
Cyber Security Fundamentals
RED LION
INFORMATION SECURITY. SMARTER.

SCOTT LYONS

- CEO of Red Lion
- Graduate of the school of hard business knocks
- Has worked all over the IT industry, from client-side to fulfilling client needs in both commercial and federal sectors
- Assisted in multiple Bsides Events, a GOON at both ShmooCon and DEF CON
- Peer Review Board Member- SYNACK Journal of Information Security
- Certification holder (won't say which)
- Passions are people and business

slyons@redlion.io
@CSP3R

RED LION
INFORMATION SECURITY. SMARTER.

JOSHUA MARPET

- COO of Red Lion
- Accomplished speaker, executive, startup CEO, and graduate of the Mach37 Cyber-accelerator
- Member of the CEO organizations Mindshare and Missionlink
- Former board member of Hackers for Charity, BSidesLV, and CSA-DelVal
- Editor of the SYNACK Journal of Information Security
- One of the Primary organizers of Security BSides Delaware
- Sleeps occasionally


jmarpet@redlion.io

@Quadling

RED LION
INFORMATION SECURITY. SMARTER.

Jeff Englander

- VP of Sales for Red Lion
- 30 years of business development
- 13 years of Information Services business development
- 15 years of Financial Services business development that included FinTech
- Awarded 100% of rebids over the past 13 years (11 contracts)
- Strong belief in keeping clients for life.....providing value each day
- JPMorgan, US Bank, GE Capital Services, GE Information Services, Boy Scout adult leader, school board member, American Univ MBA

jenglander@redlion.io
@jeffenglander

RED LION
INFORMATION SECURITY. SMARTER.

Agenda

- Fundamentals
- Risk Management
- Monitoring
- Compliance
- Cost Vs. Revenue center

RED LION
INFORMATION SECURITY. SMARTER.

Fundamentals

A basic principle, rule, law, or the like, that serves as the groundwork of a system; essential part

Fundamentals

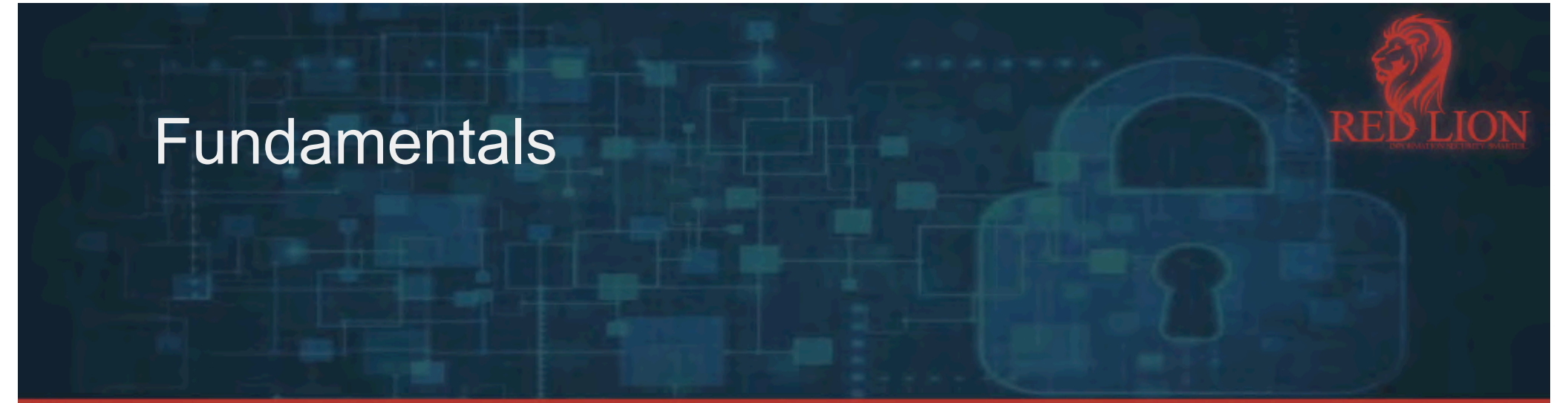
IT

- Updated OS?
- Patched?
- Logs stored?
- Default passwords changed?
- Network Diagram?
- Disaster Recovery Plan?

IT Security

- Firewall?
- Intrusion Detection System?
- Mail and Web filter?
- Antivirus?
- Anti-malware?
- Is anyone monitoring?
- Are you logging events?
- Have you checked Open Source Information?

Fundamentals



Who plans and architects IT projects?

Who do your people call for support?

Do you have Information Security?

Risk Management

The identification, assessment, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events or to maximize the realization of opportunities.

The objective is to assure uncertainty does not deflect the endeavor from the business goals.

Risk Management

Risks

Vulnerabilities

Assets

Threats

Motive

Opportunity

Access

Stealth

Assets

- Trade Secret - “Secret Sauce”
- Intellectual Property - Patents and processes
- Payroll Data
- Accounting records
- Email Archives
- Bank Account Credentials
- Active Directory Domain Admin credentials
- Anything that makes your company disappear

Threats

- Cyber Criminals
- Hacktivists
- Insider Threat
- Human Stupidity
- Misconfiguration
- Government Inaction
- Government Over-reaction
- Sleazy competitors
- Nation-state actors

Vulnerabilities

- Server Misconfiguration
- Laptop theft with unencrypted drive
- Web page with bad admin credentials
- Web page with “in the wild” exploit for it
- VPN using a bad encryption cipher
- Bad workflow or process that exposes information

Risk Management

IT

- Asset Inventory
- Information Asset Inventory
- Data Owner Review
- Incident Response Plans

IT Security

- Protective Systems
- Threat Profiling
- Information Asset Discovery
- Penetration Testing
- Vulnerability Discovery

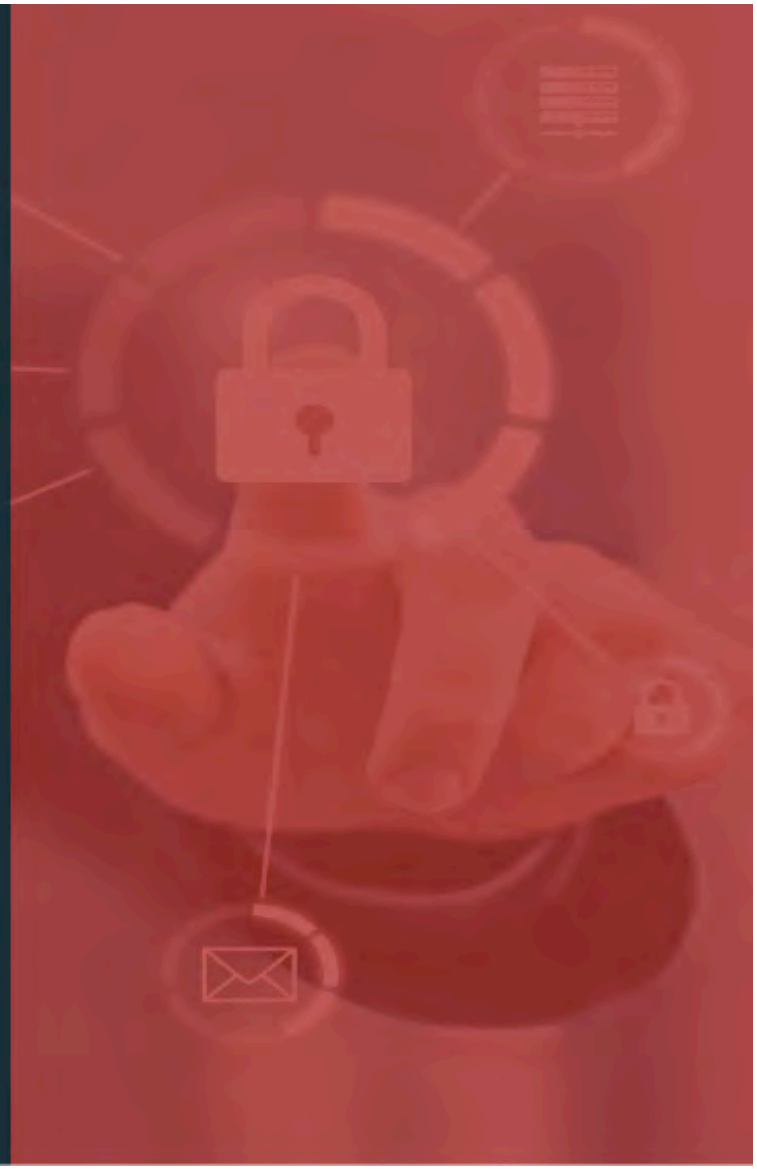
Risk Management

What do you own that is valuable?

Who wants it?

Are you appropriately protecting it?

Monitoring

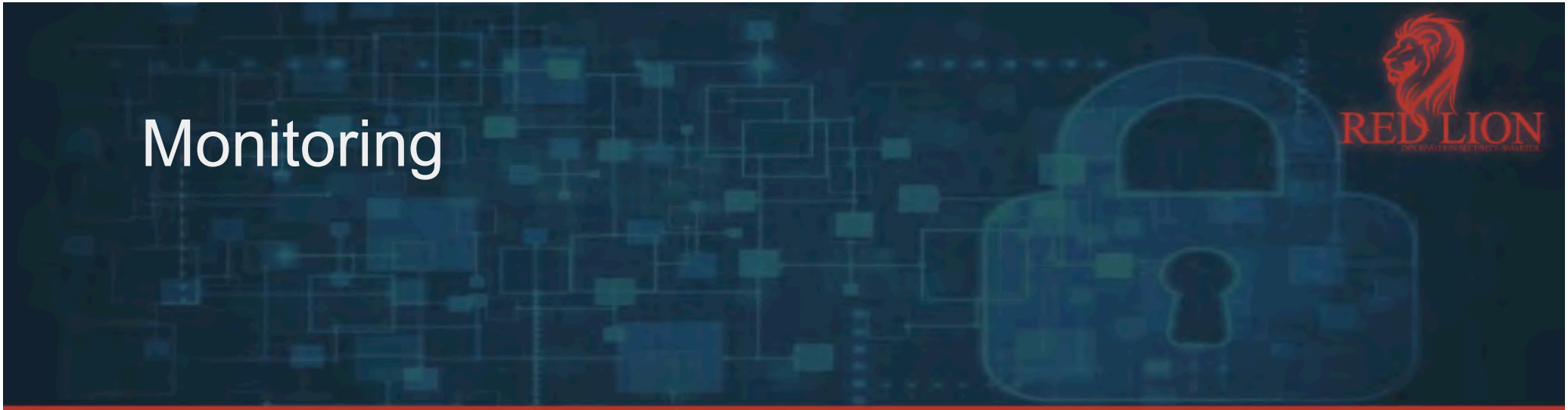


Systems, processes, and people should be monitored for efficiency, malfunction, and malicious behavior.

Monitoring

- Technology
  - Systems
  - Applications
  - Devices
- Workflow
  - Process
  - Steps
  - Audit/Evidence

Monitoring



How many applications do your workers use?

How many people have access to assets?

Who checks the logs? How often?

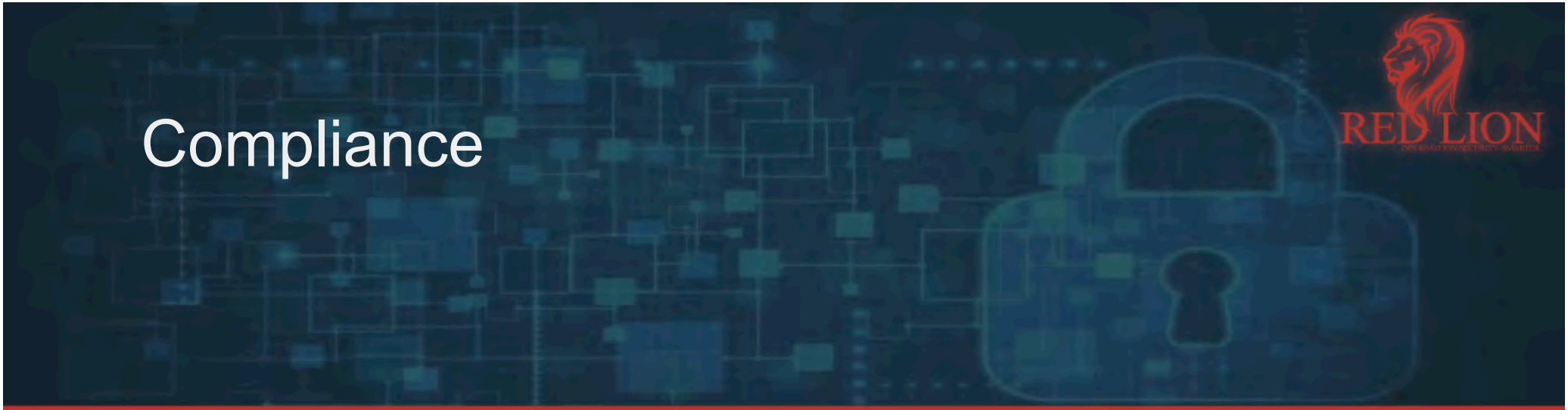
Compliance

Following established industry standards to perform quality work, with acceptable process and methodologies.

Compliance

- HIPAA
- PCI
- NIST 800-171
- DFARS/FARS
- GDPR
- Etc etc etc

Compliance



What standards are you under?

Are you ready?

Who handles compliance in your organization?

Cost vs. Revenue Center

- *Does Security and Compliance?*
- *Cost you money?*
- *Or make you money?*

Cost Vs. Revenue

- Sales Friction
- Sales Cycle lengthening
- Sales bottleneck
- Lost opportunities
- Unpaid pre-sales costs you money
- Security and compliance questionnaires cost

Cost vs. Revenue

What is your biggest sales friction bottleneck?

How long does your sales cycle get?

Can we help you solve that bottleneck?

Questions?

Joshua Marpet

@quadling
Jmarpet@redlion.io

Scott Lyons

@csp3r
Slyons@redlion.io

Red Lion

202-559-9365

Information Security
- Smarter