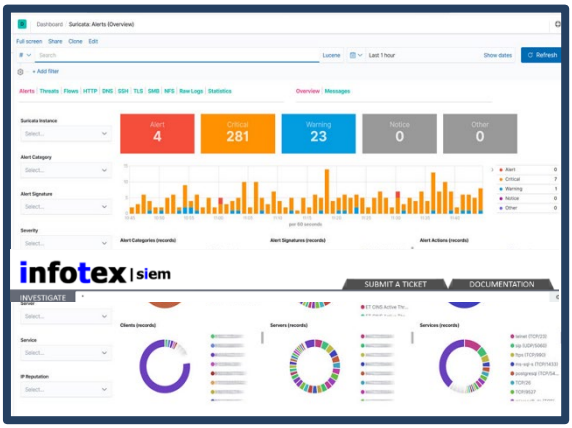
infotex

MANAGED SECURITY OPERATIONS CENTER

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, ISC2, 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!

24x7x365

Managed Security Operations Center

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

infotex

MANAGED SECURITY OPERATIONS CENTER

siem.**infotex**.com

Our 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, CD, and our SIEM, to ensure an effective, appropriate, and risk-based approach to monitoring your network.

Preventive Control: IPS

infotex uses an Intrusion Prevention Service that automatically responds to predictable attacks and poor reputation IP addresses within milliseconds. This service utilizes world class behavior anomaly signatures from Emerging Threats to enhance network perimeter security.

Detective Control: IDS

You can automate some of the processes in information security, but without Human Beings monitoring these processes, and performing threat hunting, the result is a false sense of security. If something out of the ordinary happens, our Data Security Analysts are here 24/7/365 to **investigate** and **respond** to the threat. For detection, we use thousands of signatures as well as protocol and anomaly analysis. **infotex** also adds customized signatures to detect the issues and activities that you are most concerned about, as well as known and unknown (zero day) threats.

Detective Control: ELM

Millions of event logs are generated each day by your servers, network devices, and various applications. Our Event Log Management solution not only helps you filter out the noise, but the interface includes everything you need to show your auditors that you are reviewing your logs. **Health reporting**, acknowledgement systems, customized dashboards, and real time monitoring all work together to ensure you are compliant!

infotex

MANAGED SECURITY OPERATIONS CENTER

siem.**infotex**.com

Detective Control: Forensic Capabilities

Another advantage to outsourcing the network monitoring controls to a third party is that, as a third party, we are in a much better position to capture evidence in the event you need it. Our ELM system is already configured to store data forensically, but we can also be called out on site to gather evidence… on a 24x7 basis

Detective Control: Change Detection

When somebody on your staff opens a port for a vendor, have we remembered to close it? We scan of your public IP addresses on a monthly basis and report the ports that have changed since the last scan. Not only is this a great security tool, but it is an excellent change management tool as well. And, it is now required by the Cybersecurity Assessment Tool.

Tying It All Together with SIEM:

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 to that are excellent!

24x7x365

Managed Security Operations Center

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

infotex

MANAGED SECURITY OPERATIONS CENTER

siem.**infotex**.com

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.

Who Watches the Watcher?

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!

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.

24x7x365

Managed Security Operations Center

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

Decision Tree

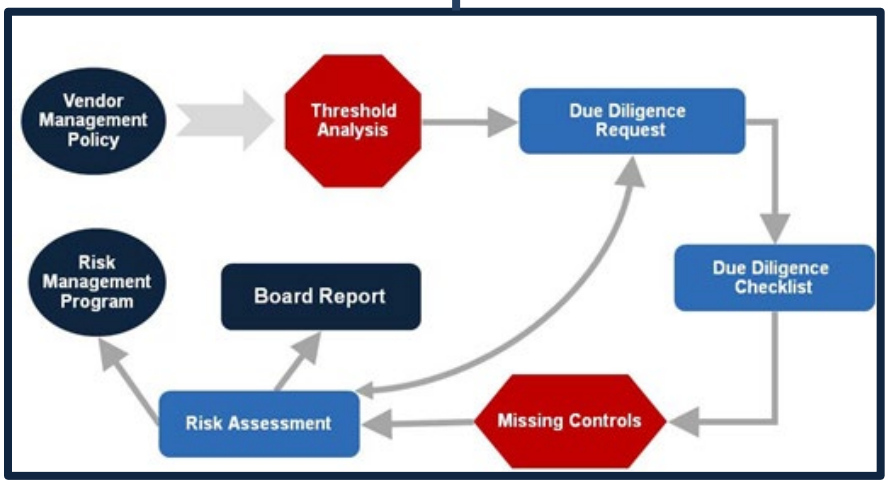
First developed in 2003, our Decision Tree is a matrix listing all the predictable security incidents and your customized instructions as to the appropriate response. We queue up a "default decision tree" to take advantage of our 20 years of experience, but we also allow you to customize response to your own unique situation

Calling Tree

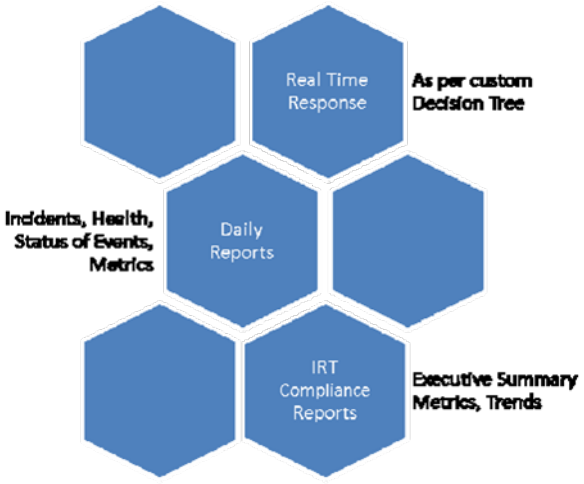
When you engage with us, **infotex** will help you create a calling tree very similar to what you're already using in your Disaster Recovery Plan, only in this case it's focused on Network Security Incidents. You will use the calling tree to direct us on how to respond to various types of incidents. While our 20 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.

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 banks and credit unions 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 package. In it you will see exactly what you should be receiving from all your technology vendors: assurance of controls!



Human Reporting



The biggest myth in Information Security is that you can automate information security. Sure, some parts of the process are automated. But human beings still need to monitor the automated processes, and that's exactly what separates **infotex** from other vendors. We sort through all the noise, and only involve you when you need to be involved. Yes, we have all the fancy charts and graphs and reports, but we push those out to you. Our Data Security Analysts decipher the graphs and charts, review the events collected, and create reports with varying levels of detail to share with your Incident Response Team. You are welcome to learn our interface and download all kinds of great information and statistics about your network. Still, rather than making you "pull" information from the system, human beings decipher the information and push it to you. **You only see what you need to see, when you need to see it**.

Balancing Technology with Humanity

Our Clients can tell you how we work not only **in** the technical act of watching your network, but also **with** the non- technical implications of our services. When we're on your team, hundreds of policy and procedure templates are always at your disposal.

Policy Development

The calling tree and decision trees, by the way, fulfill just one strategy of your overall Incident Response Program, which **infotex** will help you write, as we will become part of your Incident Response Team. Other documents related to what we do, and even our premium Policy Boilerplates Library is available to Clients.