CASE STUDY

Deeptree Delivers Comprehensive Security Services with Stellar Cyber

With Stellar Cyber, Deeptree Can "See More, Know More, Act Faster"

Headquartered in Alaska with offices in Montana and Puerto Rico, Deeptree is a managed detection and response (MDR) provider that offers cyber defense, recovery and resilience services to customers across the United States. Deeptree prides itself on offering holistic, tailored security services to companies in finance, healthcare, education, manufacturing and other sectors, combining the expertise of an enterprise-class security player with the service dedication and agility to make white-glove services available to companies of all sizes. Central to its security package, Deeptree uses the Stellar Cyber Open XDR (eXtended Detection and Response) platform to deliver world-class cybersecurity services to its clients with a focused team of analysts.

CHALLENGE: DELIVERING TAILORED SERVICES TO EVERYONE

During the COVID-19 pandemic, companies have turned more to remote workforces to get the job done. And as expected, this has broadened companies' cyber attack surfaces. With staff members predominantly using the corporate VPN, network access control and user/entity behavior analytics, in addition to standard defenses, are essential to defense. Workers aren't protected solely by the corporate systems anymore and the level of security at home is highly variable. Achieving a comprehensive view of the network is instrumental in defending the organization's assets and value streams during the pandemic. This is true no matter how large or small one's office is.

"We know that cyberattacks are twice as likely to occur in America as anywhere else and customers need a security partner with the expertise to protect their entire attack surface and who can dispatch to their location, no matter where it is," said Peter House, CEO of Deeptree. "We offer tailored, enterprise-class security services to everyone. That's the advantage of partnering with

> "We want to offer enterprise-class security services to everyone."

Stellar – scalability means scaling up or down. And offering enterprise class security to enterprises and their smaller partners alike means total coverage. When designing our

offering a criticism leveled at one operator was that some clients felt too small to matter. For our clients, we operate as white glove is white glove as long as you're a client. The difference is in quantity not quality."

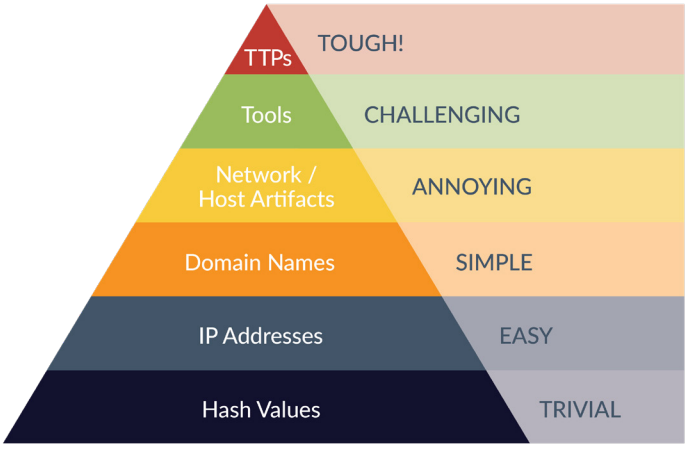
> "We knew that just acquiring a bunch of siloed security tools would leave us with difficulty correlating detections across tools, so we wanted a comprehensive security platform that integrated all of the important tools and allowed us to integrate others to meet the needs of specific customers."

CHOOSING A SOLUTION

The selection process for a central tool for its Security Operations Center meant that it needed to bypass the vices of current solutions. According to House, "We knew that just acquiring a bunch of siloed security tools would leave us with the problem of correlating detections across tools. That drives up operating costs and slows down process – leading to delayed response times. So we needed a comprehensive, best-in-class security platform that integrated all of the important tools and allowed us to integrate others as needed to meet the needs of specific customers. Healthcare and finance are two very different industries, so they need different tool sets. Stellar gives us the ability to meet those varying needs and still have a single pane of glass."

After evaluating major SOC vendors and finding them lacking features or being too restrictive when it came to integrating new capabilities, the Deeptree team found Stellar Cyber. The Stellar Cyber platform was an ideal fit for Deeptree because it integrates key security capabilities under one interface – including UEBA, EDR, NTA and SIEM – and it has open APIs that allow it to easily integrate with third-party firewall, IDS, SIEM and other systems.

In addition, the Stellar Cyber platform leverages AI and machine learning technologies to automatically correlate detections to spot and evaluate potential threats. It delivers far fewer false positives, allowing Deeptree's team of analysts to be far faster and more productive at finding and remediating complex attacks. With Stellar, Deeptree is able to operate at the top levels of the Pyramid of Pain, which have proven very difficult to address.



The Pyramid of Pain, originally developed by David Bianco: http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

A VIRTUAL BOUNCER

"The Internet is porous," says House. "With a firewall, it's not like you're not behind a castle wall. It's more like operating a bar with a thousand doors. There's a team of bouncers and they gotta check everybody and their entourage. This is especially so with COVID and remote workers. You need a virtual bouncer that sees everything and can react quickly. To catch malware in a lie – you need to look at it through viewpoints. That's the Stellar difference – multiple viewpoints. Single pane of glass."

DEEPTREE

UEBA is a cornerstone for this type of threat detection, and it's tied to NTA because network traffic reveals attacks other systems miss. Stellar Cyber's NTA and UEBA capabilities deliver insights that analysts can't see with a SIEM that simply analyzes logs. In one spear-phishing attack, for example, the malefactor knew a teacher and her students' names, and sent an email supposedly from another teacher. Using Stellar Cyber, Deeptree detected this ruse and responded immediately.

"Because we have a low footprint in terms of detection, we can be much faster and better at responding," says House. "Ira Winkler said it best, 'Protection will eventually fail, no matter what' – so one's ability to respond is crucial. It's what separates amateurs from professionals."

With Stellar machine learning driving the heavy lift of log processing, Deeptree professionals are able to focus on differentiating value. One such example is memory forensics. "We proudly use Volatility at Deeptree. And all operational staff, including Tier I technicians, receive memory forensics training. In one case, Stellar alerted us to a series of Event ID 4656 being a generated on a client host. As you know, this is one of the EIDs in the cluster that Mimikatz will generate. In under an hour, we were able to move from alert to clearing the running process as legitimate."

LOOKING AHEAD

Thanks to Stellar Cyber's Open XDR platform and its open APIs, House feels he can use it as a central core around which he can build tailored security services for specific types of customers. This also expands Deeptree's market because it can identify new segments and add value for them by cost-effectively integrating new tool sets. "Because we have Open XDR, we now feel confident we can build extended tools and integrate them into Stellar Cyber to meet new needs. This gives us forward looking confidence both from the perspective of the ever-evolving space that is cybersecurity but also to changing market needs." says House.

"I forecast that Stellar Cyber will be the major competitive differentiator for us because it allows us to see more, know more, and act faster than our competition."

House sees Stellar Cyber as a key to his growth and success because of its ability to integrate new tools and to spot and thwart attacks that other systems don't see. "I forecast that Stellar Cyber will be the major competitive differentiator for us because it allows us to see more, know more, and act faster than our competition."