PROPOSAL & SOW:

SOL SIEM™

Security Information & Event Management

24/7/365 Network & Cloud Visibility

PREPARED FOR:

NAME

Company

Contact Info

CYBERSAFE SOLUTIONS®

Table of Contents

Introduction

Cybersafe's SOL SIEM platform offers visibility into your organization's network and cloud.

Each solution is built with the understanding that there is no "one size fits all" security solution, so clients receive a customized deliverable with unique alerting and escalation procedures. Cybersafe's SIEM offers real-time alerting and live response (containment) where our experienced analysts review, investigate, and dispatch every alarm. Clients can trust that each time they hear from our SOC, it is actionable, important, and vetted to include remediation guidance. Through a robust learning and tuning phase, our team truly becomes an extension of our clients, enabling us to act quickly when something deviates from the norm. As part of our commitment to our clients, Cybersafe includes unlimited remote incident response on all covered assets.

Most organizations do not have the time, bandwidth, and/or expertise to monitor for cyber threats in real-time. Cybersafe Solutions' highly trained security analysts are there for you 24/7/365 to provide the following:

Superior Visibility

If you can't see it, you can't defend against it. Cybersafe's SOL SIEM platform creates visibility across your network and cloud.

Threat Hunting

Cybersafe SOL SIEM goes beyond simply detection and attack response. We proactively hunt for signs of security weaknesses and risky behavior to raise your organization's overall security posture

Focused Resources

Your team can spend their time on core business activities instead of monitoring and analyzing security threats.

Incident Response

All covered assets protected by SOL SIEM include remote Incident Response support.

Expertise

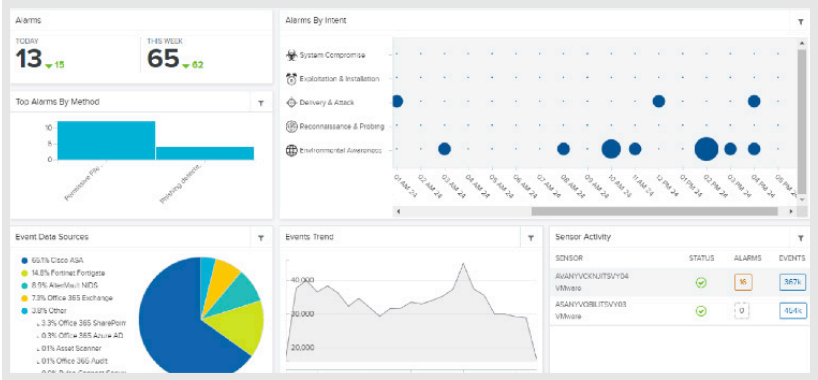
Cybersafe Solutions' team of certified security analysts turn data into action, differentiating the real attacks from the noise. We monitor alerts 24/7/365 so that you don't have to.

Leading Intelligence

SOL SIEM incorporates numerous threat intelligence sources so we are aware and on top of the latest threats before they can impact your business.

SOL SIEM

SOL SIEM is the premier solution for network cybersecurity defense today. Our network security engineers monitor your organization's network traffic in real-time, 24 hours a day, 7 days a week, 365 days a year. Cybersafe's network security monitoring provides:



Enhanced Visibility:

Cybersafe sensors provide significantly improved information over log-based monitoring solutions with real-time intrusion detection through packet capture and analysis. We have support for on-premises networks as well as Amazon Web Services and Microsoft Azure Cloud.

Cloud Integrations:

With dozens of purpose-built integrations, Cybersafe can dive deeper into your cloud and SaaS security data to identify malicious activity. Example integrations include Microsoft 365, G Suite, Cisco Umbrella, Proofpoint, and Box.

SIEM & Log Management:

Quickly correlate and analyze security event data from across your network and cloud environments with built-in SIEM and log management. Example log sources include Windows Active Directory, firewall logs, and VMware logs.

Vulnerability Assessment:

Identify on-premises systems that are potentially vulnerable to exploits with active network scanning and continuous vulnerability monitoring. Cybersafe scanners can perform unauthenticated and authenticated scans for more complete vulnerability understanding.

Behavioral Monitoring:

Instantly spot suspicious network behavior with deep traffic analysis, service monitoring, and full packet capture.

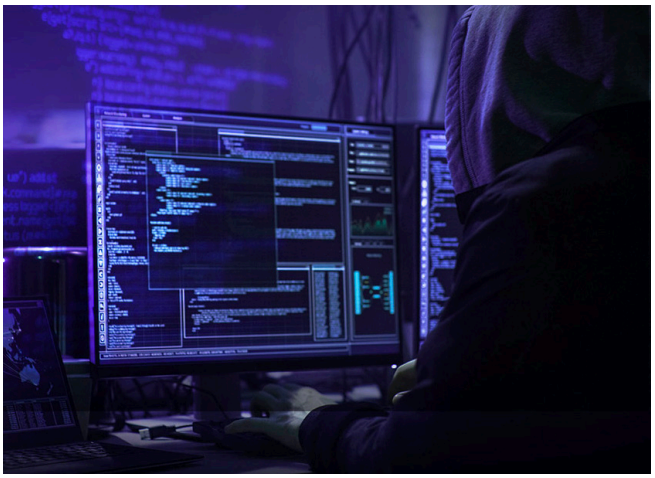
Asset Discovery & Inventory:

Understand the devices attached to your network and identify new or rogue devices quickly.

Deception Technology

How do you identify a potential threat actor that looks and behaves just like an authorized user? This was the challenge that led Cybersafe to provide Deception Technology as part of its SOL XDR offering. This is often referred to as a honeypot. Cybersafe's Deception Technology goes beyond traditional deployments, including dozens of personalities to ensure our decoys look and feel legitimate to a threat actor.

We employ a layered set of decoys designed to confuse and lure threat actors out of hiding, diverting them from valuable infrastructure and data. Cybersafe deception deployment includes decoy server infrastructure as well as decoy data hidden in file systems and user mailboxes.



Domain Doppelganger Name Monitoring

Today, the most convenient attack vector for any criminal is the employee. Tricking an employee through a phishing campaign remains one of the most popular attack methods. After discovering employees through intelligence gathering or the dark web, criminals will attempt to phish them. To increase the likelihood of success, phishing campaigns employ domains that seem familiar to a user but are illegitimate.

These lookalike domains can allow criminals to pose as employees or partners by spoofing email addresses or to create deceptive links for the victim to click on. Detection is key and starts with monitoring the internet for "phishy" domain name registrations.

Our Domain Monitoring provides visibility into:

- Typos, such as character substitutions or repeated characters (e.g. cybers@fesolutions.com or cybersafessolutions.com) and several other kinds of typos
- More technical variants such as bitflips
- Substring inclusions (e.g. cybersafesolutions-account.com)
- ...and several other kinds of variants

Once configured, we will alert you of infringing domains so you can protect your brand name and your employees from impersonation or phishing attacks.

SOL DARK

Cybersafe will notify you when it discovers compromised data that matches your email domain displaying how the data was discovered, including third-party data breaches, keyloggers, malware, or phishing exploits. As the associated passwords are often discovered in “clear-text” (meaning unencrypted), you are able to automatically compare it against your internal password criteria (minimum character lengths, number of letters, numbers, special characters, and capital letters) to focus more quickly on exposures that have a higher probability of being used to exploit or breach your network. Hashed or encrypted passwords can be just as damaging because there are now dozens of free websites that criminals can use to decrypt them within seconds.

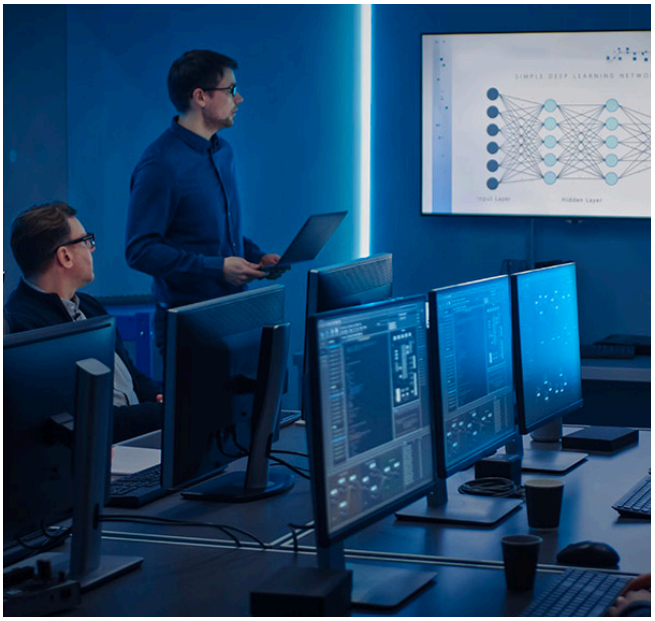
Cybersafe Solutions Delivery Model

Cybersafe understands that a strong relationship requires excellent communication and personalized attention. Therefore, Cybersafe has developed a service delivery model to ensure we are in touch with you and your business at all times. Our expert team works with you every step of the way to prevent, detect, and respond to threats. All clients have the following resources available to them.

Monitoring Reporting & Dashboards

To maximize efficiency and consistency across our operations and technologies is Cybersafe’s Security Orchestration, Automation, and Reporting Platform (SOAR). Our SOAR combines human and machine power to prioritize and standardize alert analysis and incident response. Cybersafe’s SOAR enables us to...

- Identify and respond to suspicious behavior as quickly and effectively as possible.
- Automate repetitive and mundane tasks.
- Standardize response processes across multiple analysts.
- Provide a unified and centralized console for all technologies and threat intelligence feeds.
- Provide detailed metrics and dashboards on all alert and analyst activity.



Threat Intelligence

Threat intelligence is information about potential or current attacks that threaten an individual or organization. Cybersafe Solutions leverages internal and external threat intelligence information to maximize our capabilities. Cybersafe is constantly researching the latest tools, tactics and procedures (TTP’s) in use by modern sophisticated Threat Actors so they can be rapidly detected and mitigated.

Why Cybersafe?

Cybersafe Solutions prides itself on always being at the forefront of cybersecurity – not a small task in a field that changes so rapidly. We do this by leveraging an arsenal of the latest technology, proprietary tools, and flexible solutions that are carefully curated and deployed to meet the unique needs of each client, no matter their size or where they do business. Our United States-based Security Operations Center employs a team of experts around the clock, where our analysts utilize their cybersecurity experience and certifications 24/7/365 to intervene and eradicate cyber threats from client environments.

Cybersafe understands that your cybersecurity program is only as strong as the team standing behind it. We understand that each client environment is unique and requires dedicated attention and a tailored solution. Leaning on our team of experienced professionals, we will determine your cybersecurity baseline and create an engagement plan that includes advanced visibility and best practices to reduce risk and quickly improve your cybersecurity posture.

Cybersafe's commitment to our clients will always remain the same: to be a client-centric, value-driven firm that utilizes best-of-breed technology. Our clients can trust as an extension of their team, each member of Cybersafe always has their business in mind. That's why we constantly look for new ways to enhance our solutions and keep up with the ever-changing threat landscape. Cybersafe, at its core, understands that a security provider can never stay stagnant. It is our promise to our clients to always evolve with the industry.

CYBERSAFE UNDERSTANDS THAT YOUR CYBERSECURITY PROGRAM IS ONLY AS STRONG AS THE TEAM STANDING BEHIND IT.