infotex

Triguard®

Managed SIEM by infotex

siem.infotex.com

We're on Your Team

infotex will monitor your network 24x7x365, with real human beings watching everything that happens, looking for anything potentially negative, filtering out the noise, and finding reportable incidents. **infotex** will then respond in **real-time** to critical incidents per your customized "decision tree," to a customized calling tree. A web interface is available so you can see exactly what our Data Security Analysts see.

A big difference between purchasing an application and engaging with **infotex**: we join your team. Imagine hiring a team of cybersecurity professionals with certifications from ISACA, ISC_2, and others, to establish a SIEM process designed by IT auditors. We work to get to know your unique system –your network AND your people – and we bring a balanced approach to help you fight the noise and respond to incidents.

A Good Night's Sleep

We've studied why people contract with Managed Security Service Providers, and beyond all the rhetoric that we find on well-crafted marketing sites, we've reduced it all down to one thing: You want somebody to watch your back, to be there when you can't. You want a good night's sleep!

Triguard® Managed SIEM

infotex started offering network monitoring solutions in 2000 and began developing our SIEM in 2003. Founders of bleedingsnort.com, we now receive threat intelligence from many sources including emergingthreats.net. Utilizing big data, machine learning, and artificial intelligence technologies, we utilize a group of preventive and detective controls, watching alerts from IPS/IDS, ELM, Change Detection, Rogue Device Detection and our SIEM, now known as **Triguard®**, to ensure an effective, appropriate, and risk-based approach to monitoring your network.

Customization

Having made the decision to "outsource" or to "get more professional help," the next decision you need to make is this: Are you willing to hand over the important monitoring function to a cookie-cutter approach? We customize everything to your specific, unique needs.

Tying It All Together with Triguard®

Our approach makes sure that we are correlating event logs with network traffic. Our database has evolved since the turn of the century to not only queue up data but give us the ability to pivot on that data based on unique circumstances. Not only do we queue up potential correlations, but our staff is trained to look for those patterns between network traffic alerts and event logs. The result is a much more robust approach to monitoring your network, and the security advantages of that are excellent!

Put a Watch

We interview you to gather the information we need, and next thing you know, you have a report showing pertinent information about a user account, an endpoint, an IP address, a website . . . any asset you can name. Imagine the benefits of having a third party monitor a user, vendor, or even your auditor.

US Based | 24x7x365

Managed Security Operations Center

infotex Managing Technology Risk my.**infotex**.com (800) 466-9939

infotex

Triguard®

Managed SIEM by infotex

siem.infotex.com

Managed Detection and Response (MDR)

infotex offers not only an EDR solution, but we also offer Managed Detection and Response, which allows us to monitor your system with our 24x7x365 Security Operations Center. **infotex** MDR can be part of your full **Triguard®** Managed SIEM offering or as its own engagement. Our system can digest logs from most EDR solutions, but depending on your chosen solution the delivered services may vary, the baseline offering would include and customized section of your daily report that will report important events from your EDR system.

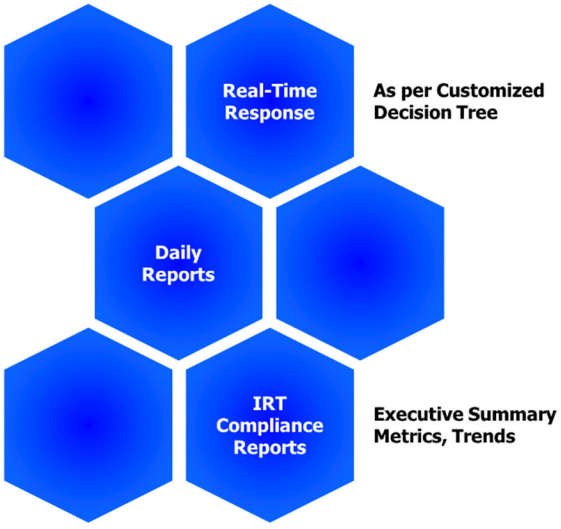
Decision & Calling Trees

First developed in 2003, our Decision Tree is a matrix listing all the predictable security incidents and your customized instructions as to the appropriate response. We queue up a "default decision tree" to take advantage of our 25+ years of experience, but we also allow you to customize response to your own unique situation.

In addition, we will help you create a calling tree very similar to what you're already using in your Disaster Recovery Plan, only in this case it's focused on Network Security Incidents. You will use the calling tree to direct us on how to respond to various types of incidents. While our years of experience will guide you in establishing an adequate incident response plan (and thus calling tree), yours can get as granular as you wish, and leverage processes already established. It can integrate with your ticketing system; it can be email driven. Whatever helps you respond to incidents properly.

Who Watches the Watchers?

At **infotex,** we walk the talk. We conform to the FFIEC Guidelines, HIPAA Security Ruling, FERPA, CIPA, Sarbanes Oxley, PCI, and other important regulations. We're in the FFIEC Technology Service Provider Examination Program… undergoing the same scrutiny as any of our financial institution Clients. This requires us to have year-long penetration tests, general controls audits, governance reviews, social engineering tests, and other tests. Be sure to check out our Due Diligence Packet!



A Compliant Solution . . .

Being in the FFIEC Examination program is not enough. We undergo several external audits, pen tests, and social engineering engagements each year. We also make sure it's easy for you to see what controls we have in place to protect our access to your network. We teach our Clients how to make sure they know the risk they face because they share information with or grant network access to vendors. Again, we walk the talk. Don't take our word for it: Ask for a copy of our Due Diligence packet. In it you will see exactly what you should be receiving from all your technology vendors: assurance of controls!

Balancing Technology with Humanity

The biggest myth in Information Security is that it can be fully automated. Automation helps, but it's the human expertise behind it that keeps you truly protected—and that's where **infotex** stands out. Our Data Security Analysts cut through the noise, interpret events, and deliver clear, actionable insights so you get exactly what you need, exactly when you need it. Our **Triguard®** system allows you to dive in for deeper analytics, but instead of making you spend time hunting, we push meaningful intelligence to you. With **infotex** on your team, you gain the benefit of our 25+ years of cybersecurity experience to keep you and your customers safe!

US Based | 24x7x365

Managed Security Operations Center

infotex Managing Technology Risk my.**infotex**.com (800) 466-9939