



Cybersecurity Readiness & Resilience for your Business



Presented By:
David D'Agostino
Director of Integer Security

Agenda:

- Current Threat Landscape
- Understanding Threats, Vulnerabilities & Risk
- Cyber-resilience
- Defense in Depth Strategy
- Integer 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 accidentally 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

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Exploitation of outdated / misconfigured security controls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



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



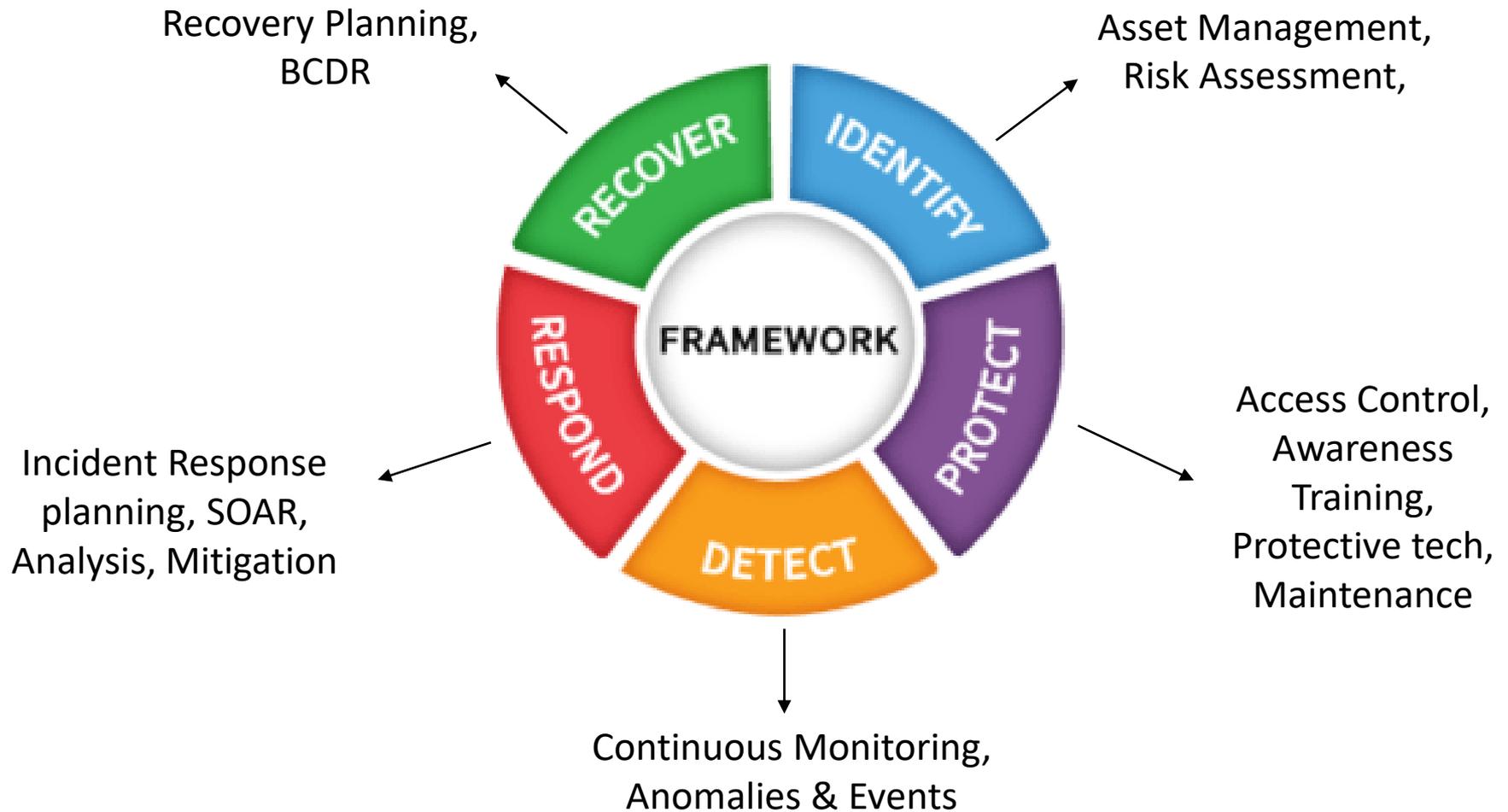


Do you & your
Executive team
really understand
your Cyber Risks?

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



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>

The logo features the word "Integer" in a blue sans-serif font, with a large grey number "1" to its left. A stylized atom graphic with three grey orbits and three grey spheres is positioned around the "1". Below "Integer" is the word "ONE" in a blue, outlined, sans-serif font. The background includes a large grey atom graphic and a blue geometric shape on the right side.

Integer ONE

The Proactive Approach
to Security

ONE Team, ONE Plan, ONE Affordable Solution

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



Improved Cyber Resilience



Proactive Control Verification



Active Threat Detection



Dedicated Team of Cybersecurity Professionals

Integer ONE

People

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

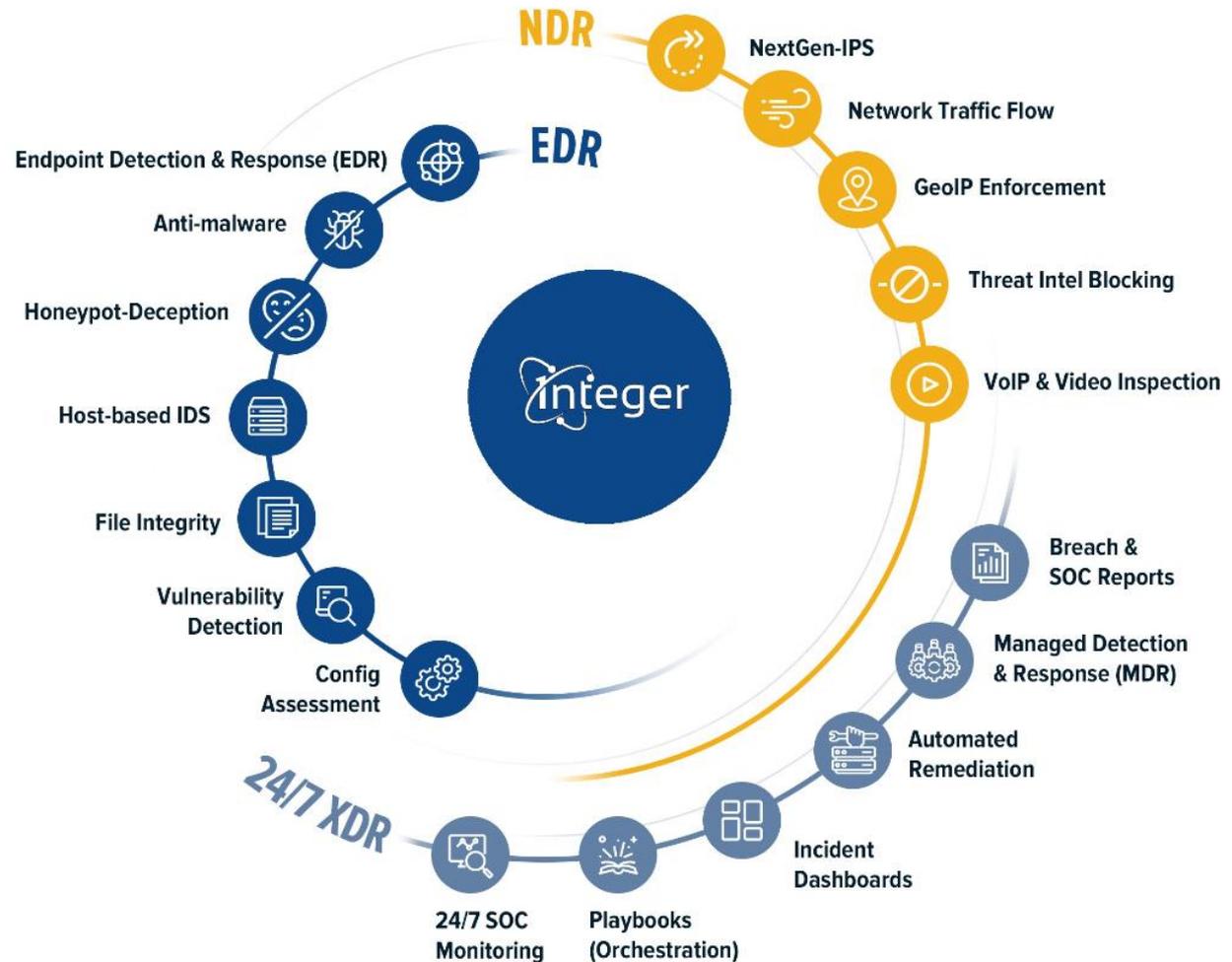
Process

- Documented onboarding
- Proactive Security Review
- Continuous SIEM Tuning
- 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

Integer ONE – Live Demo



Products and Services

Integer ONE Portal

The dashboard provides a comprehensive overview of security operations. At the top, navigation tabs include Overview, Analyze, Reports, Dashboards, Log Sources, Options, and Admin. Key metrics are displayed in a header bar: 4.67M Security Events, 2.31K SOC Incidents, 8.05K Risky Users, and 43/15 Log Sources / Agents. A process flow bar shows stages from Reconnaissance (18.3K) to Action on Objectives (0).

Incident Statistics: 2306 incidents in total, with an 85% resolution rate. A 9-minute SLA Response Time is indicated. The status breakdown is: PENDING (7), ESCALATED (0), and RESOLVED (1944).

Threat Map: A world map showing incident locations with red and orange markers, primarily concentrated in North America and Europe.

Top Events Table:

Event	Count
Cisco: Denied traffic	2201869
Cisco: Trust DNS client	593086
Cisco: Trust ICMP client	375801
sshd: Attempt to login using a non-existent user	308066
Windows Logon Success	280648
Cisco: Trust	238256
PAM: User login failed.	208494
Windows User Logoff	174837

Compliance: A pie chart showing adherence to various standards: TSC, HIPAA, PCI DSS, NIST 800 53, GPG13, and GDPR.

MITRE Tactics: A pie chart illustrating the distribution of MITRE attack tactics: Credential Access, Defense Evasion, Initial Access, Privilege Escalation, Persistence, Discovery, Execution, Command and Control, Lateral Movement, and Impact.

Integer ONE Portal

Security Information and Event X +

siem.1integersecurity.com

integer Select Organization admin

Overview Analyze Reports Dashboards Log Sources Options Admin

2021/09/05 0:00 - 2021/09/11 23:59 SEARCH

Logs Stats (from: Sun Sep 5, 2021 to Sat Sep 11, 2021)

28,947,277
Logs

Correlation | Machine Learning (AI) | Threat Intelligence

579,340
Security Events

SOC Investigation & Analysis

498
Incidents

Logs

Events

Incidents

Date	Type	Count	Options
2021-09-08	incidents	476	☰ ▼
2021-09-08	logs	22,748,981	☰ ▼
2021-09-08	events	285,524	☰ ▼

CREATE PDF 10

Incident Response Playbook

The screenshot displays the Incident Response Platform interface. On the left is a dark sidebar with navigation menus for Overview, Admin, and Monitoring. The main area shows a flowchart for a playbook titled "Suspicious Perimeter Activity".

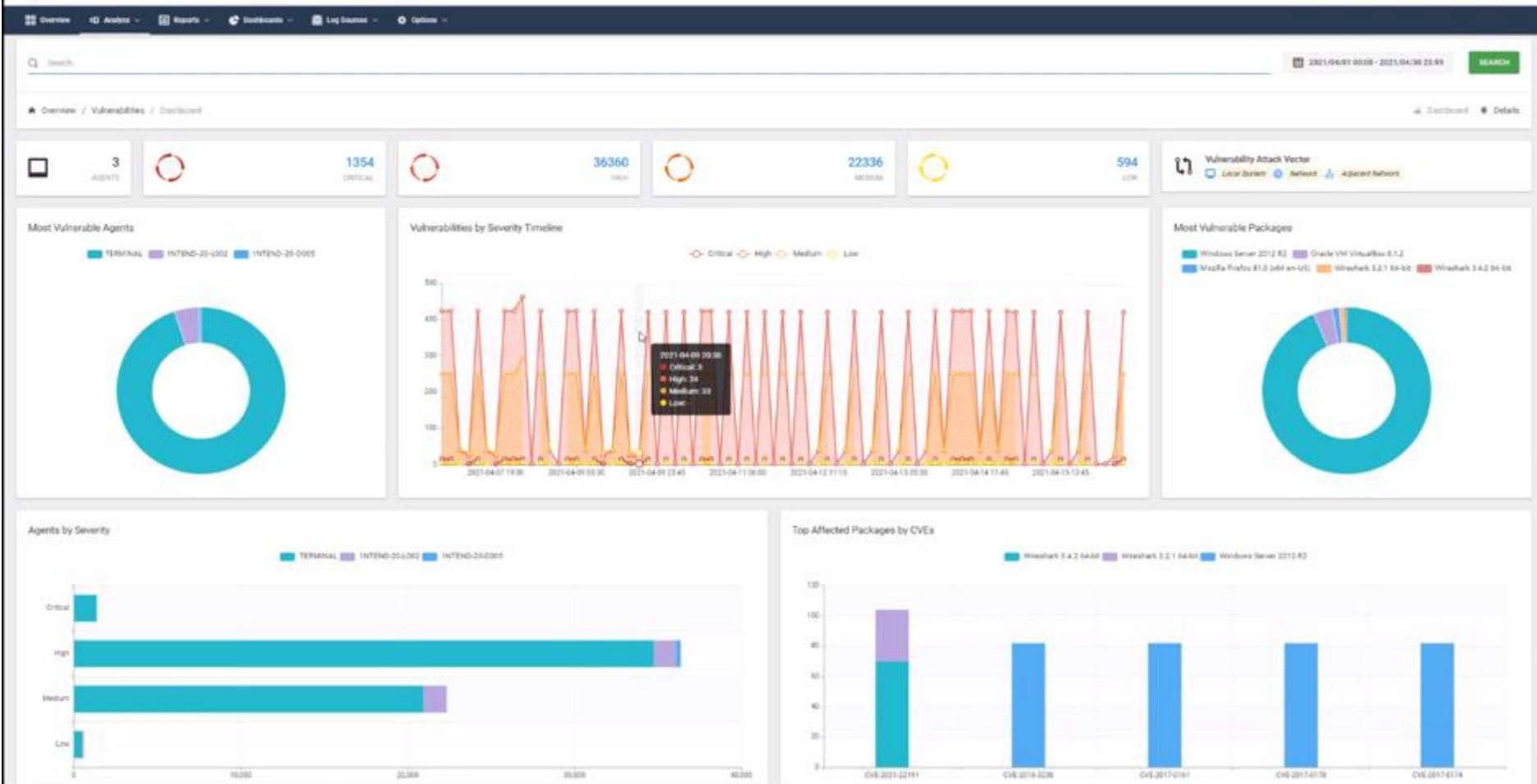
Playbook Flow:

- Incident** (Trigger) → **Public IP?** (Filter: isPublic, isNotPublic)
- Public IP?** (isPublic) → **Threat Intel** (Action) → **Threat Filter** (Filter: greater, notGreater)
- Public IP?** (isNotPublic) → **Watchlist Note** (Action) → **Add 2 WatchList** (Action) → **Search WatchList** (Action) → **Watchlist Filter** (Filter: greater, notGreater) → **Resolve** (Action)
- Threat Filter** (greater) → **Add 2 WatchList** (Action) → **Threat Note** (Action) → **Whois** (Action) → **Whois Note** (Action)
- Threat Filter** (notGreater) → **Search WatchList** (Action) → **Watchlist Filter** (Filter: greater, notGreater) → **Escalate** (Action)
- Whois Note** → **Search WatchList** (Action) → **Watchlist Filter** (Filter: greater, notGreater) → **Wait** (Action) → **Search Events** (Action) → **Event Filter** (Filter: greater, notGreater) → **Escalate** (Action) / **Resolve** (Action)

Component List (Left Panel):

- Utilities: Controls, Enrichments, Email, Notifications, Filters, HTTP, Storage, Timers
- Action Apps: Start Playbook, Manage Incident, Investigation, Searching, Incident Response
- Applications: Amazon S3, Amazon SNS, Google Analytics

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?

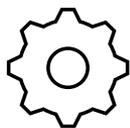
A) Yes

B) No

C) Not Sure

Questions

What Makes Integer Different?



Attestation + Tools + Control Verification!



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



Finding the balance

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



Help you determine and manage risk *first*



The Value, the partnership, the results



Thank You

www.1integersecurity.com
info@1integersecurity.com

Presented By:

David D'Agostino

Director of Integer Security