CASE STUDY

Solutions Granted Powers Intelligent SOC with Stellar Cyber Open XDR

Stellar Cyber Open XDR Platform Grants New Threat-Hunting Powers for Virginia MMSSP

Solutions Granted, Inc. is a Master Managed Security Services Provider (Master MSSP) based in Virginia. It offers information security solutions to MSPs and MSSPs through monthly service agreements that are consumption-based with no minimums or contracts. Today, the company has more than 500 MSP partners, each of which has 30-50 customers, and it manages more than 100,000 endpoints using the Stellar Cyber platform.

The company has built its rapidly-growing business around three key strengths:

- People – trained security experts who work collaboratively with partners
- Process – game-changing processes
- Technology – managed controls that protect, detect, and respond to ever-changing threats

SOLUTIONS GRANTED
PROTECTING THE PROTECTORS

"Everything is very streamlined in the Open XDR platform – it took less than one business day of training for me to set it up and match our focus to work the way we wanted it to. With our previous system, it took over a week before I could figure out what I was doing."

BEFORE

Restricted

other SIEM didn't allow access to back-end log data

Time Wasted

learning curve wasted valuable time

Costly

per-endpoint model wasn't cost efficient

WITH STELLAR CYBER

Accessibility

access syslogs and back-end data

Streamlined

easy to use, quick setup

Customer Service

Stellar Cyber response to feedback is unequaled

Multi-Tenancy

makes it simple to onboard new clients

> " Being able to access syslogs and all the back-end data allowed us to create our own alert mechanisms. IOCs change all the time, and a static solution won't allow us to evolve with new threats and take some form of remediation. Stellar Cyber did.

STELLAR CYBER®

Upgrading the SOC Platform

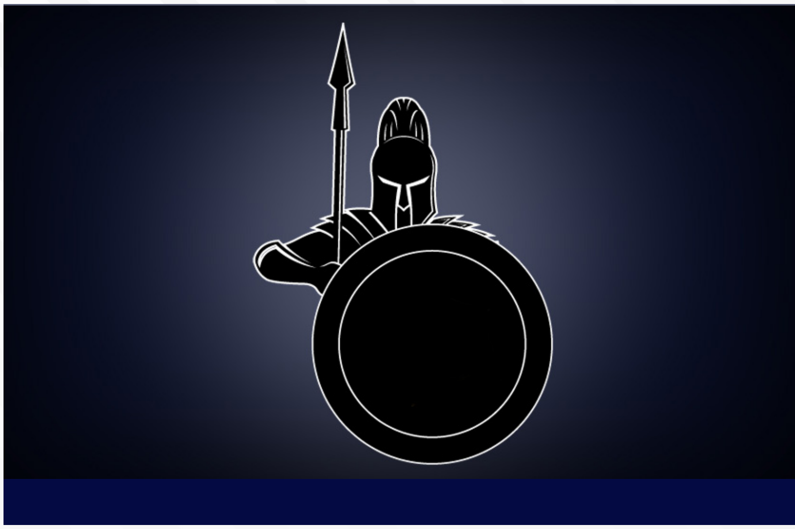
Solutions Granted does much of its work by examining Windows event logs, firewall logs, and syslogs to spot and identify incidents of compromise (IOCs), but the first SOC platform it tried wasn't giving it access to the data it needed to see.

"The platform we were using gave us the bare necessities of running a SOC, but we were restricted from accessing the back-end log data that allowed us to really delve into problems," says Cory Clark, Director of Threat Intelligence at Solutions Granted. "When we tried Stellar Cyber and dumped log data into it, we saw what we could be and what we wanted to be. Being able to access syslogs and all the back-end data allowed us to create our own alert mechanisms. IOCs change all the time, and a static solution won't allow us to evolve with new threats and take some form of remediation. Stellar Cyber did."

Another big difference between its legacy platform and the Stellar Cyber platform was Stellar Cyber's ease of use. Says Clark, "Everything is very streamlined inside the platform – it took less than one business day of training for me to set it up and match our focus to work the way we wanted it to. With our previous system, it took over a week before I could figure out what I was doing."

Stellar Cyber's built-in multi-tenancy was another key factor in the decision. Clark calls it a "firm requirement" and it's easy to see why with more than 500 partners to manage. Moreover, any reservations Clark and his team had about switching platforms were completely eliminated when they saw how responsive the Stellar Cyber team was. "I'm not the easiest person to work with when I'm evaluating a product – I'll tear it apart," says Clark. "Since Day 1, the Stellar team has absorbed my barrage of complaints and recommendations and handled them. My asks or recommendations come out in the next version of the product. The Open XDR platform is great, but the response I've gotten from the Stellar team is unequaled."

> "The Open XDR platform is great, but the response I've gotten from the Stellar team is unequaled."



Open XDR: Zeroing In on Attacks

Since many attacks target Microsoft 365 (MS 365) applications, Solutions Granted's partners were especially asking for protection from those. With Stellar Cyber, the team was able to use built-in MS 365 analytics to get automated alerts, but it also used the platform's automation tool to build queries. "For example," says Clark, "in MS365, it took me about 15 minutes to set up an alert for when someone is added as an administrator. What's even better is that once I report that I've created a new alert to Stellar Cyber, they improve the product by building an automated alert for that situation."

Over the last 2.5 to 3 years, spear phishing attacks have increased rapidly. Hackers target users' personal email accounts and use them to gain access to an enterprise's data. For example, a phishing attack will contain a link to a Google Drive file, which, when downloaded, takes over the user's account and starts exporting data from the corporate server. "We want to be able to attack those account takeovers and remedy them quickly," Clark said.

Hackers know now that they need to stage IOCs because it's harder to identify them. The Emotet malware variant is one example. The Solutions Granted team found a new strain of Emotet, which uses fake PO or invoice files to infect systems. "Emotet was our number one pain point last year, and we saw an article that said it was going to have a resurgence this year. We were able to use the Stellar Cyber platform to start seeing it. We could start identifying who is opening certain files and identifying Emotet campaigns that roll out over time. It used to be a compromised EXE file, but now we can see the type of script being run, who is downloading and extracting data – we can do all that through simple queries with Stellar."

Docusign is another example. "One of our SOC analysts saw an IOC coming in through a Zip file attacking personal emails customers were using on a machine. It comes through a link to a Google drive, downloads the Zip file, and then starts executing a script. We were able to identify and stop three instances of this in less than 24 hours, and we found them 24-36 hours before news of this attack even hit the media."

Of course, IOCs evolve constantly, and there are certain IOCs that can't be automated. For these situations, Solutions Granted uses log analysis to spot attacks. For example, if a file is saved into the root of certain directories, it's unusual because that's not where data is normally saved. "We're actively threat-hunting on every shift and finding things within 24 hours that would have gone unnoticed for weeks or months," said Clark.

Future Enhancements

Based on its success with the Stellar Cyber platform so far, Clark and his team plan to ingest as much data into it as they can. "We are going to get firewalls ingested into Stellar – I want to get more server logs, desktop logs," says Clark. "I want to start using the Stellar kill chain. I want as much information in there so we can identify as many IOCs as possible. The more data we can look at, the more successful we are."

In addition to pleasing its hundreds of partners and their customers, Solutions Granted has improved its business case by using the Stellar Cyber platform. Says Clark, "The ingestion model we have with Stellar is proving to be more profitable than the per-endpoint model we had with our previous provider."

Thanks to the Open XDR platform, Solutions Granted is serving its large customer base with better threat detection and faster responses to IOCs. The platform's purchase model is also making the company more profitable, but that's just the icing on the cake.

> "The ingestion model we have with Stellar is proving to be more profitable than the per-endpoint model we had with our previous provider."