# Cybersecurity Readiness & Resilience for your Business

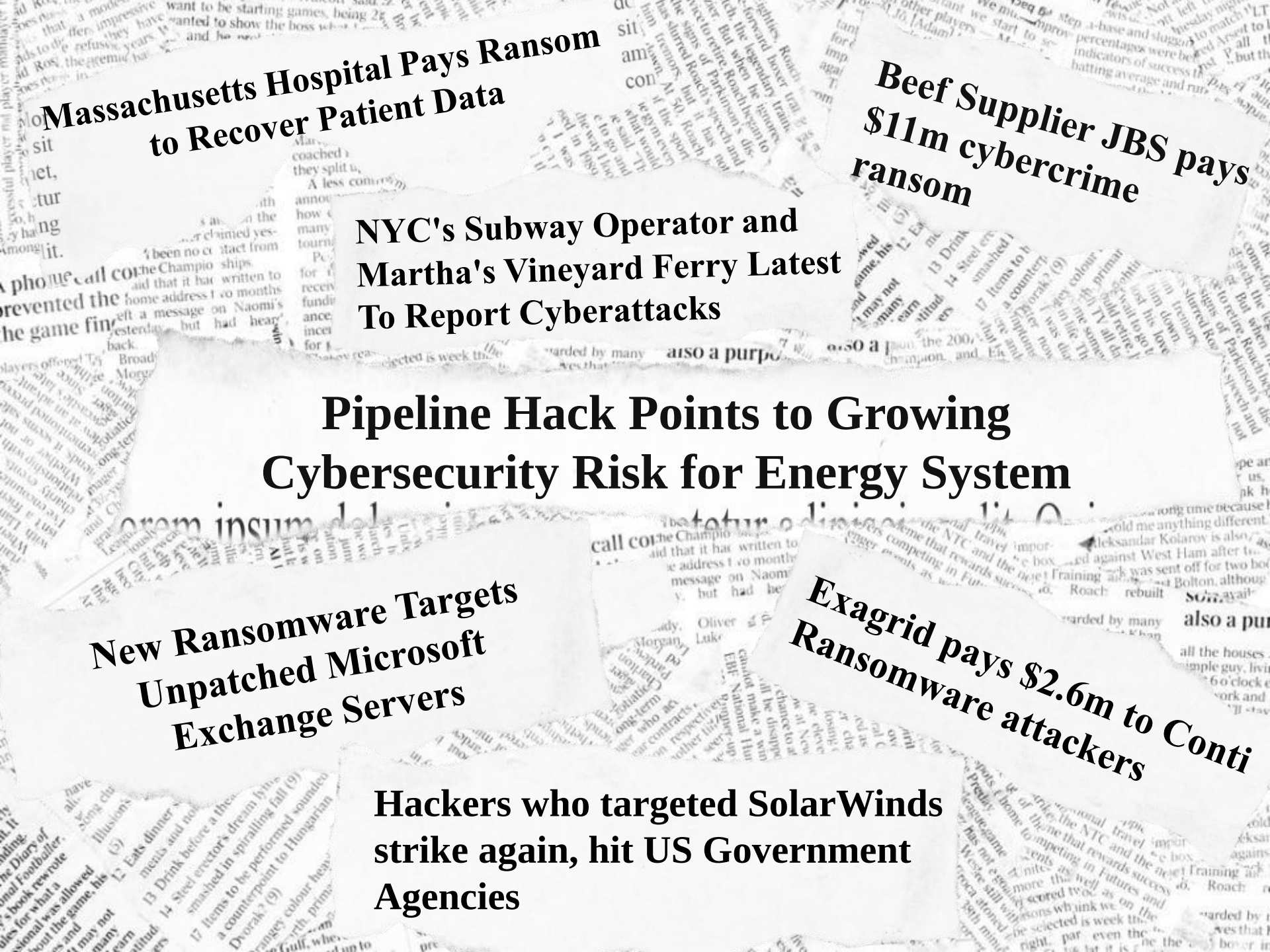
Presented By:
**David D'Agostino**
Director of 1nteger Security



111 Grant Ave. Suite 108 Endicott NY 13760 | 607-484-6930

# Agenda:

- Current Threat Landscape
- Understanding Threats, Vulnerabilities & Risk
- Cyber-resilience
- Defense in Depth Strategy
- 1nteger ONE
- What to do if hit by a ransomware attack


Massachusetts Hospital Pays Ransom to Recover Patient Data
Beef Supplier JBS pays $11m cybercrime ransom
NYC's Subway Operator and Martha's Vineyard Ferry Latest To Report Cyberattacks
Pipeline Hack Points to Growing Cybersecurity Risk for Energy System
New Ransomware Targets Unpatched Microsoft Exchange Servers
Exagrid pays $2.6m to Conti Ransomware attackers
Hackers who targeted SolarWinds strike again, hit US Government Agencies

*Recent ransomware attacks against critical infrastructure help us understand standards and practices that would have helped. For example,* ***multi-factor authentication (MFA****), a widely recognized best practice, may have prevented the Colonial Pipeline hack. According to GAO, greater and more consistent adoption of the* ***NIST CSF,*** *which was specifically developed to help critical infrastructure manage cyber risk, would benefit cyber risk management efforts across all critical infrastructure sectors.*

*-FORBES*

# Have you experienced a ransomware attack in the past?

# Understanding Threats, Vulnerabilities and RISK


Anything that can exploit a vulnerability, intentionally or accidently and obtain, damage or destroy an asset

Weakness or gaps in a security program that can be exploited by threats to gain unauthorized access

The potential for loss, damage or destruction of an asset as a result of a threat exploiting a vulnerability

# Top 5 Cybersecurity Threats for Small Businesses in 2021

- Phishing, vishing, smishing
- Credential theft
- Ransomware
- Personal devices accessing corporate systems
- Cloud computing

https://insights.samsung.com/2021/01/11/top-5-cybersecurity-threats-for-small-businesses-in-2021/

# Threat Landscape

## Phishing on the rise and highly effective

- **94%** of malware arrives from email
- More than **80%** of reported security incidents are phishing-related

## Ransomware

- In Q1 of 2021 **51%** of US Companies reported a Ransomware Attack
- The average Ransomware Payment in 2021 increased by **82%** YOY to **$570,000.00**

## Exploitation of outdated / misconfigured security controls

- Attacks are on the rise- **43%** Target small businesses
- Increase in advance style attacks
- "RAAS" is real and the ransom amount increasing everyday due to extortion tactics

2021 State Of Ransomware –Sophos

# Common Vulnerabilities

- SMB Attack surface is growing rapidly
  - Cloud
  - Remote workers
- Discovery of viruses or malware is taking too long
- Employees are falling victim to phishing tactics that expose the network to threats
- Known flaws are not being patched and updates are ignored
- Security policies are not defined or enforced
- Missing or poorly implemented encryption
- Lack of malware protection
- Business partners or supply chains are not always fully secure

Do you & your Executive team really understand your Cyber Risks?

# When was the last time you had a Cyber Risk Assessment Performed?

**A) in last 12 months**

**B) 12-24 months**

**C) 24-48 months**

**D) Never**

# NIST Cybersecurity Framework

Recovery Planning, BCDR

Asset Management, Risk Assessment,


Incident Response planning, SOAR, Analysis, Mitigation

Access Control, Awareness Training, Protective tech, Maintenance

Continuous Monitoring, Anomalies & Events

# 5 Tips to Improve Cyber-Resilience for SMB

1. Fortify your weakest link
2. Advanced threats require advanced antivirus
3. Deploy backup policies for all business
4. Use the cloud to ensure remote file access
5. Test Recovery Strategy regularly

CISA CYBER+INFRASTRUCTURE

https://us-cert.cisa.gov/resources/assessments


# ONE

## The Proactive Approach to Security

**ONE Team, ONE Plan, ONE Affordable Solution**

111 Grant Ave. Suite 108 Endicott NY 13760 | 607-484-6930

## Cybersecurity Services Providing more than just technology, 1nteger ONE provides a Proactive approach with a proven outcome.

- Improved Cyber Resilience
- Proactive Control Verification
- Active Threat Detection
- Dedicated Team of Cybersecurity Professionals

# 1nteger ONE

## People 

- Dedicated Security Consultant (vCISO)
- Project Manager
- Security Analyst
- SOC Engineers
    - Level 1
    - Level 2

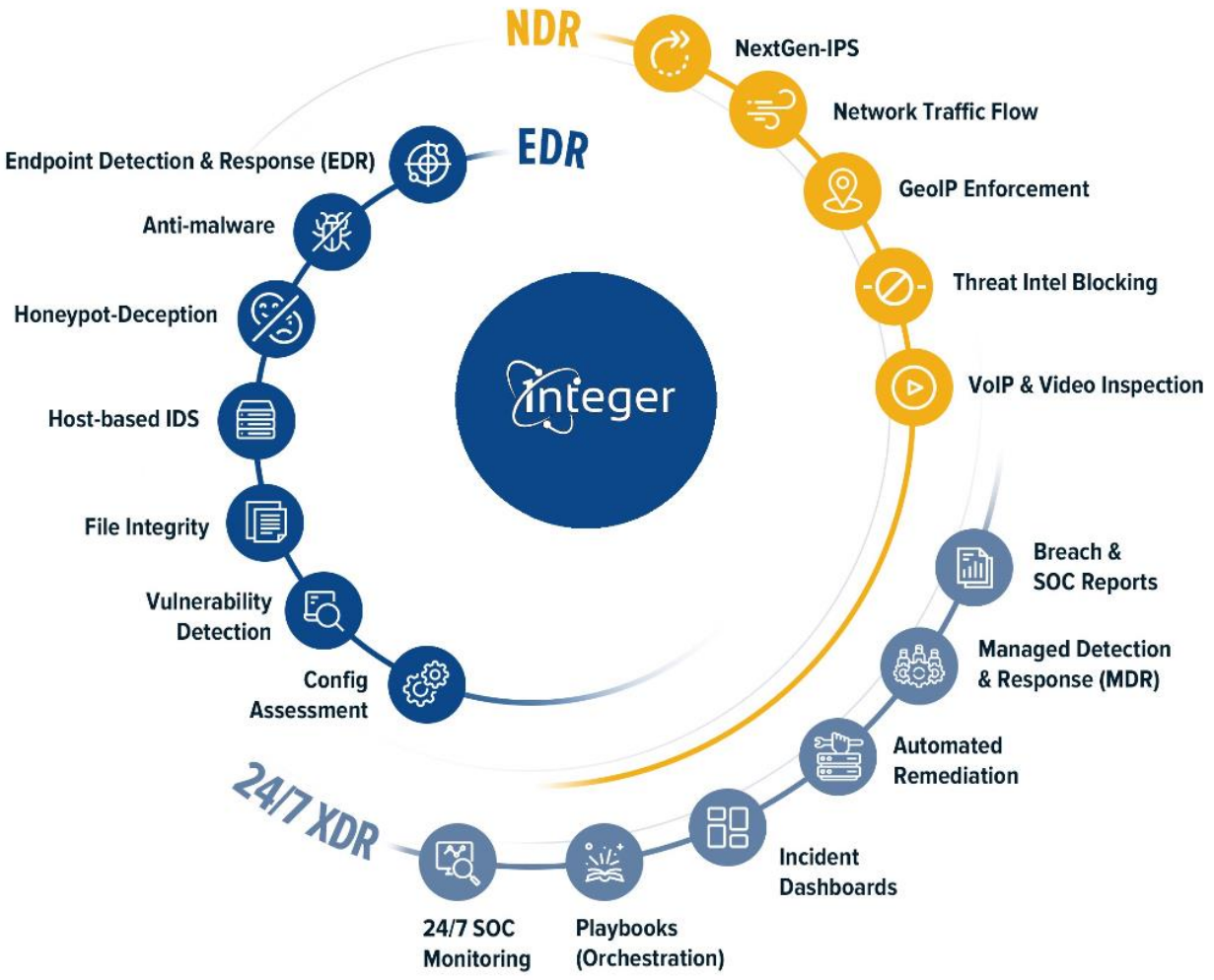
## Process 

- Documented onboarding
- Proactive Security Review
- Continuous SIEM Tunning
- Continuous Vulnerability Scanning
- Threat Hunting (24x7 SOC)
- Honeypot Deception
- Incident Response Playbook
- Alignment to NIST CSF Framework
- Risk Assessment
- Quarterly Consulting Review

## Technology 

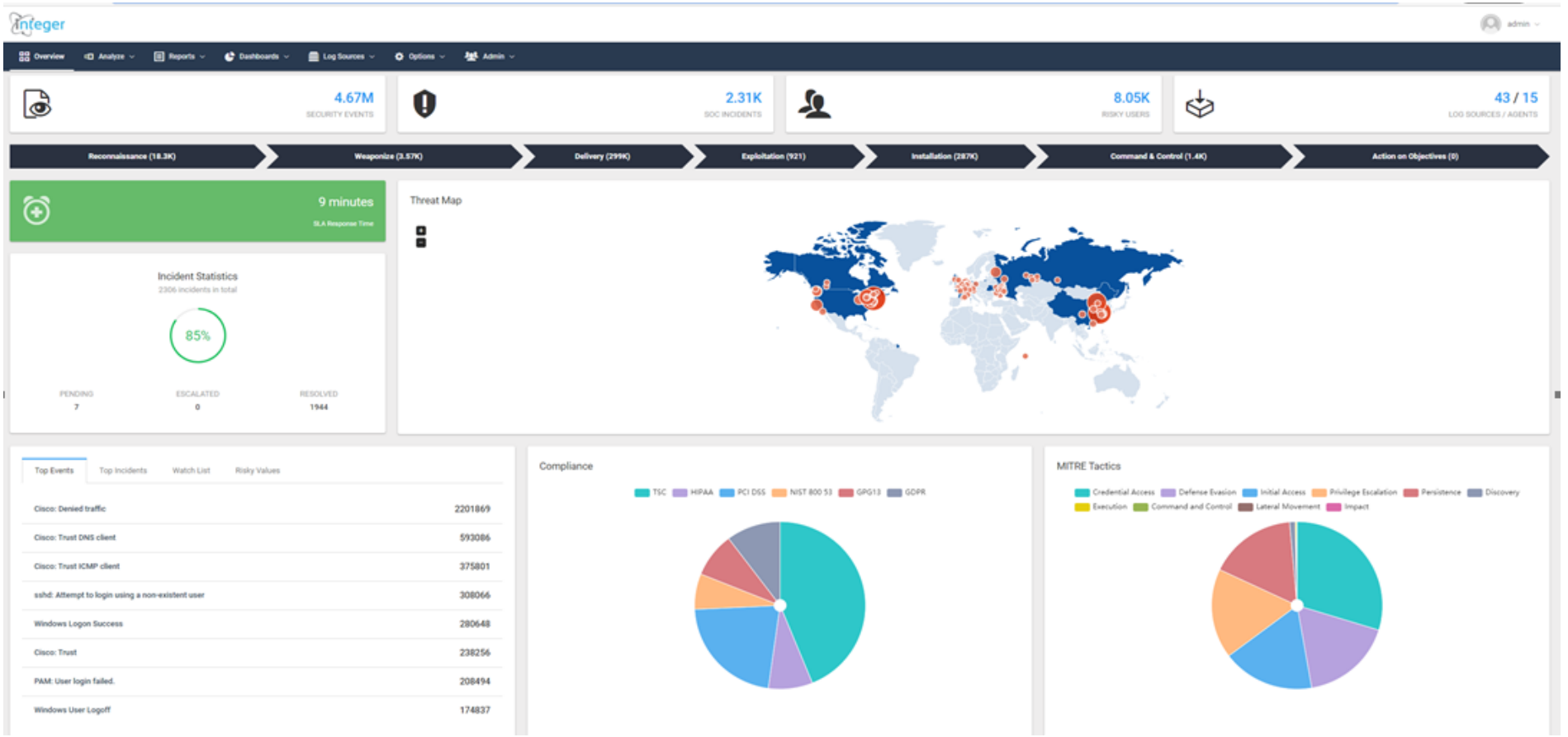
- Vulnerability Scanner
- Endpoint Security Agent
- Log Collection/Retention
- SIEM (Security information & Event Management)
- Next Gen IDS/IPS
- Cloud integration
- API integration
- Live Dashboard Access
- Dark web Monitoring
- Security Awareness Training

# 1nteger ONE – Live Demo

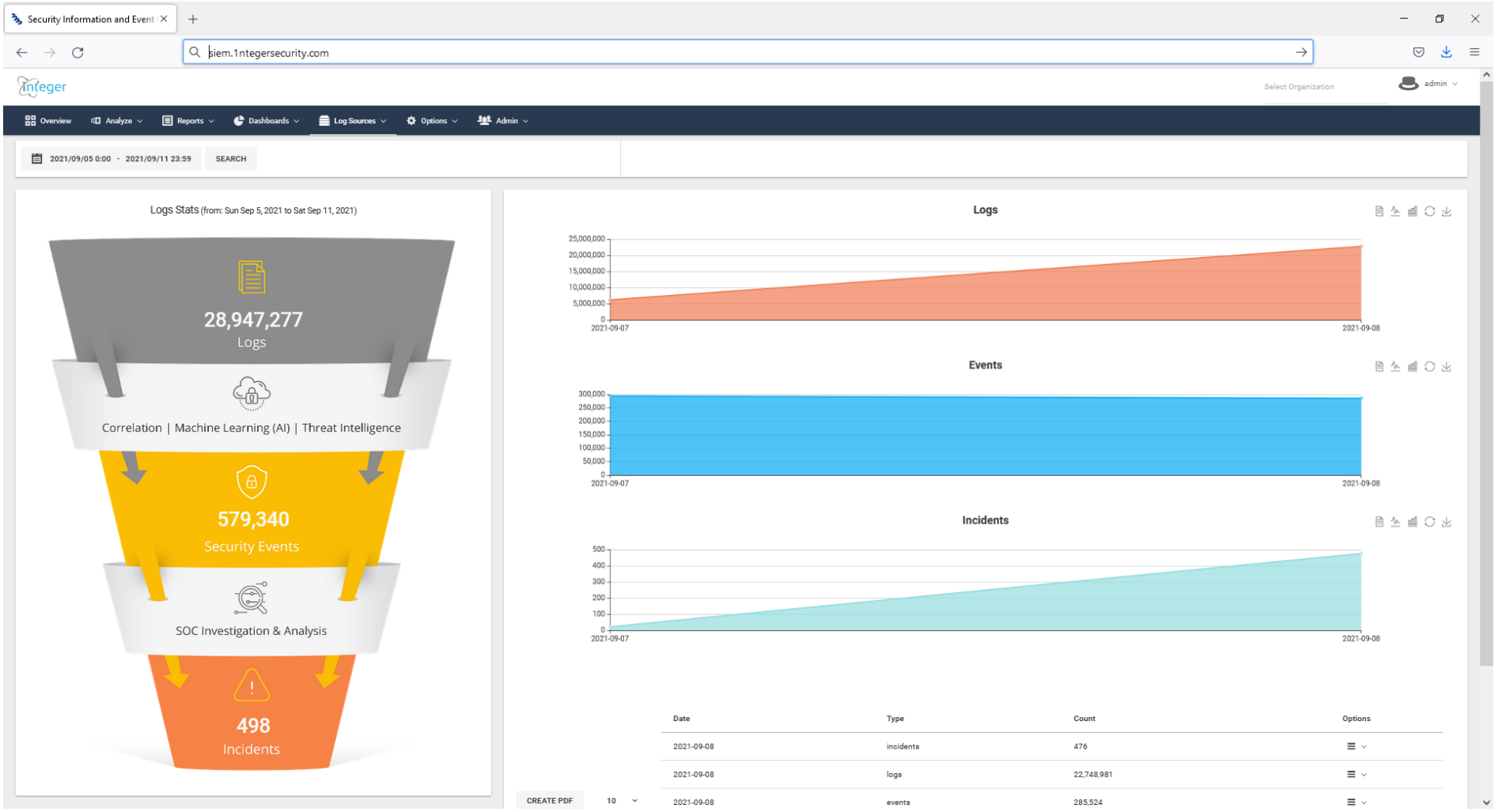


# Products and Services

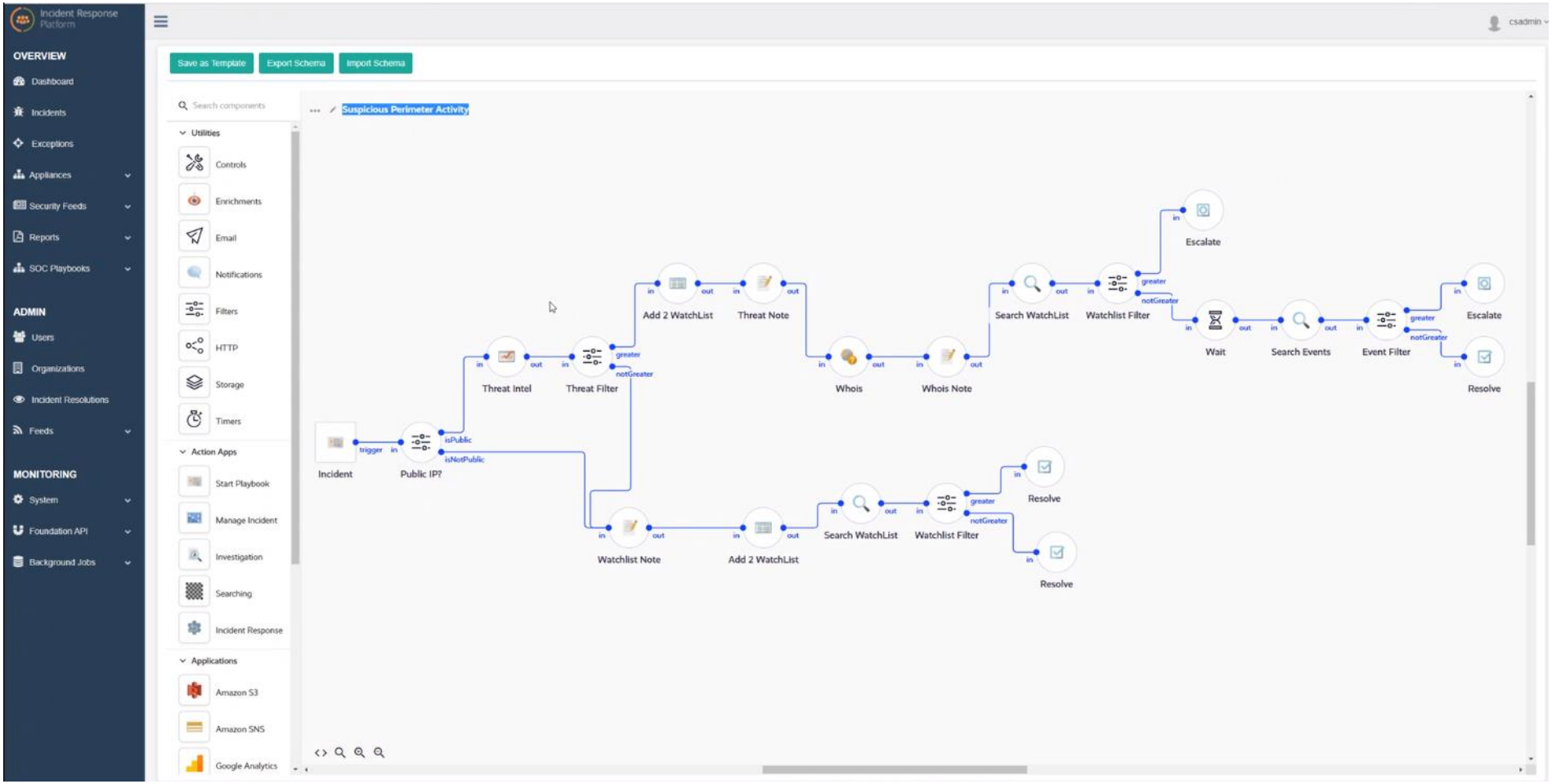
## 1nteger ONE Portal



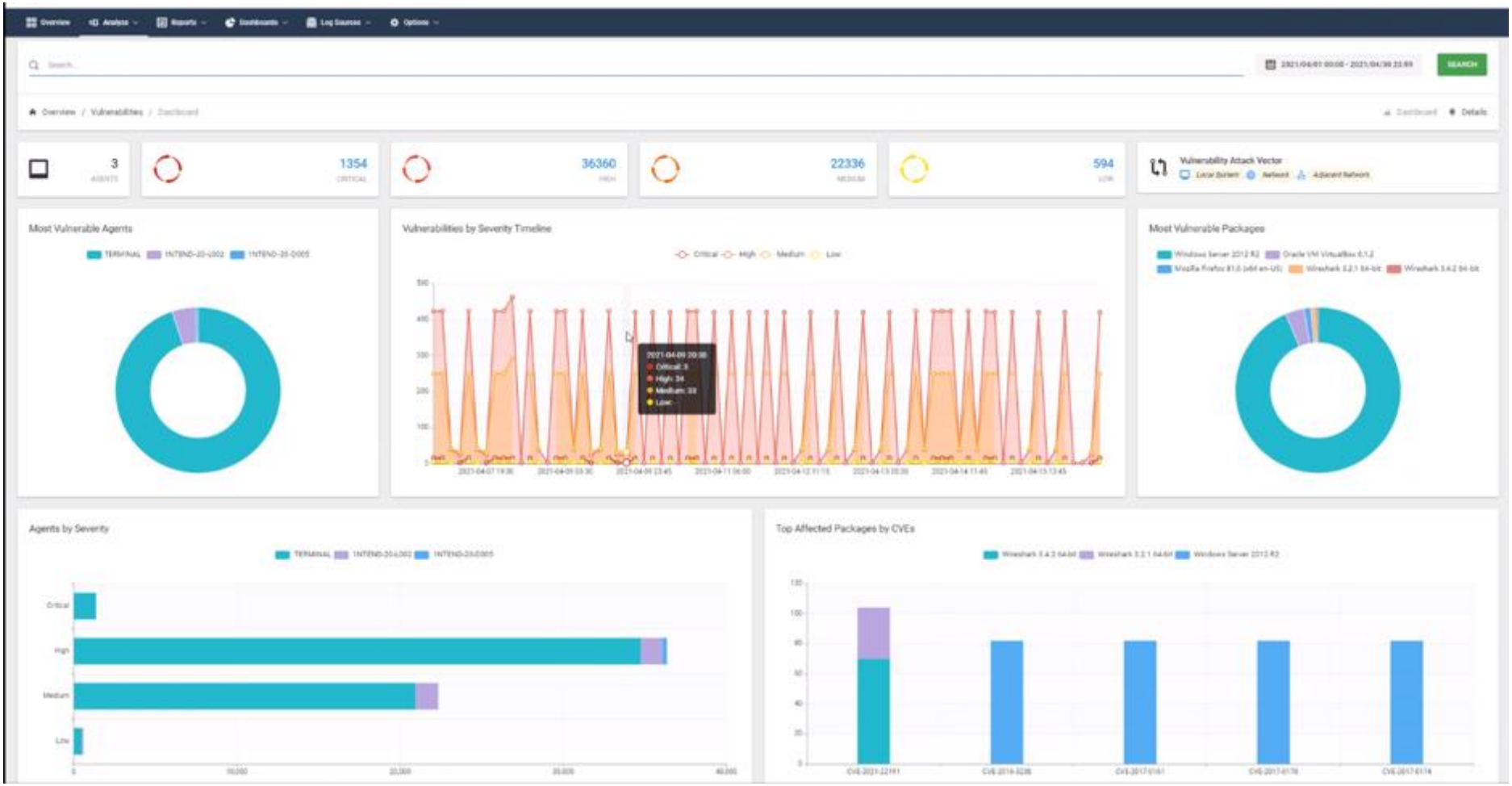
# 1nteger ONE Portal



# Incident Response Playbook



# Vulnerability Management



# Defense in Depth Top 10

1. Backup/Business Continuity
2. Endpoint Protection (EDR- Encryption, Port Protection)
3. Two-Factor Authentication
4. User Awareness Training *
5. Continuous Vulnerability Management *
6. XDR & SIEM *
7. Active threat monitoring and detection*
8. Incident Response Management *
9. Risk Assessments *
10. Proactive Review & Validation *

*included with ONE

# How confident are you in your company's ability to Identify, respond, remediate, and recover from a cyber-attack?

**A) Very Confident**

**B) Somewhat Confident**

**C) Not Confident**

# What to do if your business is hit by a ransomware attack

**Activate the Incident Response Plan (if you have one)**

- Isolate systems- stop the spread
- Identify Ransomware variant
- Identify Initial Access
- Identify all infected systems
- Determine if data was Exfiltrated

**Consider Impact**

**Inform PR/Legal Teams/Cyber Insurance***

**Recover**

- Locate, verify, and re-store backups
- Sanitize Systems or create new build

**Postmortem Review**

- Root cause analysis
- Lessons learned/Required remediation steps

# Does your organization have a Cyber Liability Insurance Policy?

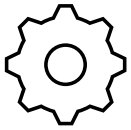
**A) Yes**

**B) No**

**C) Not Sure**

# Questions

# What Makes 1nteger Different?



Attestation + Tools + ***Control Verification!***

Finding the balance

- How much security is enough? JUST enough.
- Cost of Control < Cost of Impact

Help you determine and manage risk *first*

An entire team of Security experts focused our client's infrastructure, polices, and risk

The Value, the partnership, the results


# Thank You

www.1ntegersecurity.com
info@1ntegersecurity.com

Presented By:
**David D'Agostino**
Director of 1nteger Security

111 Grant Ave. Suite 108 Endicott NY 13760 | 607-484-6930