HOCS CONSULTING

Modern-Day Cybersecurity Protection

A Complete Guide to SOC/SIEM

Today's Cyber Threats Demand a Cohesive Approach

Modern cybersecurity is complex. And, between advanced technology concepts and confusing acronyms, it's easy to see why so many business owners can get overwhelmed. But in today's cyber landscape, with threats increasing in frequency and complexity, there's no room for error.

Historically, managed service providers, also called MSPs, have looked to several security tools to patch together one robust security solution. But over time, one solution—SOC/SIEM—has evolved to provide comprehensive threat detection management and response.

> 60% of small businesses that suffer from a cyberattack go out of business within six months.

Real-World, Managed Security

In this eGuide, we'll dive into how the SOC/SIEM solution works. We'll explore why SOC/SIEM is critical to safeguarding a business today. And finally, we'll highlight what makes HOCS Consulting's SOC/SIEM solution superior to other solutions on the market.

To better understand what SOC/SIEM is, let's start with what it isn't and then go from there.

> In 2022, the average cost of a data breach globally hit $4.35 million.
>
> *-Statista*

01. Clearing Up Acronym Confusion

The myriad of acronyms in the business world can lead to confusion. It's no wonder many people are fuzzy on what these terms mean and often mistakenly interchange them. In the spirit of understanding, let's clarify a few commonly misunderstood acronyms.

SIEM

Security Information Event Management

SIEM provides intelligent threat detection and security incident response through continuous real-time collection and analysis of security events across your entire infrastructure. SIEM is also key to meeting compliance requirements.

SOC

Security Operations Center

A SOC is a 24/7/365-manned facility that fortifies your security defenses with human cybersecurity expertise. Certified SOC analysts are trained to analyze escalated alerts and can take immediate action if necessary.

Not the Same as ....

SOX

Sarbanes-Oxley

Often confused with SOC, SOX is a set of compliance regulations in the financial industry requiring all publicly traded companies to establish, test, document and manage internal controls and procedures around financial reporting.

SOC 2

Service Organization Control Type 2

Another acronym often confused with SOC, SOC 2 is a voluntary compliance framework developed and awarded by the American Institute of Certified Public Accountants (AICPA). SOC 2 compliance requires the successful completion of regular third-party audits for advanced security controls around data availability, processing integrity, confidentiality and privacy.

02. The Ultimate Competitive Advantage

SOC/SIEM is enterprise-grade threat detection that can keep your business a step ahead through a powerful combination of people, processes and technology.

Collect. Correlate. Analyze.

How SOC/SIEM Works:

COLLECT

First, the SIEM provides a centralized log of security alerts generated across your entire IT infrastructure.

CORRELATE

Then, managed endpoint detection (EDR) powered by artificial intelligence (AI) monitors the alerts and builds a library of learned patterns in user activity to detect the slightest anomaly. SOC/SIEM technology can sift through thousands of alerts to identify that needle in the haystack — a capability no other tool or human can match.

ANALYZE

Finally, alerts identified as potentially harmful are automatically escalated to a certified SOC staffed by security analysts. Escalated alerts are vetted and, if necessary, isolated and remediated.

03. Benefits of One Holistic Solution

Protect

- Compliance requirements, auditing and reporting
- Cyber insurance qualifications

Prevent

- Expert analysis and response
- Intelligent defense against known threats

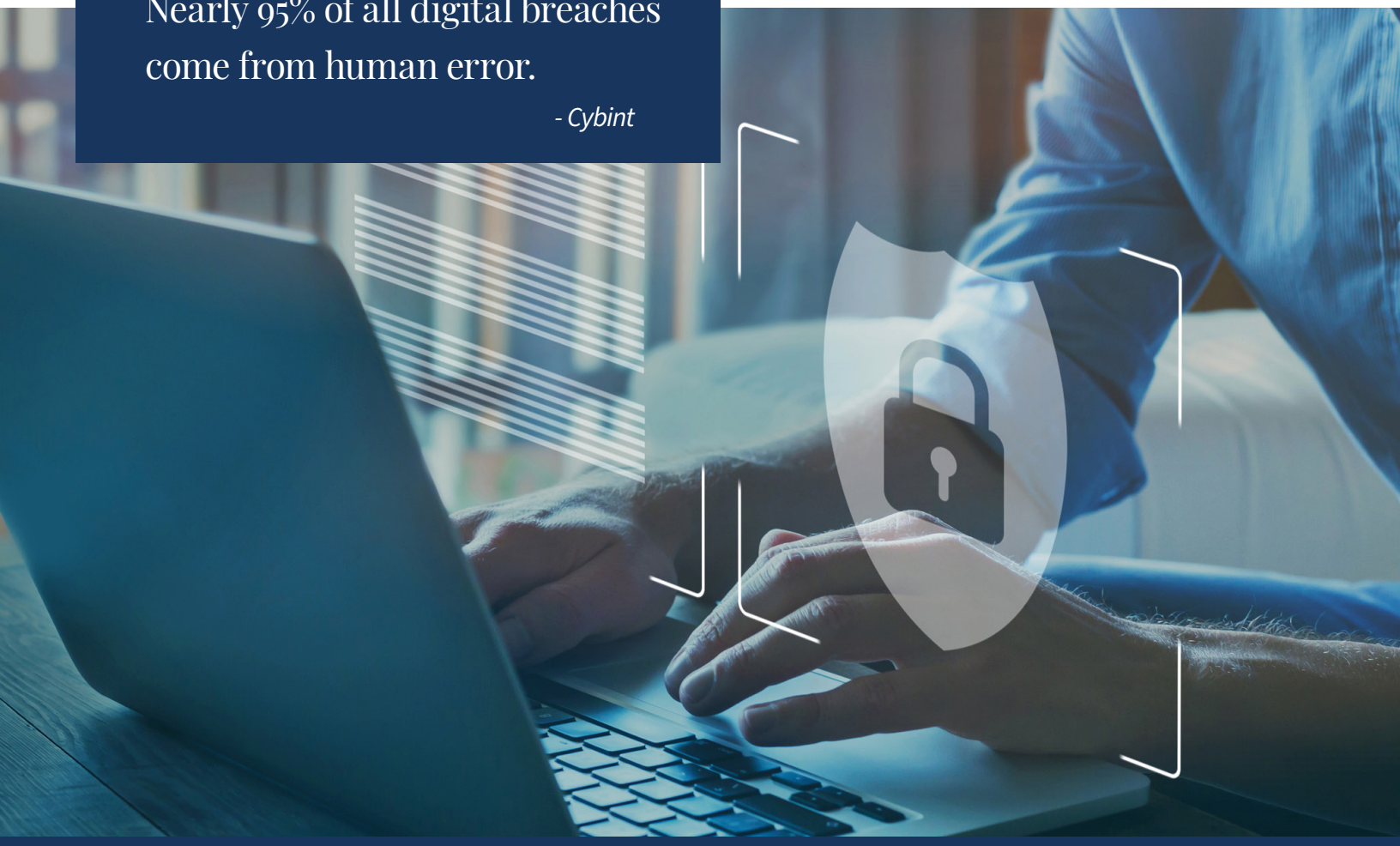
Detect

- Holistic visibility into your entire infrastructure
- Accelerated intrusion detection

Respond

- Forensic incident investigation support
- Business continuity and data restoration

> Nearly 95% of all digital breaches come from human error.
>
> *- Cybint*



04. Why HOCS Consulting

HOCS Consulting's SOC/SIEM provides a comprehensive, best-of-breed security solution through cutting-edge technology, time-tested processes and expert human analysis.

Fully Managed

HOCS Consulting delivers comprehensive, all-in-one SIEM-as-a-Service and SOC-as-a-Service. Our first-rate security solutions combine industry-certified IT professionals, proven processes and cutting-edge technology to effectively monitor, detect, analyze and respond to modern security threats.

Flexible

We provide flexible options for any budget – from SMBs to enterprises. And, if you have internal IT resources, our team can function as a supplement.

SOC 2 Certified and Compliant

HIPAA, ISO 27001, PCI-DSS, NIST, ISO, EU GDPR, PCI-DSS, SOX 404, FFIEC and more.

Healthcare Industry Specialization

From meeting HIPAA compliance to implementing electronic health record (EHR) projects, HOCS Consulting has a long history of supporting healthcare organizations.

Innovative Tech Solutions and Unparalleled Service

- Managed IT
- Cybersecurity
- Data Access Control
- Cloud
- Compliance
- Consultancy
- Continuity

HOCS Consulting is a full-service managed service provider serving organizations throughout the United States. Since 1991, we have been providing innovative, personalized solutions in managed IT, cybersecurity, cloud and more. HOCS Consulting is best known for its reputation for excellence, integrity and always making the right decisions for our clients.

For more information, visit **hocsinc.com** or call **(866) 246-4627**