it and we don't have to ask you about that again.

288

00:42:42.150 --> 00:42:56.760

karen.grosset: Now the reports are all easily read right here online, you can just click right on a report to bring that up in PDF view you can save these forward these email them print them whatever you need to do.

289

00:42:57.930 --> 00:43:01.020

karen.grosset: For your use on the reports.

290

00:43:02.070 --> 00:43:10.410

karen.grosset: And you'll also, as I mentioned, we've got the daily monthly reports as well that management and consolidated monthly report, you'll have access to all those

291

00:43:11.430 --> 00:43:21.810

karen.grosset: Now let's say goodbye almost up the head. So we do have because we are accessing all the log files and the information and events that are occurring on your network.

292

00:43:22.440 --> 00:43:30.060

karen.grosset: We do have some great information here to present at the firewalls level in the Windows level and a lot of feedback we get from this with

293

00:43:30.570 --> 00:43:40.380

karen.grosset: Our customers say these two screens are worth it right here, because in addition to having our eyes on your network 24 seven monitoring and making sure everything's safe and secure.

294

00:43:40.860 --> 00:43:53.640

karen.grosset: You get so much information to be able to manage your network as effectively as possible and information like this like administrative changes VPN activity inbound destinations.

295

00:43:54.600 --> 00:44:02.010

karen.grosset: Administrative failed logins or account lockout that really helps with managing information and managing the network.

296

00:44:03.090 --> 00:44:15.330

karen.grosset: Now, if for any reason. I call this the detective screen if you needed to go back and filter through some log files, you can do that here you know maybe you want to select all the firewall logs that have

297

00:44:16.440 --> 00:44:22.860

karen.grosset: Been on the system for the past year, you can do that and create a report and they'll all be listed here for your review.

298

00:44:24.180 --> 00:44:34.080

karen.grosset: VPN locations is great. Everyone always says they like maps. So this is probably very, very active for people these days as people are working remotely.

299

00:44:34.980 --> 00:44:47.400

karen.grosset: Maybe nobody in China. But if somebody does happen to be traveling on vacation, maybe, and they were at a conference and they brought their laptop, you'll be able to see that activity here within the VPN map.

300

00:44:48.780 --> 00:44:58.620

karen.grosset: I'm going to skip ahead to system health. So with the collection servers have speak to the installation we do require some collection servers. And you can see how those

301

00:44:59.100 --> 00:45:14.130

karen.grosset: Are doing within the status and the health there and then will allow you some threatened talent as well, like I mentioned, there's strength in numbers. So the more networks that were monitoring the better we are at finding

302

00:45:14.940 --> 00:45:24.000

karen.grosset: deviant behavior and really based lining normal behavior. So we see things that stand out better. And we not only are monitoring municipal networks.

303

00:45:24.540 --> 00:45:31.590

karen.grosset: But we do we work in the banking industry as well as the healthcare industry, which have very stringent guidelines.

304

00:45:32.520 --> 00:45:43.320

karen.grosset: So again, working across industries really helps us see a lot of activity that's going on out there to be able to help you stop things in their tracks as quickly as possible.

305

00:45:44.010 --> 00:45:58.470

karen.grosset: And then finally the settings is where you can just have defined, you know, things like the different types of alerts that you want to be made aware of with thresholds, etc. So it's really how you administer the portal.

306

00:46:01.500 --> 00:46:03.060

karen.grosset: So going back

307

00:46:06.210 --> 00:46:18.060

karen.grosset: Mentioned the portal and our support, so we know there are a lot of different vendors out there with cyber security solutions, but we do feel that Tyler's tact as a step above

308

00:46:18.510 --> 00:46:25.830

karen.grosset: A lot of them, most of them really the fact that we are so proper offensive and what we're monitoring, we are looking at the entire network.

309

00:46:26.160 --> 00:46:32.700

karen.grosset: That really helps us get a good feel of the day to day activity and helps any anomalies really stand out.

310

00:46:33.360 --> 00:46:42.150

karen.grosset: The fact that we have human eyes on your network 24 seven. In addition to our automated tools really helps us quickly pinpoint any anomalies.

311

00:46:42.630 --> 00:46:53.130

karen.grosset: And experience experts, you know I mentioned again strengthen numbers, the more customers that we're monitoring the better we are at really weeding out any suspicious activity.

312

00:46:54.180 --> 00:47:01.920

karen.grosset: So I'm winding down and I know it's really critical timing so that folks can get set up for the next session. So just a couple more minutes.

313

00:47:02.460 --> 00:47:07.470

karen.grosset: I'll let you read the quotes. But I think you'll get a feel from a lot of our existing customers.

314

00:47:08.280 --> 00:47:19.650

karen.grosset: The two big feedback that we get our yes we can sleep easily at night now knowing that we've got a team of cyber security experts monitoring our network 24 seven

315

00:47:20.340 --> 00:47:33.390

karen.grosset: That's really the big reasons that a lot of folks jump into this because they just don't have the resources, the time, the expertise on their end so they put that in our hands and we're very effective at finding anything that puts them at risk.

316

00:47:34.470 --> 00:47:42.810

karen.grosset: But then the other big takeaway is folks come back and they say, you know, we didn't know what we didn't know. We weren't aware that we had ports opened

317

00:47:43.140 --> 00:47:58.470

karen.grosset: All over the place, we weren't aware that we were allowing access to all these unauthorized users. So it really helps them get a good understanding of their network and go back and make actionable items to keep things as secure as possible.

318

00:47:59.970 --> 00:48:08.550

karen.grosset: So the installation. I always say it's going to be the easiest thing you ever install from Tyler technologies and feedback is is in agreement with that.

319

00:48:09.390 --> 00:48:17.730

karen.grosset: It's a just a subscription with service with an installation that we really do the heavy lifting on. We do have you spin up some collection servers.

320

00:48:18.210 --> 00:48:23.310

karen.grosset: So that we can transfer the log files securely from your system over to our sock.

321

00:48:23.700 --> 00:48:34.140

karen.grosset: And then we asked for about 60 minutes of somebody times is familiar with the network so that they can open up and have log sending our way and it's really we're using Sussman and sis logs.

322

00:48:34.650 --> 00:48:46.530

karen.grosset: For the law collections. And then we finished up the heavy lifting on our side of the house. And once we've done that day of installation within a day or two, you getting your first reports and you have access to the portal.

323

00:48:46.830 --> 00:48:56.970

karen.grosset: We'll do a follow up training with you to make sure folks understand you know what they're looking through looking at through the reports and how to use the portal to get the most out of it.

324

00:48:58.590 --> 00:49:09.780

karen.grosset: We also because sage started back in 2002 and really had been providing cyber security services before cyber security was even a term and they take it very, very seriously.

325

00:49:10.110 --> 00:49:19.410

karen.grosset: And they literally have a life cycle and a maturity process of security and can offer different services like penetration tests.

326

00:49:21.330 --> 00:49:34.350

karen.grosset: vulnerability assessments, even just starting with a cybersecurity resilience assessment. A lot of people like that, if they're just jumping into getting up to speed with cyber security. So we really have a lot to offer on that side as well.

327

00:49:35.880 --> 00:49:41.790

karen.grosset: So I'm not quite sure if Michael we have any time for questions or not, or if any of them post

328

00:49:42.450 --> 00:49:45.090

karen.grosset: If any of them post and I'm happy to answer them.

329

00:49:45.630 --> 00:49:51.540

Famis Florida4: We have a. We have a few more minutes. There were no questions in the chat if anybody has a question.

330

00:49:52.440 --> 00:49:59.370

Famis Florida4: dump it into the chat there and I'll pass it on actually will all be able to see it, but as it stands now.

331

00:50:01.650 --> 00:50:07.440

Famis Florida4: There's no questions in the chat to, um, so how many education customers. You guys have

332

00:50:10.530 --> 00:50:10.740

Famis Florida4: Sure.

333

00:50:11.010 --> 00:50:15.990

karen.grosset: Oh, that's a good question. I'm say because

334

00:50:17.010 --> 00:50:18.480

karen.grosset: Oh, I'm sorry. Can you hear me.

335

00:50:18.570 --> 00:50:21.000

Famis Florida4: Yes, can now. Yeah, okay.

336

00:50:22.170 --> 00:50:23.250

karen.grosset: Oh, okay.

337

00:50:24.810 --> 00:50:37.620

karen.grosset: So on the education side since we've spun up the text, you know, and offered it on our for our public sector. I'm going to say we've got about two dozen. Okay. And it's really good getting

338

00:50:38.370 --> 00:50:47.310

karen.grosset: Up and running in and it's always interesting because the students pose their own little quandary, if you will, with their devices.

339

00:50:48.030 --> 00:51:01.290

karen.grosset: We can we can monitor all their devices. We can actually if there's a way to filter those out. Most people do want those filtered out, just FYI, because we'll spend a lot of time on our side monitoring that activity.

340

00:51:01.710 --> 00:51:12.360

karen.grosset: And then we report on that and the IT folks on the school side, say, you know what, that's great information, but we have no jurisdiction over what they go out and do anyway so

341

00:51:12.750 --> 00:51:24.360

karen.grosset: So most of our school customers do go ahead and just filter out the student device activity. Anyway, knowing that you know on the administrative side if anything were to get through. We're finding all that

342

00:51:24.960 --> 00:51:31.890

karen.grosset: And I'm happy to say, you know, we're finding things time like you know pops on one is programs Trojans

343

00:51:32.640 --> 00:51:42.780

karen.grosset: All sorts of stuff, a lot of office Microsoft 365 compromises, like I mentioned, but we do such a good job. We are so thorough with so comprehensive we find things

344

00:51:43.470 --> 00:51:57.330

karen.grosset: You know as soon as they occur that none of our customers have ever had an event and you know really been taken down by malware or anything like that. So our success rate is 100% and do exactly what we need to do. Okay, and

345

00:51:57.840 --> 00:52:01.740

Famis Florida4: For any of you guys who are in my security session before this.

346

00:52:03.030 --> 00:52:08.760

Famis Florida4: I am I have to be vendor agnostic, but I do recommend I did recommend that

347

00:52:10.080 --> 00:52:11.280

Famis Florida4: Districts without

348

00:52:12.360 --> 00:52:22.230

Famis Florida4: Security as a service, look into it. So you guys would be one of the things that I was talking about last session about

349

00:52:23.850 --> 00:52:34.110

Famis Florida4: Districts. You just, you can't monitor your own network 24 seven so so Tyler tech here is is another option to add to your list if you're looking at

350

00:52:36.240 --> 00:52:39.450

Famis Florida4: The different ones. If you're looking at for internet or or

351

00:52:41.160 --> 00:52:59.880

Famis Florida4: Dell secure works or anything like that, go ahead and add Tyler tech to your list and and as you look into it. Does anybody else. I see Adam has a question, but it's more about funding so anybody who can ask that might want to respond back to Adam.

352

00:53:01.080 --> 00:53:07.200

Famis Florida4: About grant funding and stuff. Anyone else before we spin the big wheel.

353

00:53:08.550 --> 00:53:09.300

Famis Florida4: So,

354

00:53:10.530 --> 00:53:12.690

Famis Florida4: Okay, so if

355

00:53:12.750 --> 00:53:14.040

karen.grosset: I'm not mistaken.

356

00:53:14.280 --> 00:53:15.510

Famis Florida4: You guys have

357

00:53:17.340 --> 00:53:19.230

Famis Florida4: You guys are giving away.

358

00:53:20.250 --> 00:53:23.820

Famis Florida4: A GIFT CARD. Correct. Is that you, Jim.

359

00:53:26.670 --> 00:53:27.000

Hold on.

360

00:53:29.730 --> 00:53:31.320

Famis Florida4: Just Mike. Somebody must have stepped

361

00:53:31.320 --> 00:53:32.580

Famis Florida4: Away, Karen, you guys.

362

00:53:33.570 --> 00:53:34.590

Famis Florida4: Let me make sure I got the right

363

00:53:34.740 --> 00:53:36.900

karen.grosset: To strengthen me. There you go.

364

00:53:38.010 --> 00:53:38.280

Famis Florida4: Yeah.

365

00:53:38.340 --> 00:53:41.760

jim.ash: There's $100 amazon gift card.

366

00:53:42.090 --> 00:53:42.990

jim.ash: Okay, and

367

00:53:44.190 --> 00:53:46.410

jim.ash: Whoever the wheel predicts or

368

00:53:46.440 --> 00:53:48.660

jim.ash: Okay, it's too. We will email that

369

00:53:49.020 --> 00:53:50.460

jim.ash: Information to them down so

370

00:53:50.850 --> 00:53:52.560

Famis Florida4: Good, though. What we're gonna do is

371

00:53:52.800 --> 00:53:54.870

Famis Florida4: We're going to spend twice because we have a

372

00:53:55.980 --> 00:54:00.480

Famis Florida4: We have $100 gift card which will spend for first

373

00:54:01.650 --> 00:54:08.220

Famis Florida4: The, the list is closed. I've got everyone's name I pulled it off of the list here, I'll, I'll spin the wheel here in a second.

374

00:54:10.350 --> 00:54:24.660

Famis Florida4: And. And then the second spin will be for the bluetooth speaker. I'm going to go ahead and take over your screen. Make sure if you win the first one you get in touch with the folks at Tyler tech and let, let me go ahead and share my screen here.

375

00:54:25.980 --> 00:54:28.020

jim.ash: So this will stop. Other people cheering

376

00:54:29.310 --> 00:54:29.730

You go

377

00:54:30.780 --> 00:54:35.880

Famis Florida4: Okay, and we're going to spend this if y'all can see y'all see a wheel.

378

00:54:36.900 --> 00:54:37.470

Famis Florida4: You see the wheel.

379

00:54:37.500 --> 00:54:38.520

Famis Florida4: Yes. Okay.

380

00:54:39.600 --> 00:54:40.080

Famis Florida4: All right.

381

00:54:42.780 --> 00:54:59.670

Famis Florida4: To you. And the winner is. It's funny, I couldn't get rid of that one. We're going to go ahead and again we have a winner. It's nobody else. You know, I thought, Man, I can't get rid of that line. What's the odds of it landing on that line we're one in however many people are here.

382

00:55:00.900 --> 00:55:05.160

Famis Florida4: Okay, Jim. Are you there. Hold on, let me unmute Jim

383

00:55:10.320 --> 00:55:10.740

Jim

384

00:55:12.090 --> 00:55:12.450

Famis Florida4: Right.

385

00:55:14.760 --> 00:55:18.780

Famis Florida4: He's hopefully he's there because he won $100 gift card and

386

00:55:19.380 --> 00:55:20.160

Scantlin: You might hear me.

387

00:55:20.490 --> 00:55:21.360

Famis Florida4: Yes, Jim.

388

00:55:23.610 --> 00:55:29.070

Famis Florida4: Congratulations, you are the winner of the $100 gift cards. You have to get with with

389

00:55:30.180 --> 00:55:34.470

Famis Florida4: Jim there ash actually at Tyler tech you wanted to email you

390

00:55:34.920 --> 00:55:39.510

jim.ash: Yes, Jim. Jim ash ash at Tyler tech.com

391

00:55:40.080 --> 00:55:40.740

Scantlin: When we

392

00:55:40.860 --> 00:55:42.090

Scantlin: Start up start over again.

393

00:55:43.710 --> 00:55:44.820

jim.ash: Jay, I am

394

00:55:45.840 --> 00:55:46.860

jim.ash: A sh.

395

00:55:47.280 --> 00:55:48.570

Scantlin: Okay, Tyler tech

396

00:55:49.680 --> 00:55:49.980

Tech.

397

00:55:52.380 --> 00:55:54.660

Famis Florida4: It'll be it'll be another gym there so

398

00:55:55.500 --> 00:55:55.830

Scantlin: Thank you.

399

00:55:56.310 --> 00:56:04.410

Famis Florida4: Okay. And then for the second one, Jim, if it lands on your name again we're going to spend it again. You only get one one prize. I think I can take me

400

00:56:06.120 --> 00:56:16.800

Famis Florida4: I've been adjusting this list, the whole time. It's like you had to be here. Most of the time to get on this list. Okay. And I saw we get rid of that point. But here we go. This is for the bluetooth speaker.

401

00:56:18.570 --> 00:56:24.120

Famis Florida4: If you do it, don't do do do do do do and what are the odds of that.

402

00:56:24.450 --> 00:56:25.710

Famis Florida4: Because again,

403

00:56:27.750 --> 00:56:31.080

Famis Florida4: I love the little clapping. If I don't know if you guys can hear my speaker.

404

00:56:32.940 --> 00:56:43.110

Famis Florida4: This is going to be. Jeff, are you know now it's Elizabeth Oh my god, Elizabeth. I know you're here. I'm going to unmute you.

405

00:56:44.550 --> 00:56:51.600

Famis Florida4: Oh, you're here. Oh, yeah. You're not even muted okay you and for you. You are going to have the email.

406

00:56:52.860 --> 00:56:57.240

Famis Florida4: Somebody else sorry this is this is actually my first presentation.

407

00:56:57.540 --> 00:57:02.460

Famis Florida4: I have. Okay. You do. All right. And you've won the bluetooth speaker so

408

00:57:03.060 --> 00:57:05.910

Famis Florida4: That's it for today, if nobody else has

409

00:57:05.910 --> 00:57:14.040

Famis Florida4: Anything, we'll go ahead and call it a day. And thanks. Tyler tech thanks for your, your participation and famous. We really appreciate you guys

410

00:57:15.330 --> 00:57:15.870

jim.ash: Thank you.

411

00:57:16.260 --> 00:57:17.910

Famis Florida4: Okay. Have a great day. Take care.

412

00:57:18.660 --> 00:57:19.140

jim.ash: Bye bye.