Mid-Range Michiana Users Group

RANDY JONES, CISSP

SECURITY ARCHITECT

Today’s security challenges

ADVANCED ATTACKS

HUMAN ERROR

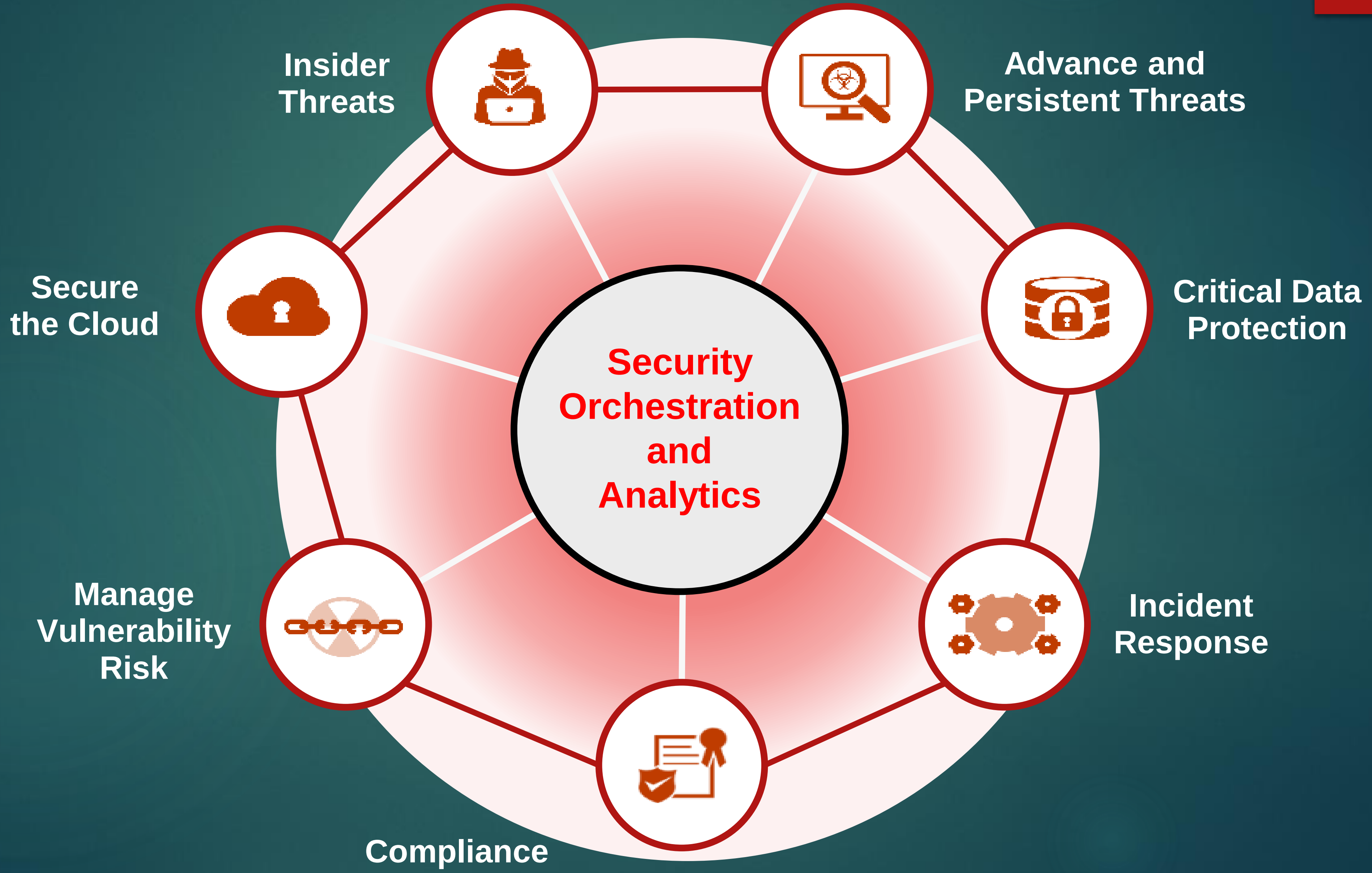
INNOVATION

COMPLIANCE

SKILLS GAP

TIME

Todays security operations priorities


Security Orchestration and Analytics
Insider Threats
Advance and Persistent Threats
Critical Data Protection
Incident Response
Compliance
Manage Vulnerability Risk
Secure the Cloud

How do they get inside the network?

- Users
- Application vulnerability
- Traditional methods
- Advanced non-malware attacks

- Spam, phising, spear phising, human error, malicious internal users
- Not current on patches
  - Client applications
- Applications not secure
  - SQL Injection
  - Cross-site scripting
  - Hardcoded default passwords
- Common system tools used maliciously
  - no malware files downloaded
  - Anomaly detection needed

2018 Verizon Data Breech Report
Where are we?

- ***Ransomware and social attacks have been the big stars in the past year when it comes to cybersecurity,*** according to the latest edition of Verizon's popular yearly report.
- Drawing from datasets aggregated from 67 other organizations, including 53,308 security incidents and 2,216 data breaches, Verizon's 2018 Data Breach Investigations Report shows that ransomware was the most common type of malware reported. ***Based on 1,379 malware incidents, 56 percent involved ransomware.***
- Ransomware **is seen as so effective**, Verizon says, **because it can be attempted with little risk to the attackers, doesn't require them monetize stolen data and can have a larger impact when deployed against large organizations like corporations or local governments.**
- **"It is now the most prevalent form of malware, and its use has increased significantly over recent years,"** said Bryan Sartin, executive director of security professional services at Verizon in a press release. "What is interesting to us is that businesses ***are still not investing in appropriate security strategies to combat ransomware,*** meaning they end up with no option but to pay the ransom – the cybercriminal is the only winner here!"

Biggest risks per industries analyzed

- **Education** – Social engineering targeting personal information is high, which is then used for identity fraud. Highly sensitive research is also at risk, with 20 percent of attacks motivated by espionage. Eleven percent of attacks also have "fun" as the motive rather than financial gain.
- **Financial and insurance** – Payment card skimmers installed on ATMs are still big business; however, we're also now seeing a rise in "ATM jackpotting," where fraudulently installed software or hardware instructs the ATMs to release large amounts of cash. DDoS attacks are also a threat.
- **Healthcare** – This is the only industry where insider threats are greater than threats from the outside. Human error remains a major contributor to healthcare risks.
- **Information** – DDoS attacks account for over half (56 percent) of the incidents within this sector.
- **Public sector** – Cyber-espionage remains a major concern, with 43 percent of breaches being espionage motivated. However, it is not only state-secrets that are a target - personal data is also at risk.

What can we do?

1. Stay vigilant - log files and change management systems can give you early warning of a breach.

2. ***Make people your first line of defense - train staff to spot the warning signs.***

3. Keep data on a “need to know” basis - ***only employees that need access to systems to do their jobs should have it.***

4. ***Patch promptly*** - this could guard against many attacks.

5. ***Encrypt sensitive data*** - make your data next to useless if it is stolen.

6. Use two-factor authentication - this can limit the damage that can be done with lost or stolen credentials. ***Weak passwords is still the most effective method to compromise admin credentials***

7. Don’t forget physical security - not all data theft happens online.

There is no silver bullet

- Defense in depth
- User Security Awareness training
- Next Generation Anti-Virus
- SIEM (security information event management)
- Security Intelligence
- Compensating controls
- Privileged User Account management
- Separation of duties
- Data classification and identification
- Regular DR and BC simulations
- Security compliance standards as a guide in endpoint plans
- **Stay current on patches**

Thank you for your time