MIKE RICHLINE

Understanding the Value of Your SIEM and SOC

KEYS CONFERENCE

1

Disclaimer

A FEW THINGS FIRST

This presentation is for information only.
Evaluate risks before acting based on ideas from this presentation.

This presentation contains opinions of the presenters.
Opinions may not reflect the opinions of Tandem.

This presentation is proprietary.
Unauthorized release of this information is prohibited.

KEYS CONFERENCE

2

Mike Richline

AREA MANAGER

CONETRIX TECHNOLOGY

KEYS CONFERENCE

3

8 • THE BUSINESS JOURNAL OF CORPUS CHRISTI • June 14, 2007

Entrepreneur

Partners in maintaining technology

By Rebecca Esparza
Contributing Writer

Anyone that has wasted precious time fussing with a recalcitrant computer knows unless you have an affinity for technology, it is best to let the experts handle it.

Brothers Mike and Josh Richline have seized on that theory with their own company, Richline Technical, since April 2001. Before then, Mike worked with a local technical consulting company and Josh was doing similar work at a San Antonio firm. Mike's college roommate, Tommy King, joined as a partner in 2003.

"I initially started out on my own because at the time, there was only one other company in town doing high-end consulting," recalled Mike.

"With a lot of persistence, we opened this business up when I was 24. Maybe that persistence was mixed with a little bit of arrogance, too," he laughed. "I wanted to overcome the stigma that you had to go out of town to get this kind of work done."

Technical snafus could be avoided simply by maintaining the health of your computer, added Josh.

"Most companies think on a reactive basis, meaning they send technicians out only when there is something wrong with their computer. With our managed services, we keep things from breaking. Our technicians prevent trouble from happening," he said.

And now technology has progressed to where their technical staff can monitor work stations and servers remotely, without even leaving their headquarters in downtown Corpus Christi.

"We monitor servers in New Mexico, Houston, Arizona, Austin, San Antonio and the Rio Grande Valley. One company in East Texas has hired us as their technical department," said Mike.

He stressed Richline Technical is not your typical shop that fixes computers. "We have a 24-hour, seven-day-a-week operation that monitors critical devices," he said. "The longer it takes your computer technician to fix it, the more it will cost your business in the long run. Our goal is to keep your network up and running. You never want to go down, especially for long periods of time."

It is a new era for the company, as they move away from being called for repairs only, to "managed services," where clients hire them to perform routine maintenance on a monthly basis.

"While most [information technology] companies operate on that reactive basis, our services prevent that computer from breaking in the first place," noted Josh. "We're also moving towards becoming a 'help desk' function for smaller companies, remotely managing their machines."

Josh added the brothers put a lot of extra work building the company, literally from scratch. "You need to be ready to work 80 hours a week sometimes," he noted, of a business owner's hectic schedule.

He encourages would-be entrepreneurs to develop a thick skin, don't get easily discouraged and be willing to do anything. For example, the brothers recalled a job in the early days of the company at North Shore Country Club. "We had to run cable through their attic and it must have been well over 104 degrees in there," Josh remembered.

"It was the middle of the summer," lamented Mike. "And here we were, underneath a metal roof that just radiated the heat. It was miserable, but we did it."

Both brothers agree their entrepreneurial spirits were probably forged at an early age, when their parents required they earn the money for their first cars on their own. "It was the way we were raised, if we wanted something we had to work for it," said Josh.

Meanwhile, Mike noted the ha
of moving from reactive to pre
is getting people to realize they
do regular maintenance.

"Your car and house undergo
maintenance, why not do the
your computer systems?" argue

Like most companies, the
brothers want to evolve their
and have plans in place fo
changes.

"We're trying to build a one-s
meaning a place where a com
get everything technologica
done in one place," said Josh.

The goal is to fill the building
ferent groups of experts in the
such as telephone systems,
services, Web design and ever
systems.

"When businesses in Corpu
think technology services, we want them
to think Richline Technical," Josh added.

Partners at Richline Technical (pictured left to right) Mike Richline, Josh Richline and Tommy King, offer clients preventive
in order to maintain their computer operations.

Paul Iver

4

Agenda

HERE'S THE PLAN

- What are SOC and SIEM?
- Role in Cybersecurity Strategy
- Reasonable Expectations
- Questions & Answers

KEYS CONFERENCE

5

KEYS CONFERENCE

What are SOC and SIEM?

6

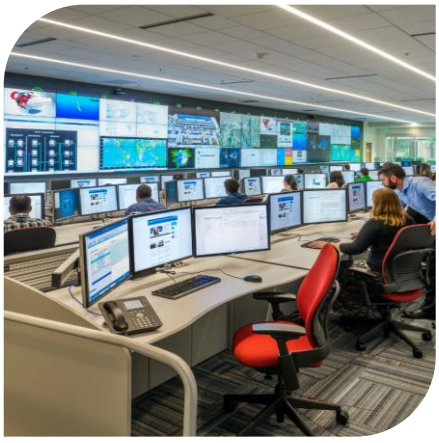
What is a SOC?

Not a “SOCK” or a “SOC 2”

KEYS CONFERENCE

7

What is a SOC?



Security **O**perations **C**enter

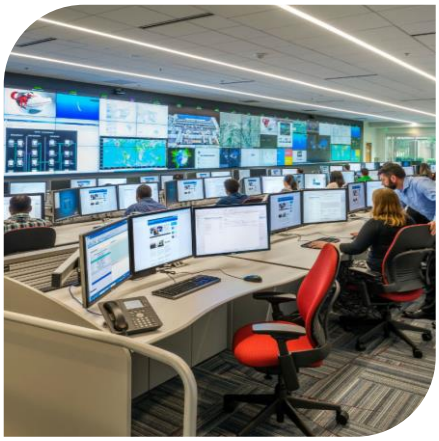
“A centralized function within an organization employing people, processes, and technology to continuously monitor and improve an organization's security posture while preventing, detecting, analyzing, and responding to cybersecurity incidents.”

Source: McAfee

KEYS CONFERENCE

8

What is a SOC?



Security Operations Center

- Monitors for Threats
- Provides Context
- Makes Decisions

KEYS CONFERENCE

9

What is a SIEM?

Security Information Event Management

"Security Information and Event Management (SIEM) is software that improves security awareness of an IT environment by combining security information management (SIM) and security event management (SEM). SIEM solutions enhance threat detection, compliance, and security incident management through the gathering and analysis of real-time and historical security event data and sources."

Source: McAfee

KEYS CONFERENCE

10

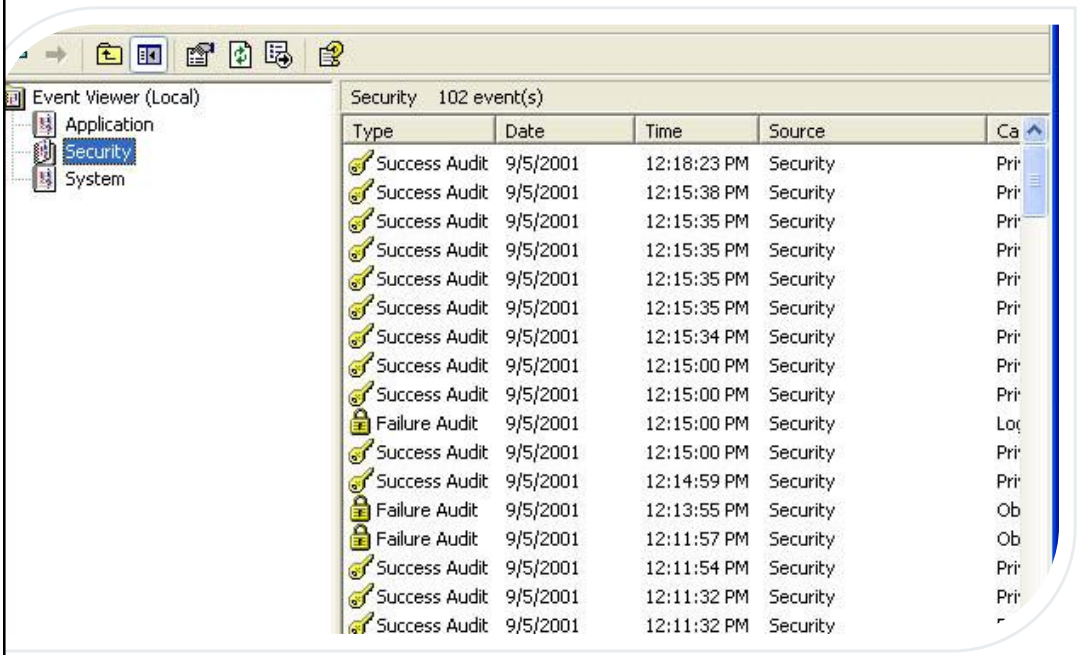
What is a SIEM?

Security **I**nformation **E**vent **M**anagement

- Software or Appliance
- Gathers and Analyzes Logs
- Produces Alerts

KEYS CONFERENCE

11



Event Log

KEYS CONFERENCE

12

What Goes into Your SIEM?

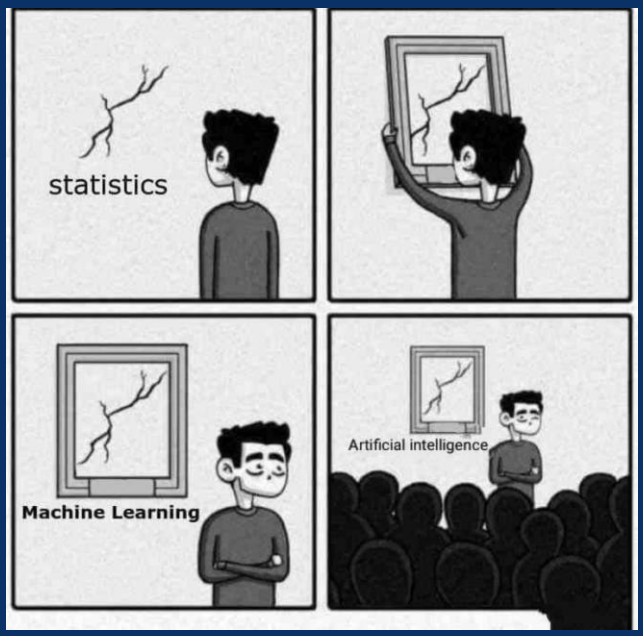
HERE ARE A FEW EXAMPLES

- Domain Controller
- Firewalls
- All Security Suites (EDRs)
  - Symantec\Norton\Traditional AV
  - Cylance\Crowdstrike\Defender
- Office 365
- Core Application Servers
  - SQL
  - Exchange
  - Business Critical
- Internet-Exposed Servers
- Routers
- Switches
- Proxy Servers\Web Filters
- DNS Logs (?)
- VPN Endpoints
- SDWan Devices
- Hypervisor Hosts
- WLAN Gear and Access Points

KEYS CONFERENCE

13

14



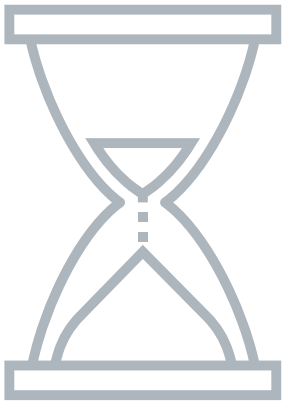
15

SOC & SIEM's Role in Cybersecurity Strategy

16

OWEN HUGHES | SENIOR EDITOR, ZDnet

“Burnout might be the most critical cybersecurity risk facing organizations in 2022.”



KEYS CONFERENCE

17

3x

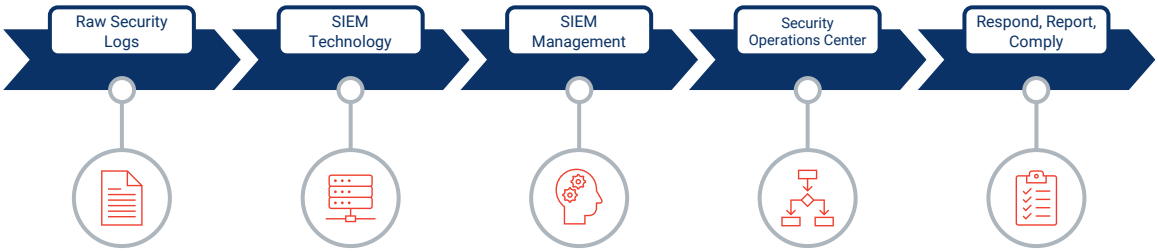
more likely to ignore security best practices

KEYS CONFERENCE

18

SOC & SIEM

HOW THEY WORK TOGETHER



KEYS CONFERENCE

19

KEYS CONFERENCE

Reasonable Expectations for Your SOC & SIEM

20

What Should I Expect

FROM A WELL-TUNED SOC AND SIEM

1 Data Accessibility

2 SIEM Flexibility

3 Skilled SIEM Operators

4 Helpful Reporting

KEYS CONFERENCE

21

Heath Bowlin

CONETRIX TECHNOLOGY

SENIOR NETWORK ENGINEER

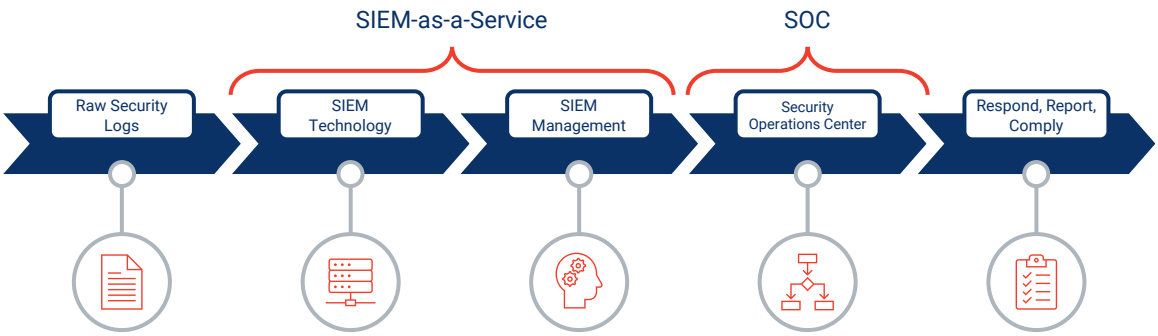
"I'm not saying I'm Batman, but me and Batman have never been seen in the same room together." - Heath

KEYS CONFERENCE

22

Cybersecurity Monitoring

BY CONETRIX TECHNOLOGY



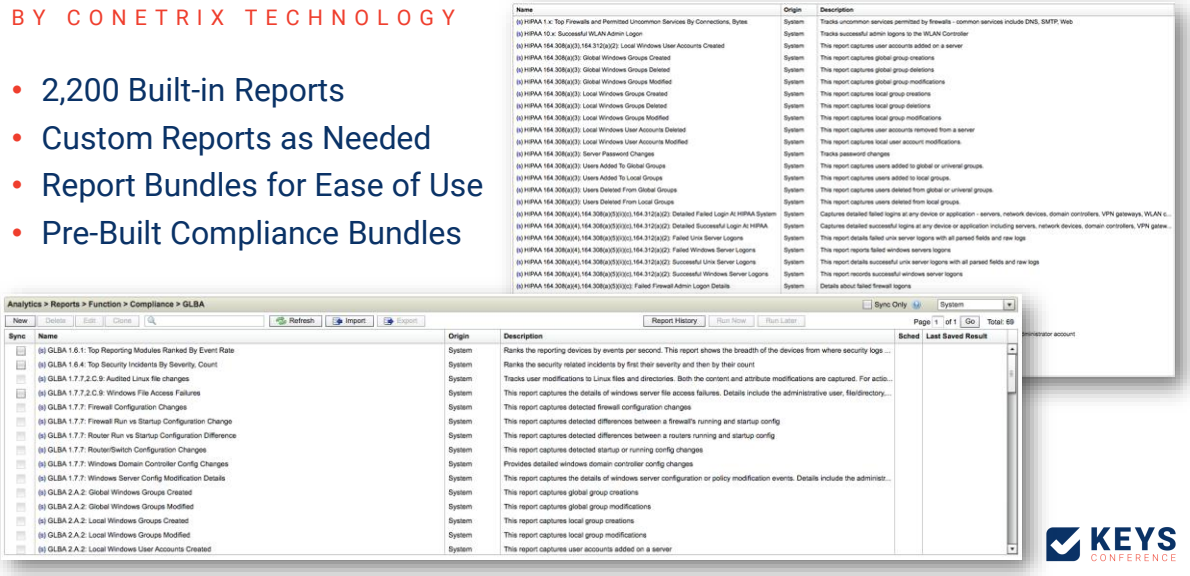
KEYS CONFERENCE

23

Reports

BY CONETRIX TECHNOLOGY

- 2,200 Built-in Reports
- Custom Reports as Needed
- Report Bundles for Ease of Use
- Pre-Built Compliance Bundles



KEYS CONFERENCE

24

LEARN MORE

STOP BY THE BOOTH TO MEET

CoNetrix*Technology*

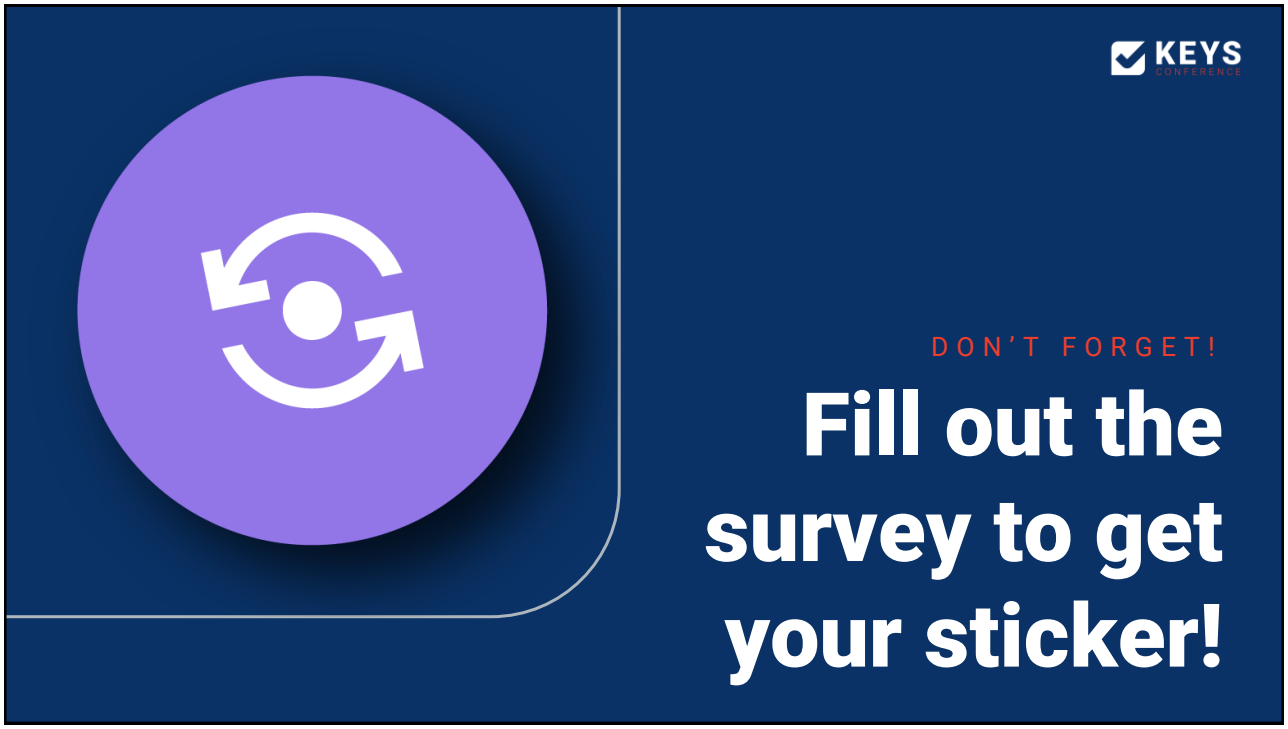
KEYS CONFERENCE

25

?

KEYS CONFERENCE

26



27

KEYS
CONFERENCE

THANKS FOR JOINING!

Understanding the Value of Your SIEM and SOC

Mike Richline
AREA MANAGER
CONETRIX TECHNOLOGY
mrichline@conetrix.com

28

Upcoming Sessions

TANDEM

Testing Your Operational Resilience

Brady Cook, Tandem

RISK & COMPLIANCE

A Chat with Your Friendly Examiner

Ruth Norris, Texas Department of Banking

CYBERSECURITY

Cybersecurity Session

TBD

KEYS CONFERENCE

29