# Cybersecurity Preparedness

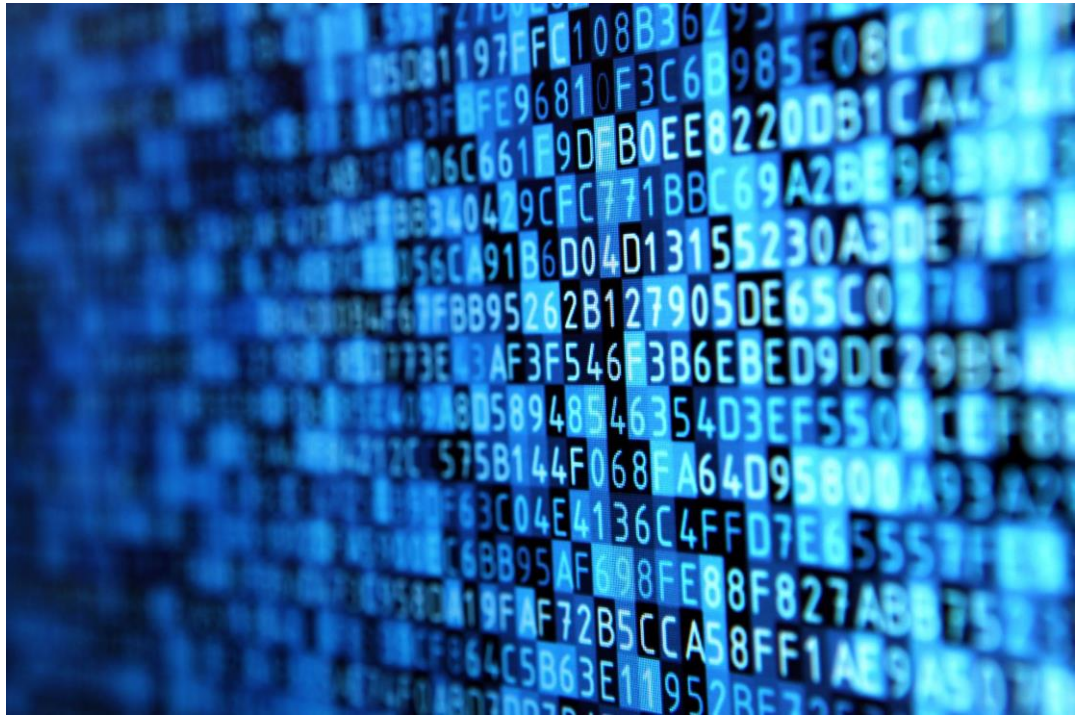
ADS role in cybersecurity planning and response

# Overview

- Current and ongoing threats
- ADS Incident Response process
- Cyber Annex and ADS coordination

# Persistent threats

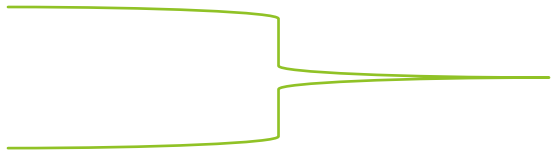
- Phishing scams
- Malware
- Data breaches
- Denial of service
- Brute force attacks
- Spyware
- Credential theft
- Ransomware



# Goals

A cybercriminal is a person who conducts some form of illegal activity using computers or other digital technology such as the Internet. The criminal may use computer expertise, knowledge of human behavior, and a variety of tools and services to achieve his or her goal.

- Data theft for profit
- File encryption for ransom
- Persistence for monitoring and eavesdropping
- Disruption – politics or popularity
- Vandalism



Hacktivism

# Current threats

- Advanced Persistent Threats (APTs)
  - Russian-based actor targeting healthcare, financial, and government among others
  - No current activity with State, but over 3M attempts the last 45 days nationwide
  - Names like Mummy Spider and Cozy Bear – allow for threat profiles and tracking of activities.
  - Overwhelms network hardware or servers to deny availability of the resource
- Distributed denial of service
  - Flooding the target with traffic, or sending it information that causes the system to crash, making it unavailable
  - Often comes from multiple sources and is difficult to block
- HermeticWiper
  - Bypasses windows security features to overwrite contents of the computer
- Website defacement
  - Reduces confidence in hosting organization
- Disinformation
  - Creates chaos and indecision

# Goals

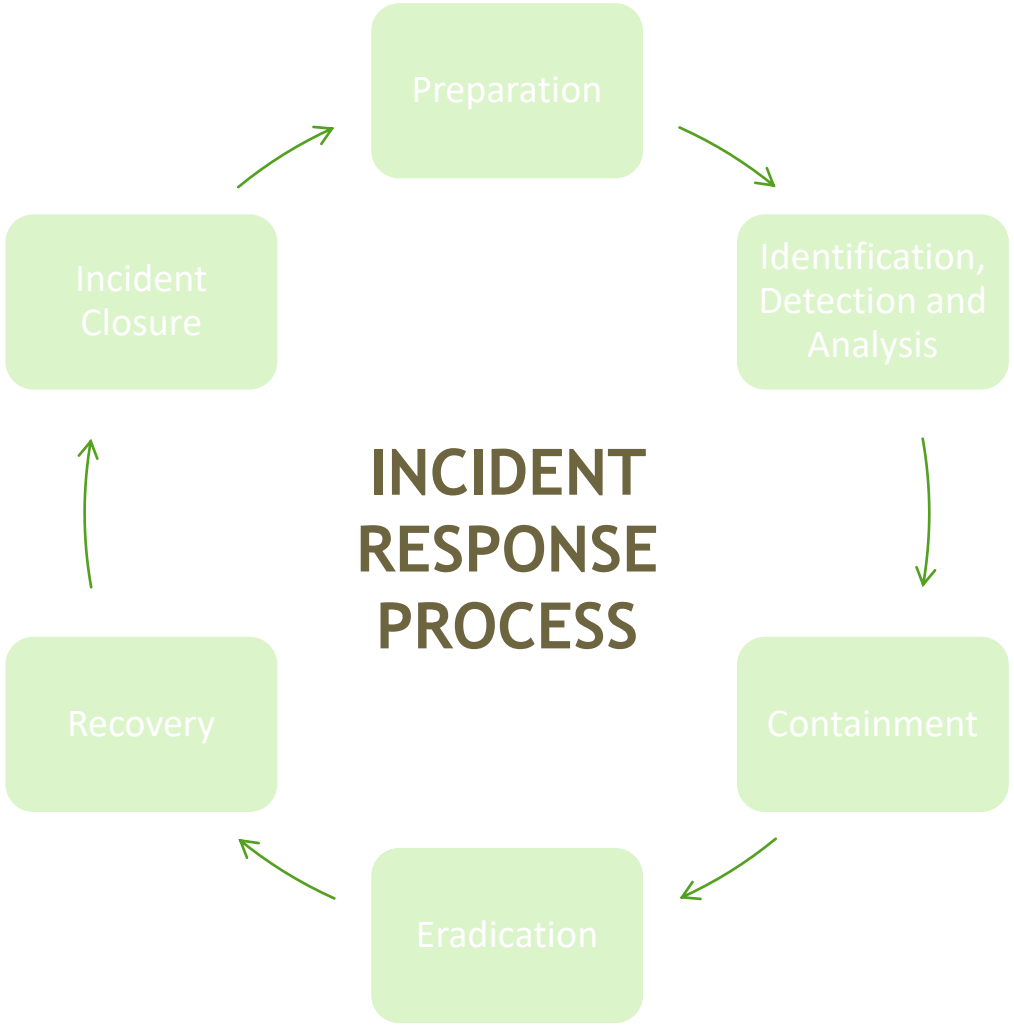
- Non-kinetic warfare (asynchronous)
  - include disinformation campaigns, cyber attacks, and economic espionage against federal, state, and local governments to gain strategic and economic advantages over the United States
  - Can be executed by a much weaker opponent against a stronger opponent
- Damage and disrupt critical services
  - Colonial pipeline, hospital ransomware attacks
- Exact a cost for opposition
  - Threaten, demonstrate, attack – escalation path
- Influence opponent's population
  - Gas prices, business and profits
- Theft of intellectual property
  - Defense tech, high tech sector, aviation
- Espionage
  - Knowing what their adversary decision makers thought and plans may be

# Cyber Incident Response

- “At a glance” incident response workflow
- Severity index
- Follows established principles for cyber response
- Establishes notification and broader notice to internal and external partners

| Classification | Definition |
|---|---|
| Level 5<br>Emergency<br>(Black) | Poses an immediate threat to the provision of wide-scale critical infrastructure services, government stability, or the lives of Vermonters |
| Level 4<br>Severe<br>(Red) | Likely to result in a significant impact to public health or safety, economic security, civil liberties, or public confidence |
| Level 3<br>High<br>(Orange) | Likely to result in a demonstrable impact to public health or safety, economic security, civil liberties, or public confidence |
| Level 2<br>Medium<br>(Yellow) | May impact public health or safety, economic security, civil liberties, or public confidence |
| Level 1<br>Low<br>(Green) | Unlikely to result in a demonstrable impact to public health or safety, economic security, civil liberties, or public confidence |
| Level 0<br>Baseline<br>(White) | Unsubstantiated or inconsequential event |

# INCIDENT RESPONSE PROCESS




Maintaining and improving incident response capabilities and preventing incidents by ensuring that systems, networks, and applications are sufficiently secure.

Confirming, characterizing, classifying, categorizing, scoping, and prioritizing suspected incidents.

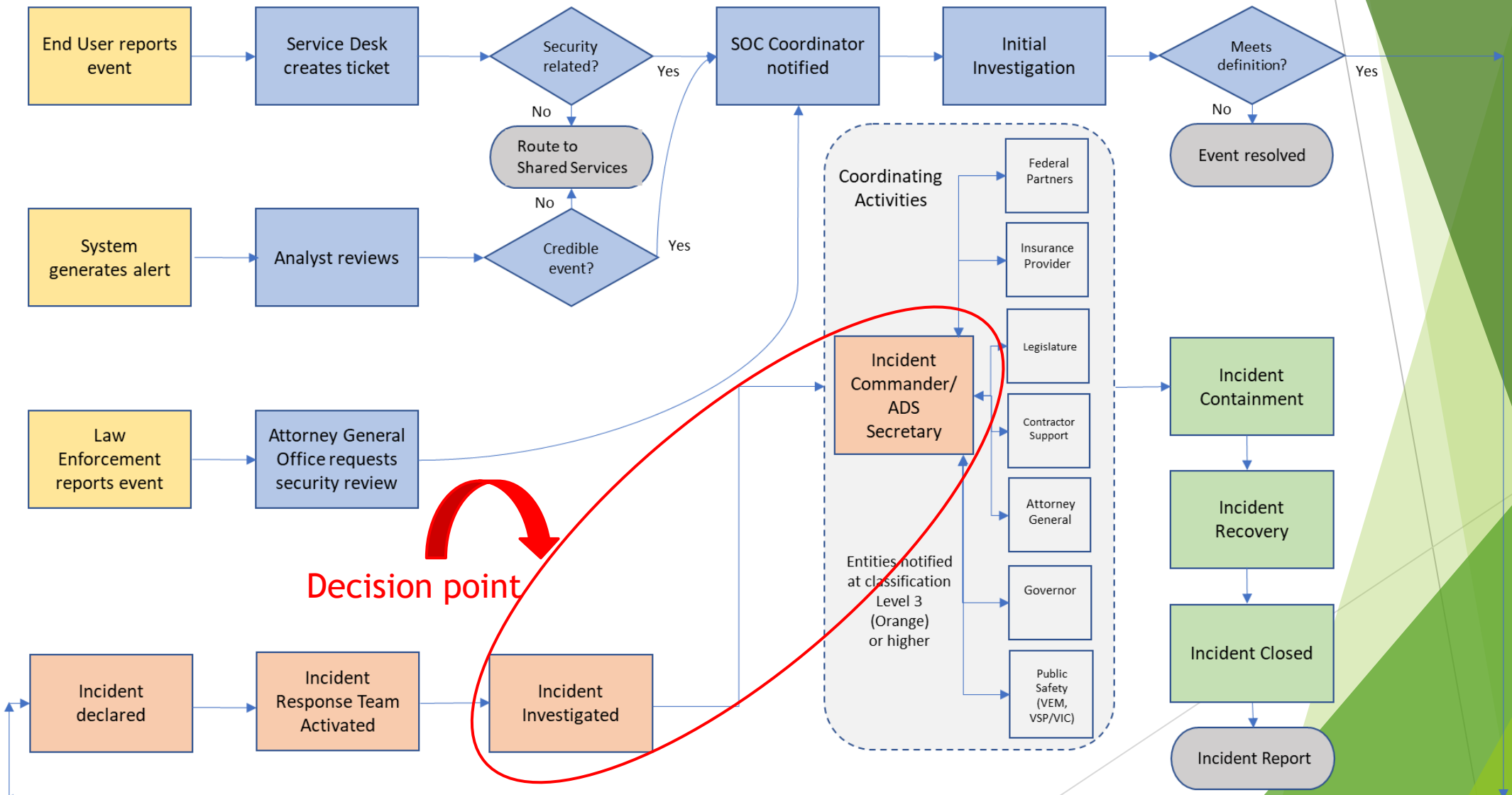
Minimizing loss, theft of information, or service disruption.

Eliminating the threat.

Restoring computing services quickly and securely.

Assessing response to better handle future incidents through utilization of reports, “Lessons Learned,” and after-action activities, or mitigation of exploited weaknesses to prevent similar incidents from occurring in the future.

# Incident Workflow



# Further Response Plans

- Playbooks – broad categories (10 individual books)
  - Malicious programs
  - Access violations
  - Social Engineering
  - Disruption
  - Data breach
- Allows security team to better focus on tasks specific to the incident
- Provides command and control guidance in the absence of direct leadership, addressing communications or physical presence interruption

# What is the Cybersecurity Incident Annex?

- Enables a coordinated and multi-disciplinary **management of consequences** that result from a cybersecurity incident that
  - impairs essential government services,
  - destabilizes community lifelines, and
  - threatens critical infrastructure.
- The scope covers cybersecurity incidents related to the
  - State of Vermont (SOV) services,
  - local government services,
  - community lifelines affecting Vermont residents, and
  - critical infrastructure serving Vermont.
- It is not an IT incident response plan
  - Previous slides – ADS driven

**Intentionally a high-bar for activation. Approach is similar to the protocol for weather events—the SEOC activates for extreme events, not for routine events.**

# Support of statewide response efforts

- Fully participating (permanent) member of Cyber Response Advisory Board
- Consulted and provided input for Cyber Annex
- Maintains communication with DPS, VEM, VIC, Federal partners, and State Homeland Security Unit
- Participates in information exchanges with critical infrastructure sectors (ongoing development) – Federal partner driven coordination