Selling with the Bulls: USF System Fall 2022
Networking, Prospecting, Needs, and Customer Conversations

ReliaQuest Commercial Account Executive

RELIAQUEST

ReliaQuest's GreyMatter is a cloud-native security operations platform that is delivered as a service any time of day, any place in the world. Built on an Open XDR architecture it offers bi-directional integration across any vendor solution, whether on-premises or in one or more clouds, to ingest data and automate actions. It brings together telemetry from any security and business solution to deliver singular visibility across the enterprise ecosystem and unifies detection, investigation, response, and resilience, so organizations can accelerate incident response and manage cyber risk better. Hundreds of Fortune 1000 organizations trust ReliaQuest GreyMatter to operationalize security investments to focus teams on the right problems, close visibility and capability gaps to proactively manage risk and accelerate initiatives for the business. ReliaQuest is a private company headquartered in Tampa, Fla., with multiple global locations. For more information, visit www.reliaquest.com

A recent study of more than 400 security decision makers at large enterprises confirmed the critical gap ReliaQuest fills for its customers. The report found that enterprises, in an effort to protect themselves, have implemented numerous security tools and technologies. However, 71% say they have added tools faster than they can productively use them while 69% now spend more time managing the tools than effectively defending against threats. Even with all this effort, a majority of enterprises say their security posture has not improved and they do not have confidence their systems and processes will be resilient in the face of an attack.

ReliaQuest's GreyMatter helps companies solve these problems by connecting the existing technology, people, and processes that enterprises rely on through a centralized SaaS platform. GreyMatter also includes the quality content, playbooks, and security expertise of world-class security operations, and the transparency and ongoing measurement that enterprises need from a trusted partner.

RELIAQUEST GREYMATTER

Acting as a force multiplier on an organization's existing cybersecurity investments, only ReliaQuest's GreyMatter security operations platform integrates disparate technologies to provide a unified, actionable view that fills the gaps in enterprise security programs. As a result, only GreyMatter can provide enterprises with true visibility; automation across the entire security workflow; and ongoing benchmarking and measurement to give enterprises the confidence needed in their security tools, programs and processes.

1. **True Visibility**

At the heart of ReliaQuest GreyMatter is the universal translator. ReliaQuest built a patented translation layer to gather and normalize data on demand from leading security technologies and cloud providers.

The company's framework integrates data from customer toolsets to give companies a single, comprehensive view across their environment. This isn't a one-time API connection. Dedicated engineers continuously map fields on a technology and source level on a per customer basis. This goes way beyond any other data bridge in the industry.

Because of this bi-directional integration and resulting visibility, GreyMatter delivers threat detection content tuned to the company's environment and mapped to frameworks like NIST, the Kill chain and MITRE ATT&CK to provide better threat coverage and enable faster threat response

With this combination of capabilities, customers experience an ROI of 350% in less than 6 months according to an independent analysis by Forrester. On average, Reliaquest customer experience 74% improved detection capabilities, 90% reduction in noise, and 30% increase in visibility. This results in reduced headcount expenses of $1.2M over three (3) years.

Attrition of experienced security analysts combined with a shortage of qualified talent is an ongoing challenge for every security organization. Visibility provided through the universal translator enables a newly hired analyst to be competent across all the security tools in their organization. This reduces ramp time of new analysts by months and force multiplies the capabilities of every analyst on the team.

2. **Automation and Unified Security Workflow**

The security workflow includes preparation (optimization of tools), detection, investigations, response, and measurement (analysis). GreyMatter unifies this workflow because of the visibility provided across what are typically disparate tools. A unified security workflow accelerates the entire process and ultimately reduces Mean Time to Respond (MTTR). A unified workflow reduces noise, enables a consistent response to investigations, and makes automation across the entire lifecycle possible.

The industry often thinks of automation only in terms of response. But ReliaQuest looks for opportunities to automate across the security lifecycle.

In addition to automating the data collection stage to speed investigation, GreyMatter contains several pre-built playbooks across commonly detected events and use cases to help your team confidently automate in line with your standard operating procedures.

And ReliaQuest is applying automation in yet another way. ReliaQuest GreyMatter improves a company's security posture with machine learning-driven, automated hunts and automated attack simulations to validate security controls and systems, identify gaps and prioritize remediation based on risk to the business.

Attrition is often the result of analysts being constantly forced to complete repetitive, duplicative, mundane lengthy tasks across multiple systems to eliminate what is often a false positive alert. A

unified security workflow reduces the noise by 90% enabling the analyst to focus on important tasks rather than being buried by an unfulfilling and endless workload. The ability to automate across the entire workflow accelerates MTTR which reduces risk and operating costs.

3. **Ongoing Measurement / Model Index Process**.

An essential requirement of any security operations team is to be able to validate the effectiveness of the program, processes, tools, and people. GreyMatter is also designed to give a company the ongoing reporting and measurement to track improvements in visibility, efficacy of tools and maturity of your teams and processes. GreyMatter does this through a process called the Model Index. Model Index is unique because it gives a holistic view of the security posture since ReliaQuest has visibility across all tools. Security gaps and tool efficacy can be seen by evaluating the deployed rules/content against a security framework such as MITRE ATT&CK. Team efficiency can also be viewed over time to understand how effective the team is. Risk scenario coverage is mapped to key threats providing visibility of known risks. Finally, these results can be benchmarked across industry averages to evaluate a company to other companies in the same industry.

PROSPECT COMPANY - SUN STATE INTERNATIONAL

What is now Sun State International Trucks, LLC. (www.sunstateintl.com) originally began in the 1920s as Orange State Motor Co. The original building was on Twigg St. in downtown Tampa. When they outgrew that location in 1970, it moved to the current location on Highway 60/ Adamo Drive and became Sun State International Trucks, LLC.

By the 1980s Orange State had become Boswell International, and in the year 2000 Oscar Horton purchased Sun State International Trucks, LLC. which included two (2) locations, the Adamo Drive store, and the Sarasota store with revenue totaling $28 million. In 2003 the company opened its second Tampa location, the Aftermarket Shop. In 2005 Sun State purchased Moore International and opened the Central Florida store in Davenport, FL. In 2011 the company expanded again and became the Hyundai Translead trailer dealer for the state of Florida. In 2015 the company expanded its product offerings again and purchased the rights to be the IC Bus dealer for the state of Florida, and opened Sun State Bus Centers, as well as adding Fontaine Trailers to our product line.

In 2018 Sun State opened its first parts only store in Clearwater, FL, Sun State Truck & Trailer Parts. With the success of the first parts store and the need to better meet the ever-expanding customer base, a second Sun State Truck and Trailer Parts store was opened in Brooksville, FL in the fall of 2019.

With 2022 revenues projected to exceed $200 million and the authorized dealer for International's flagship line of products, Hyundai Translead, Globe trailers, and IC Bus, Sun State is a critical part of commerce in Florida and the southeast United States.

- American Truck Dealer (ATD) of the Year for 2020 to 2022 and recipient of Tampa Bay Business Hall of Fame
- Aftermarket Center offering truck, trailer and bus modifications and a wide range of services, from cleanings to body swaps and frame modifications
- Diamond Logic and over-the-air programming to automate performance; OnCommand Connection, the industry's only all makes/all models telematics solution to monitor fleet health; and after-hours, mobile service/preventative maintenance teams

- Member of the International Dealer Network, the industry's largest with more than 1,000 service locations in North America

YOUR PROSPECT'S OVERVIEW: SAM SMITH

- Sam Smith recently joined Sun State International as Chief Information Security Officer (CISO). Sam has a long history in the information security and was the CISO for a logistics company for three years.

SCENARIO:

You are an Commercial Account Executive for ReliaQuest and Sun State International is one of your target customers. Your digital team just notified you that Sam Smith, the CISO, registered on the web site to get access to a research white paper that noted:

- Top Pain Points for Security Operations
    - Inability to get security products to work integrate 28%
    - Governance, risk, and compliance 25%
    - Extending security controls / tools to a hybrid/ multi-cloud environment 24%
- Over 50% of Enterprises report that they spend too much time maintaining security tools (EDR: End Point Detection Reporting and SIEM: Security Information and Event Management)
- Almost 50% of enterprises report data from security tools (EDR and SIEM) is overwhelming
- 86% of enterprises report they are unable to act upon all security alerts daily
- Over half (55%) of enterprises believe they are missing logs (reports) from systems that would help security

You've also noted from ReliaQuest research that there is a:

- 400% improvement in threat detection capabilities in the first 90 days of deploying ReliaQuest capabilities.
- 98% reduction in security system downtime, accelerating threat identification and response
- 35% decrease in the total cost of ownership, due to more efficient security defenses.

The team also shared that Sam had reviewed several pages about GreyMatter on the web site. You conducted a background search and found analyst reports on the critical nature of the transportation industry and the amount of critical information about freight that is communicated between the vehicles and the systems. It's critical that Sun State is online and connected 24X7X365.

You are not an expert in trucking or transport, so you spent a few minutes working with ReliaQuest leadership to gain a better understanding of the possible challenges Sam may be facing. Here are some of the inputs:

- Companies like Sun State are valuable targets. In addition to expensive vehicles, the company has important customer, vehicle, and transportation information (like truck locations) along with multiple digital entry points.
- It is critical that a company like Sun State International is connected to its customers. Trucks communicate with the dealer network to self-report issues and navigate to repair locations.
- Companies like Sun State also have mobile apps that allow users to keep their vehicles operating as well as order parts, check inventory, and leasing.
- There is a shortage of IT security workers especially in larger companies. Turnover is the highest when the work is mundane, and the workers are chasing alarms all day and trying to integrate systems.

EXAMPLE OBJECTIONS:

- What is this going to cost Sun State International?
- Sam already knows what to do. She / He has been in the industry for years.
- Sun State has a strong relationship with its primary IT providers who provide great assistance.
- Can ReliaQuest handle the needs and critical data of a major operation like Sun State International.
- Connecting Sun State's critical systems to a third party via the cloud is a significant security risk. More connections and a single access point risks everything.

CHARACTERS:

- ReliaQuest Commercial Account Executive
- Sam Smith, CISO Sun State International

COMPETITOR ROUNDS

PREWORK ROUND 1 (PROSPECTING): Prospecting email to Sam Smith due 11:59p on 10/17/2022

Send your prospecting email to Sam Smith by 11:59p on Monday, October 17th. The goal of the email is to obtain a commitment for a short 10-minute discovery call.

NETWORKING: Meet the Employers Thursday evening 10/20/2022

The Muma College of Business School of Marketing and Innovation will host a Meet the Employers event on Thursday evening, October 20th. Competitors in Selling with the Bulls: USF System will network with company representatives. Company representatives will identify the best networking students and those students will earn points toward the Top Bull award.

Network with ReliaQuest company representatives during the Muma College of Business School of Marketing and Innovation Meet the Employers event on Thursday evening, October 20th, to obtain insights on Sam Smith and Sun State that will be assistance in building rapport for the prospecting phone call on Friday morning.

ROUND 1 (PROSPECTING): Prospecting phone call to Sam Smith, Friday morning 10/21/2022

You have been attempting to contact Sam Smith and Sam has not responded despite the interest demonstrated by Sam's time on the ReliaQuest web site. You take the initiative and call Sam in the hopes of catching her / him before the day gets underway.

The goal of the phone call is to obtain a commitment for a short 10-minute discovery meeting.

The time limit on the phone call is 5 minutes. You will make this call from the Muma College of Business Center for Marketing and Sales Innovation Customer Experience Lab.

ROUND 2 (Discovery Meeting): Web meeting with Sam Smith, Friday mid-day 10/21/2022

You contacted Sam Smith via phone and were able to set up a 10-minute conversation with Sam. This is that meeting.

The goal of this meeting is:

- To develop an understanding of Sam Smith's and Sun State's present situation along with their interest level in contracting with ReliaQuest.
- To determine the timing on Sam Smith's plans to make information technology decisions and the associated project timelines.
- To understand Sam Smith's ideal state and how ReliaQuest can help achieve that state.

- To explain what current ReliaQuest clients are experiencing and validate those similar results would meet the Sam Smith's needs.
- Close on having Sam Smith agree to a meeting where you will present a solution to address Sam Smith's needs.

ROUND 3 (Sales Close Meeting): Meeting with Sam Smith, Friday late afternoon 10/21/22

Information on what you learned during the meeting will be shared following the round.

This round will be 15 minutes.

The goal of this meeting is to:

- Explore the problems that are prompting Sam to consider a relationship with ReliaQuest
- Close on a ReliaQuest contract: Support for the entire company $100,000 per year. Three (3) year commitment and 20% discount.

APPENDIX A: SELECT CYBER SECURITY TERMS (adapted from Wikipedia)

Alarm fatigue or alert fatigue occurs when one is exposed to a large number of frequent alarms (alerts) and consequently becomes desensitized to them. Desensitization can lead to longer response times or missing important alarms. Like crying wolf, such false alarms rob the valid alarms of the value they were intended to add (duly alerting people to danger).

Analytics is the discovery, interpretation, and communication of meaningful patterns in data. It also entails applying data patterns towards effective decision making. In other words, analytics can be understood as the connective tissue between data and effective decision making within an organization. Especially valuable in areas rich with recorded information, analytics relies on the simultaneous application of statistics, computer programming and operations research to quantify performance.

Automation is the technology by which a process or procedure is performed with minimal human assistance.

A **botnet** is a number of Internet-connected devices, each of which is running one or more **bots**. Botnets can be used to perform distributed denial-of-service attack (DDoS attack), steal data, send spam, and allows the attacker to access the device and its connection. The owner can control the botnet using command and control (C&C) software. The word "botnet" is a combination of the words "robot" and "network". The term is usually used with a negative or malicious connotation.

Cloud computing is the on-demand availability of computer system resources, especially data storage and computing power, without direct active management by the user. The term is generally used to describe data centers available to many users over the Internet. Large clouds, predominant today, often have functions distributed over multiple locations from central servers.

Advocates of public and hybrid clouds note that cloud computing allows companies to avoid or minimize up-front IT infrastructure costs. Proponents also claim that cloud computing allows enterprises to get their applications up and running faster, with improved manageability and less maintenance, and that it enables IT teams to more rapidly adjust resources to meet fluctuating and unpredictable demand.

Computer software, or simply software, is a collection of data or computer instructions that tell the computer how to work. This is in contrast to physical hardware, from which the system is built and actually performs the work.

A **computer virus** is a type of **malware** that, when executed, replicates itself by modifying other computer programs and inserting its own code.

A **computer worm** is a standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it.

A **data breach** is the intentional or unintentional release of secure or private/confidential information to an untrusted environment. Other terms for this phenomenon include unintentional information disclosure, data leak, information leakage and also data spill. Incidents range from concerted attacks by black hats associated with organized crime, political activist or national governments to careless disposal of used computer equipment or data storage media.

A **denial-of-service attack** (DoS attack) is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.

In a **distributed denial-of-service attack** (DDoS attack), the incoming traffic flooding the victim originates from many different sources. This effectively makes it impossible to stop the attack simply by blocking a single source. A DoS or DDoS attack is analogous to a group of people crowding the entry door of a shop, making it hard for legitimate customers to enter, thus disrupting trade.

A **domain name** is an identification string that defines a realm of administrative autonomy, authority or control within the Internet. Domain names are used in various networking contexts and for application-specific naming and addressing purposes. In general, a domain name identifies a network domain, or it represents an Internet Protocol (IP) resource, such as a personal computer used to access the Internet, a server computer hosting a web site, or the web site itself or any other service communicated via the Internet. Domain names are formed by the rules and procedures of the Domain Name System (DNS).

An **exploit** (from the English verb to exploit, meaning "to use something to one's own advantage") is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug or vulnerability to cause unintended or unanticipated behavior to occur on computer software, hardware, or something electronic (usually computerized). Such behavior frequently includes things like gaining control of a computer system, allowing privilege escalation, or a denial-of-service (DoS or related DDoS) attack.

A **firewall** is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted internal network and untrusted external network, such as the Internet.

The term **kill chain** was originally used as a military concept related to the structure of an attack; consisting of target identification, force dispatch to target, decision and order to attack the target, and finally the destruction of the target. Conversely, the idea of "breaking" an opponent's kill chain is a method of defense or preemptive action. More recently, this concept has been applied to information security, using it as a method for modeling intrusions on a computer network.

An **Internet Protocol** address (IP address) is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication. An IP address serves two main functions: host or network interface identification and location addressing.

Malware (a portmanteau for malicious software) is any software intentionally designed to cause damage to a computer, server, client, or computer network. Malware does the damage after it is implanted or introduced in some way into a target's computer and can take the form of directly executable code, scripts, so-called "active content", and other forms of data. Some kinds of malware are largely referred to in the media as computer viruses, worms, Trojan horses, ransomware, spyware, adware, and scareware, among other terms.

On-premises software (also known as on-premise, and abbreviated "on-prem") is installed and runs on computers on the premises of the person or organization using the software, rather than at a remote

facility such as a server farm or cloud. On-premises software is sometimes referred to as “shrinkwrap” software, and off-premises software is commonly called “software as a service” ("SaaS") or “cloud computing”.

Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising oneself as a trustworthy entity in an electronic communication. Typically carried out by email spoofing or instant messaging, it often directs users to enter personal information at a fake website which matches the look and feel of the legitimate site.

Phishing attempts directed at specific individuals or companies have been termed spear phishing. In contrast to bulk phishing, **spear phishing** attackers often gather and use personal information about their target to increase their probability of success.

Proactive Hunts is the process of testing a company’s Information Technology exposure to various known or expected vulnerabilities with known or contracted resources.

Ransomware is a type of malware from cryptovirology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid. While some simple ransomware may lock the system in a way which is not difficult for a knowledgeable person to reverse, more advanced malware uses a technique called cryptoviral extortion, in which it encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them.

Software as a service (SaaS) is a software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted. It is sometimes referred to as "on-demand software". SaaS is typically accessed by users using a thin client, e.g. via a web browser. SaaS has become a common delivery model for many business applications. SaaS has been incorporated into the strategy of nearly all leading enterprise software companies.

A **threat** is a possible danger that might exploit a vulnerability to breach security and therefore cause possible harm. A threat can be either "intentional" (i.e. hacking: an individual cracker or a criminal organization) or "accidental".

Threat Intelligence Platform is an emerging technology discipline that helps organizations aggregate, correlate, and analyze threat data from multiple sources in real time to support defensive actions. TIPs have evolved to address the growing amount of data generated by a variety of internal and external resources (such as system logs and threat intelligence feeds) and help security teams identify the threats that are relevant to their organization. By importing threat data from multiple sources and formats, correlating that data, and then exporting it into an organization’s existing security systems or ticketing systems, a TIP automates proactive threat management and mitigation. A true TIP differs from typical enterprise security products in that it is a system that can be programmed by outside developers, in particular, users of the platform.

A **Trojan horse**, or Trojan, is any malware which misleads users of its true intent. The term is derived from the Ancient Greek story of the deceptive Trojan Horse that led to the fall of the city of Troy.

Trojans are generally spread by some form of social engineering, for example where a user is duped into executing an e-mail attachment disguised to appear not suspicious, (e.g., a routine form to be filled in), or by clicking on some fake advertisement on social media or anywhere else.

A **virtual private network** (VPN) extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Applications running on a computing device, e.g. a laptop, desktop, smartphone, across a VPN may therefore benefit from the functionality, security, and management of the private network. Encryption is a common though not an inherent part of a VPN connection.