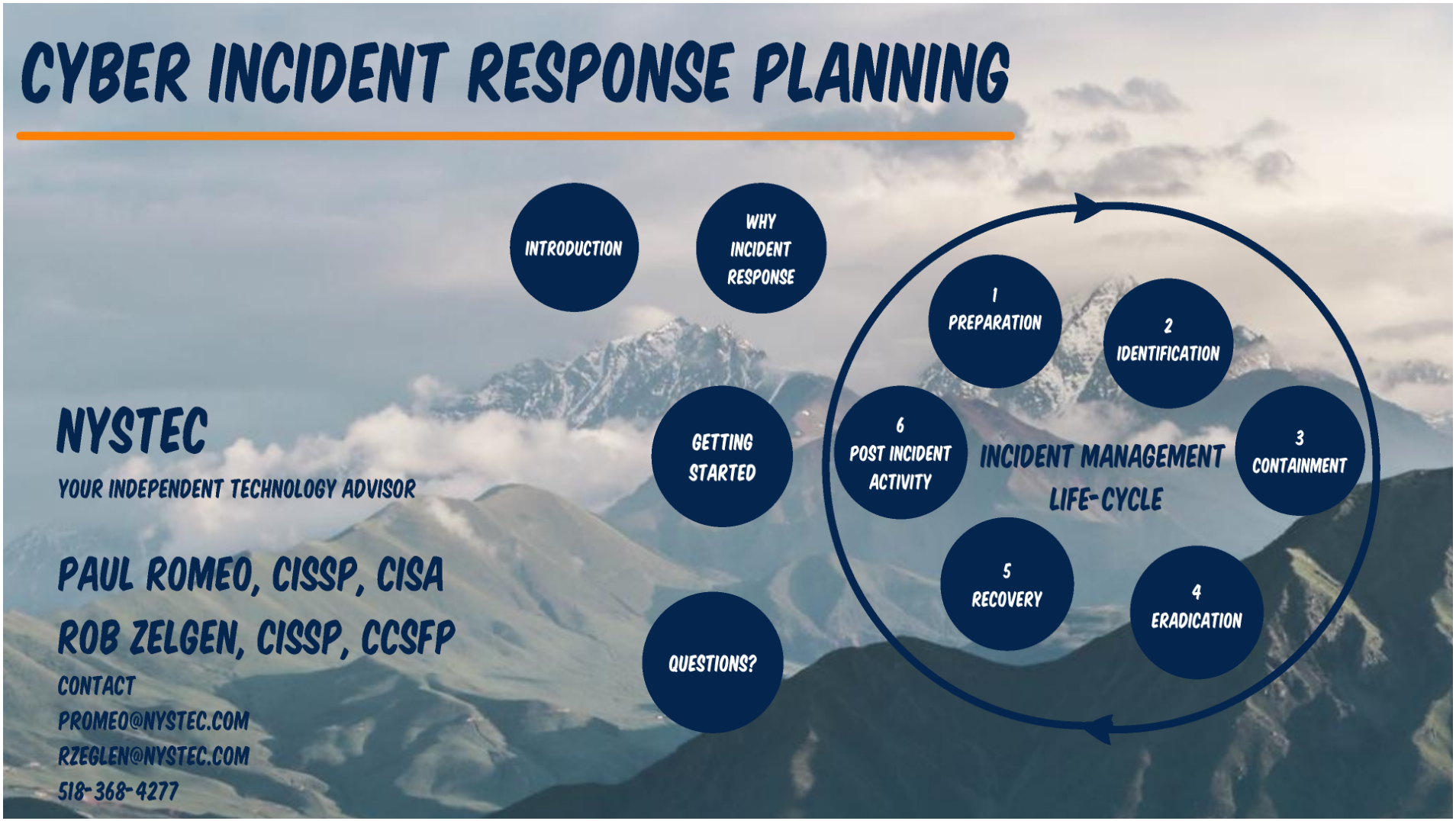
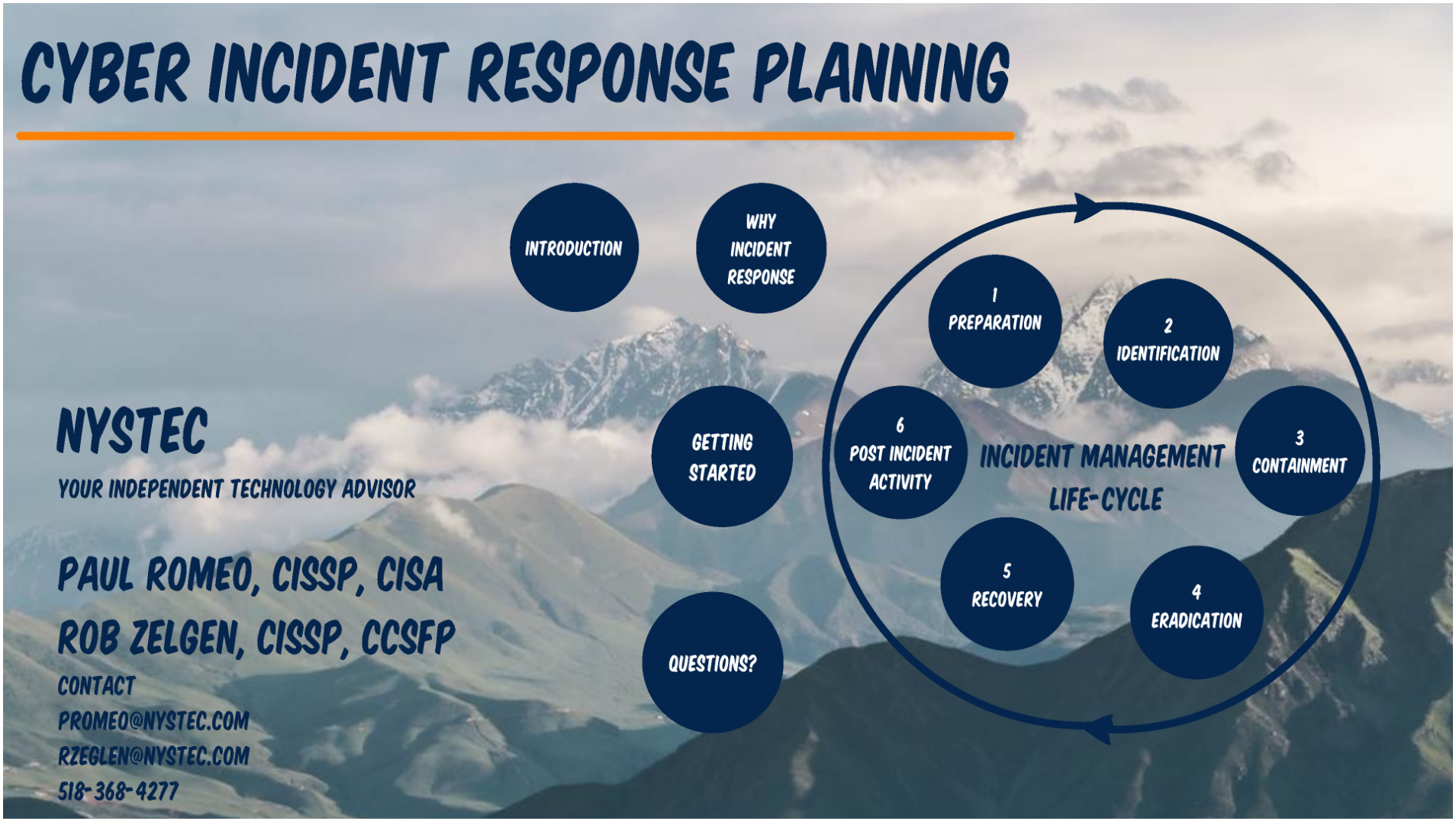
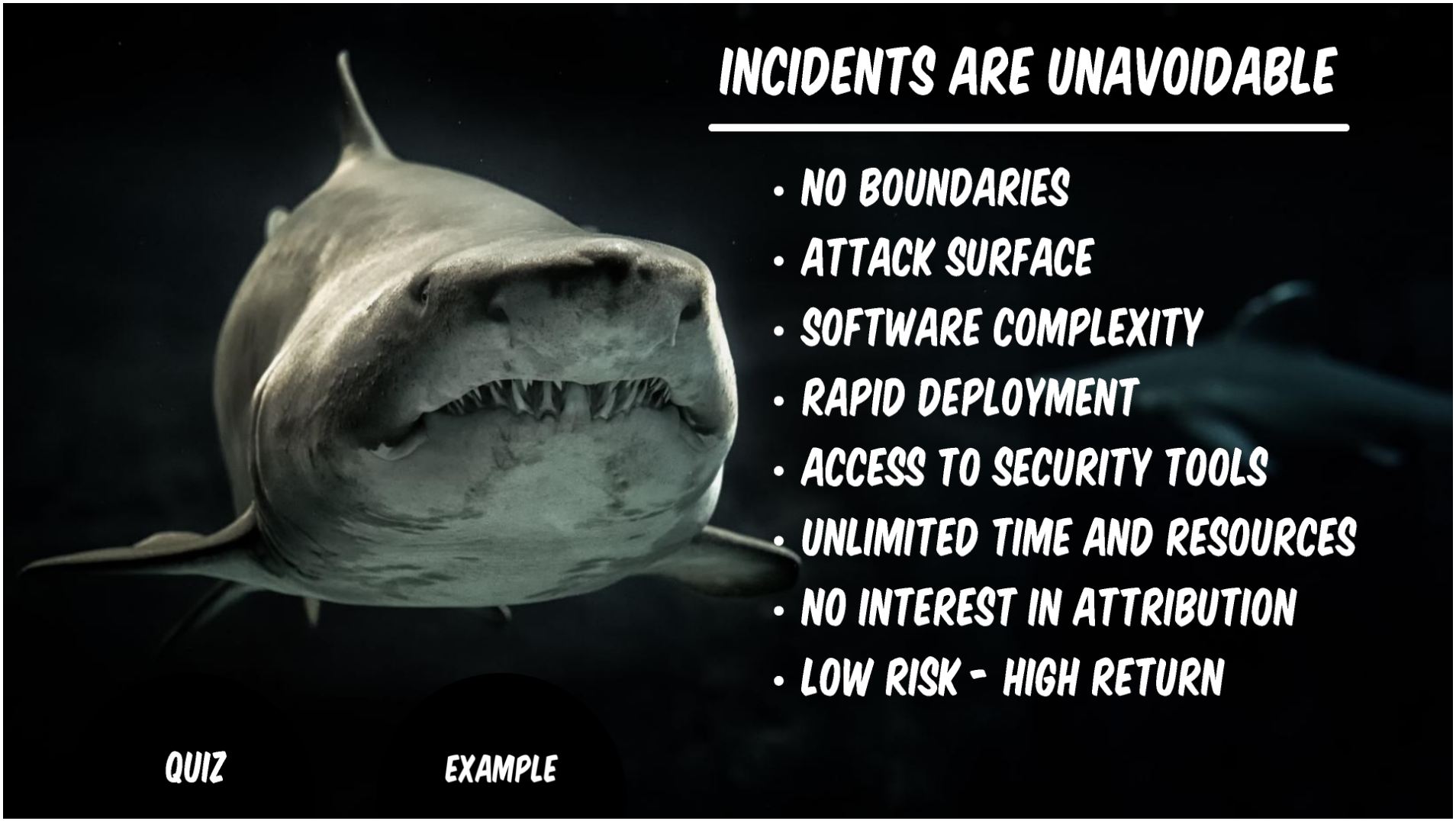

CYBER INCIDENT RESPONSE PLANNING
INTRODUCTION
WHY INCIDENT RESPONSE
GETTING STARTED
QUESTIONS?
NYSTEC
YOUR INDEPENDENT TECHNOLOGY ADVISOR
PAUL ROMEO, CISSP, CISA
ROB ZELGEN, CISSP, CCSFP
CONTACT
PROMEO@NYSTEC.COM
RZEGLEN@NYSTEC.COM
518-368-4277
INCIDENT MANAGEMENT LIFE-CYCLE
1 PREPARATION
2 IDENTIFICATION
3 CONTAINMENT
4 ERADICATION
5 RECOVERY
6 POST INCIDENT ACTIVITY


BACKGROUND
• NYSTEC
• ROB ZEGLEN CISSP
• PAUL ROMEO CISSP


CYBER INCIDENT RESPONSE PLANNING
INTRODUCTION
WHY INCIDENT RESPONSE
GETTING STARTED
QUESTIONS?
NYSTEC
YOUR INDEPENDENT TECHNOLOGY ADVISOR
PAUL ROMEO, CISSP, CISA
ROB ZELGEN, CISSP, CCSFP
CONTACT
PROMEO@NYSTEC.COM
RZEGLEN@NYSTEC.COM
518-368-4277
INCIDENT MANAGEMENT LIFE-CYCLE
1 PREPARATION
2 IDENTIFICATION
3 CONTAINMENT
4 ERADICATION
5 RECOVERY
6 POST INCIDENT ACTIVITY


INCIDENTS ARE UNAVOIDABLE
• NO BOUNDARIES
• ATTACK SURFACE
• SOFTWARE COMPLEXITY
• RAPID DEPLOYMENT
• ACCESS TO SECURITY TOOLS
• UNLIMITED TIME AND RESOURCES
• NO INTEREST IN ATTRIBUTION
• LOW RISK - HIGH RETURN
QUIZ
EXAMPLE

IMPACT OF CYBER INCIDENTS

IMPACT OF CYBER INCIDENTS

4.5 BILLION

IMPACT OF CYBER INCIDENTS

4.5 BILLION

4.5 BILLION RECORDS WERE COMPROMISED IN THE FIRST HALF OF 2018 . . . AT A RATE OF 291 RECORDS PER SECOND

GEMALTO'S 2018 BREACH LEVEL INDEX

IMPACT OF CYBER INCIDENTS

4.5 BILLION

4.5 BILLION RECORDS WERE COMPROMISED IN THE FIRST HALF OF 2018 . . . AT A RATE OF 291 RECORDS PER SECOND

GEMALTO'S 2018 BREACH LEVEL INDEX

3.86 MILLION

IMPACT OF CYBER INCIDENTS

4.5 BILLION

4.5 BILLION RECORDS WERE COMPROMISED IN THE FIRST HALF OF 2018 . . . AT A RATE OF 291 RECORDS PER SECOND

GEMALTO'S 2018 BREACH LEVEL INDEX

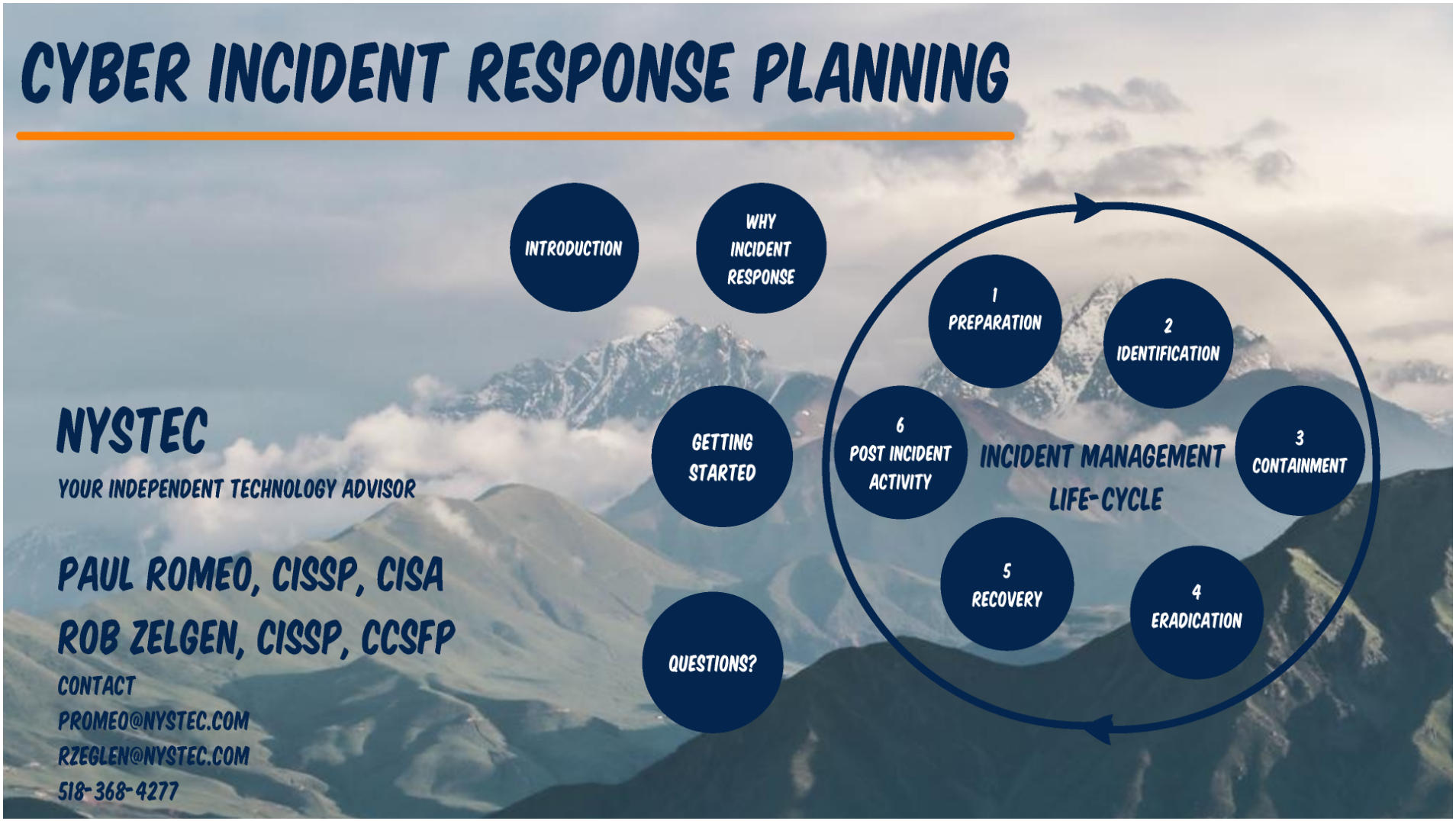
3.86 MILLION

AVERAGE COST OF A DATA BREACH IS $3.86 MILLION - $148 PER RECORD - 26,000 RECORDS PER BREACH

PONEMON INSTITUTE - 2018 COST OF DATA BREACH STUDY


NOTPETYA
• TAX SOFTWARE ME DOCS
• RAPID PROPAGATION WITH ETERNAL BLUE, ETERNAL ROMANCE AND MIMIKATZ
• DESIGNED TO DESTROY, NOT EXTORT
• TOTALED $10 BILLION IN DAMAGES
MAERSK
https://www.newsweek.com/russia-accused-massive-12-billion-cyber-attack-807867

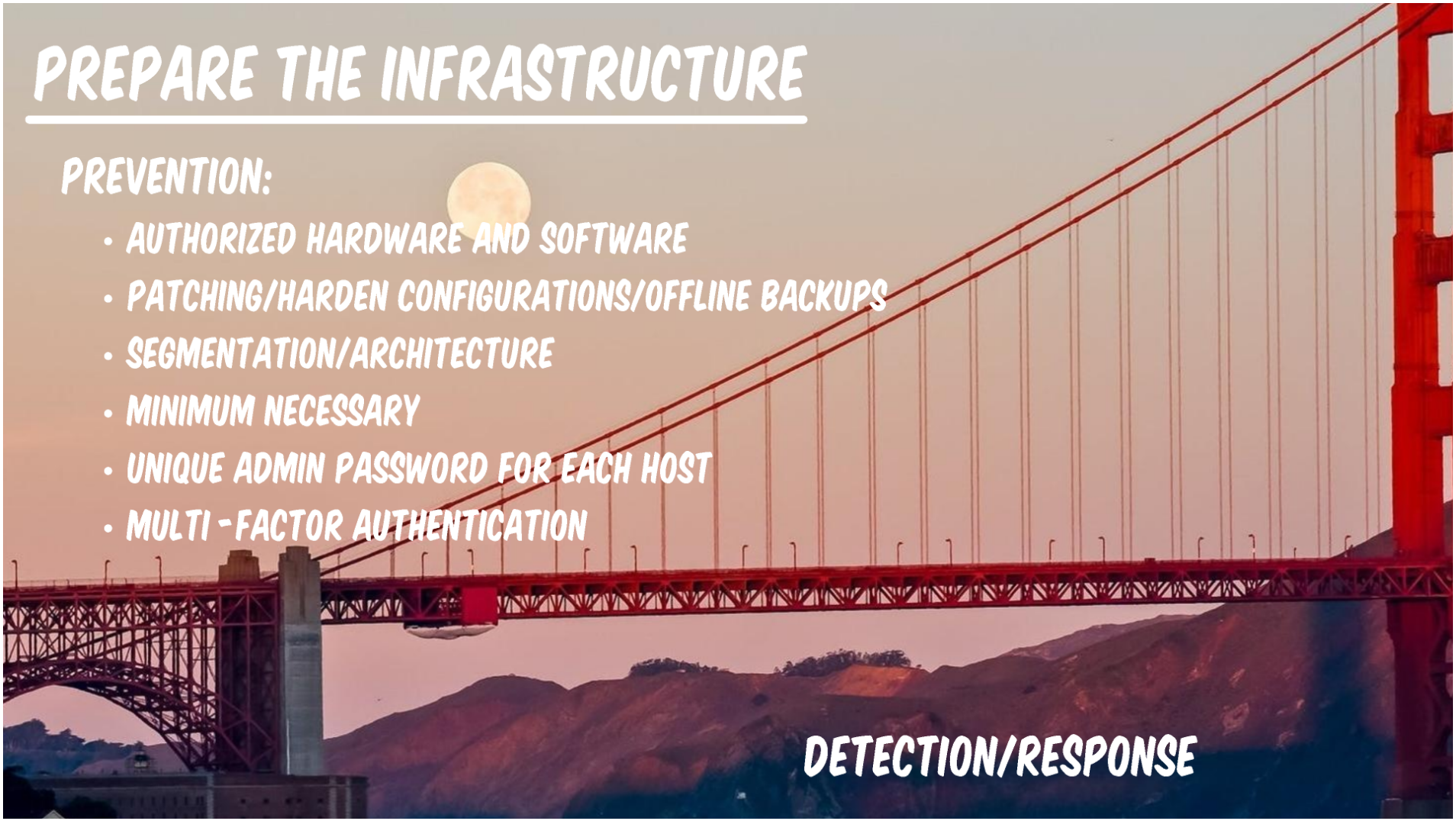

"...THE SECOND YOU SAW IT, YOUR DATA CENTER WAS ALREADY GONE."
CRAIG WILLIAMS, DIRECTOR OF OUTREACH AT CISCO'S TALOS DIVISION
• 20% OF GLOBAL SHIPPING MARKET
• 800 SHIPS AND 76 PORTS/HARBORS
• THOUSANDS OF COMPUTERS, SERVERS
• PHONE SYSTEMS DOWN
• PORTS CLOSED
• WIPED OUT ENTIRE ACTIVE DIRECTORY
THE UNTOLD STORY OF NOTPETYA, THE MOST DEVASTATING CYBER ATTACK IN HISTORY
HTTPS://WWW.WIRED.COM/STORY/NOTPETYA-CYBERATTACK-UKRAINE-RUSSIA-CODE-CRASHED-THE-WORLD/
MIKKO HYPPONEN - 'CYBER ARMS RACE' AT LES ASSISES DE LA SÉCURITÉ ET DES SYSTÈMES D'INFORMATION 2018


CYBER INCIDENT RESPONSE PLANNING
INTRODUCTION
WHY INCIDENT RESPONSE
GETTING STARTED
QUESTIONS?
NYSTEC
YOUR INDEPENDENT TECHNOLOGY ADVISOR
PAUL ROMEO, CISSP, CISA
ROB ZELGEN, CISSP, CCSFP
CONTACT
PROMEO@NYSTEC.COM
RZEGLEN@NYSTEC.COM
518-368-4277
1 PREPARATION
2 IDENTIFICATION
3 CONTAINMENT
4 ERADICATION
5 RECOVERY
6 POST INCIDENT ACTIVITY
INCIDENT MANAGEMENT LIFE-CYCLE

PREPARATION: EFFECTIVE AND EFFICIENT RESPONSE


PREPARE THE ORGANIZATION
• EXECUTIVE SUPPORT, AUTHORITY, RESOURCES
• RISK MANAGEMENT PROCESS
• LEGAL REQUIREMENTS
• INCIDENT RESPONSE STRATEGY
• INTERNAL TEAM VS. OUTSOURCED
• OPERATIONS VS. FORENSICS
• CONTACT LAW ENFORCEMENT


ESTABLISH AND PREPARE RESPONSE TEAMS
• LEGAL/CRISIS TEAM/INSURANCE COMPANY
• ROLES/RESPONSIBILITIES
• TRAIN THE TEAM
• RUNBOOKS / CHECKLISTS
• DRILL AND TEST


PREPARE THE INFRASTRUCTURE
PREVENTION:
• AUTHORIZED HARDWARE AND SOFTWARE
• PATCHING/HARDEN CONFIGURATIONS/OFFLINE BACKUPS
• SEGMENTATION/ARCHITECTURE
• MINIMUM NECESSARY
• UNIQUE ADMIN PASSWORD FOR EACH HOST
• MULTI-FACTOR AUTHENTICATION
DETECTION/RESPONSE

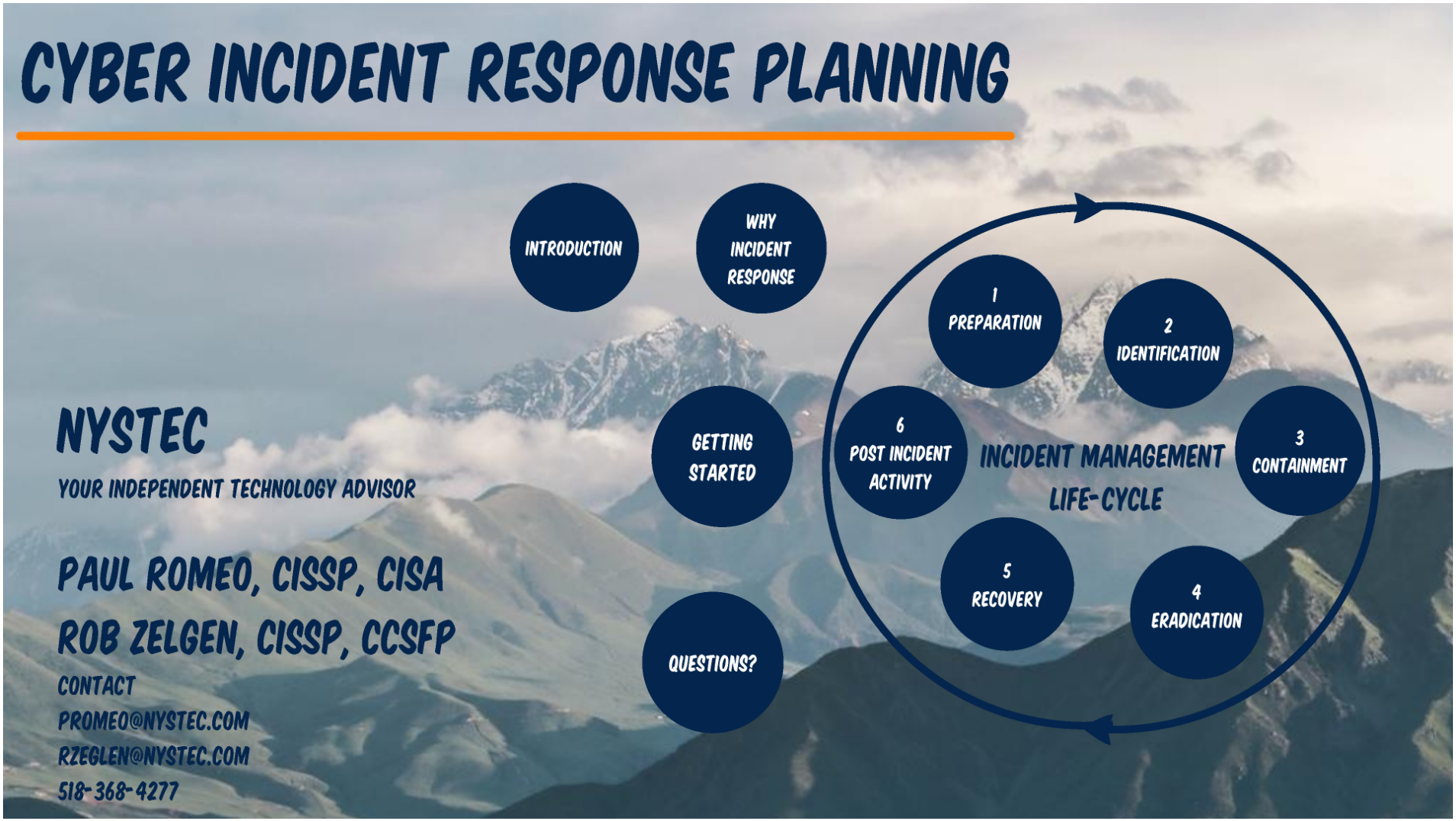
PREPARE THE INFRASTRUCTURE

DETECT AND RESPOND:

- DEFINE AUTHORIZED SYSTEM/USER BEHAVIOR
- DOCUMENT BASELINES
- MONITOR
  - NETWORK TRAFFIC
  - SUSPICIOUS CHANGES/ACTIVITY
  - UNAUTHORIZED/SYSTEMS OR SOFTWARE
- APPROVED WARNING BANNERS

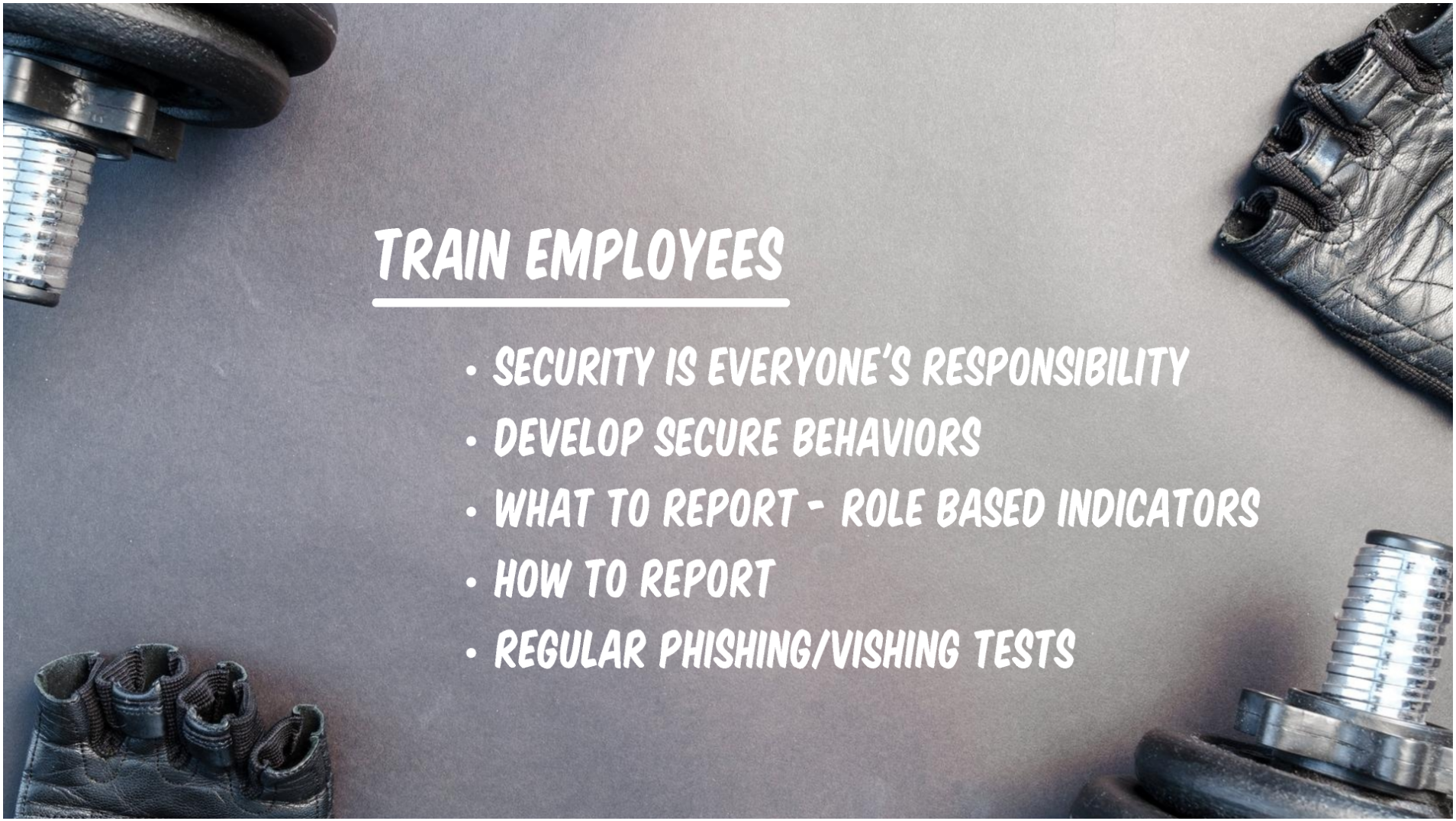
DECIDE AHEAD OF TIME

- ZERO HOUR APPROVED COMMUNICATIONS
- DOCUMENT ASSET/PROCESS OWNERS
- DOCUMENT CRITERIA FOR DOWNTIME


CYBER INCIDENT RESPONSE PLANNING
INTRODUCTION
WHY INCIDENT RESPONSE
GETTING STARTED
QUESTIONS?
1 PREPARATION
2 IDENTIFICATION
3 CONTAINMENT
4 ERADICATION
5 RECOVERY
6 POST INCIDENT ACTIVITY
INCIDENT MANAGEMENT LIFE-CYCLE
NYSTEC
YOUR INDEPENDENT TECHNOLOGY ADVISOR
PAUL ROMEO, CISSP, CISA
ROB ZELGEN, CISSP, CCSFP
CONTACT
PROMEO@NYSTEC.COM
RZEGLEN@NYSTEC.COM
518-368-4277

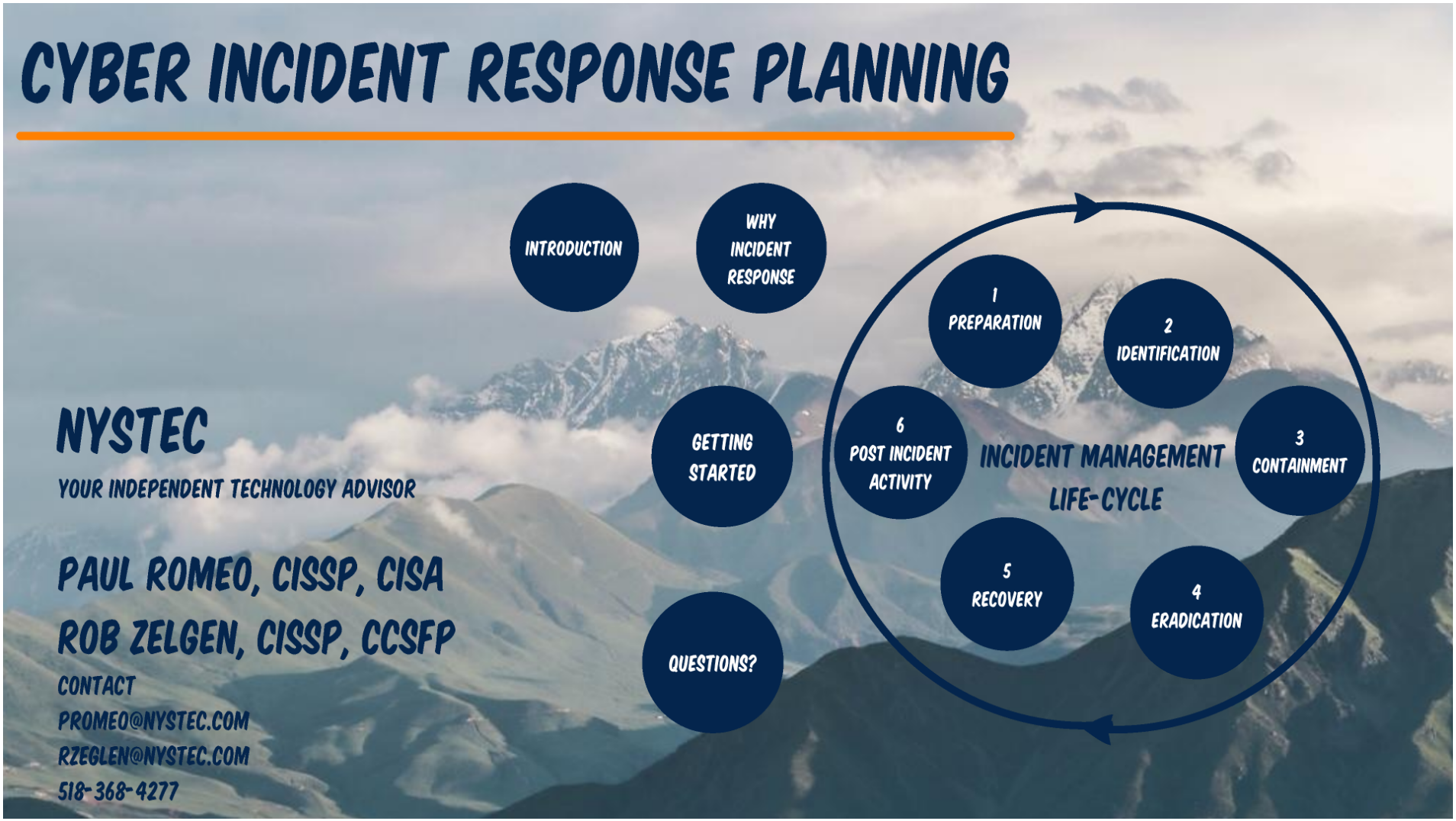
IDENTIFICATION: EARLY DETECTION

1. PRECURSORS
2. INDICATORS OF ATTACK (IOA)
3. INDICATORS OF COMPROMISE (IOC)
4. INCIDENT
5. BREACH
6. CRISIS
7. DISASTER

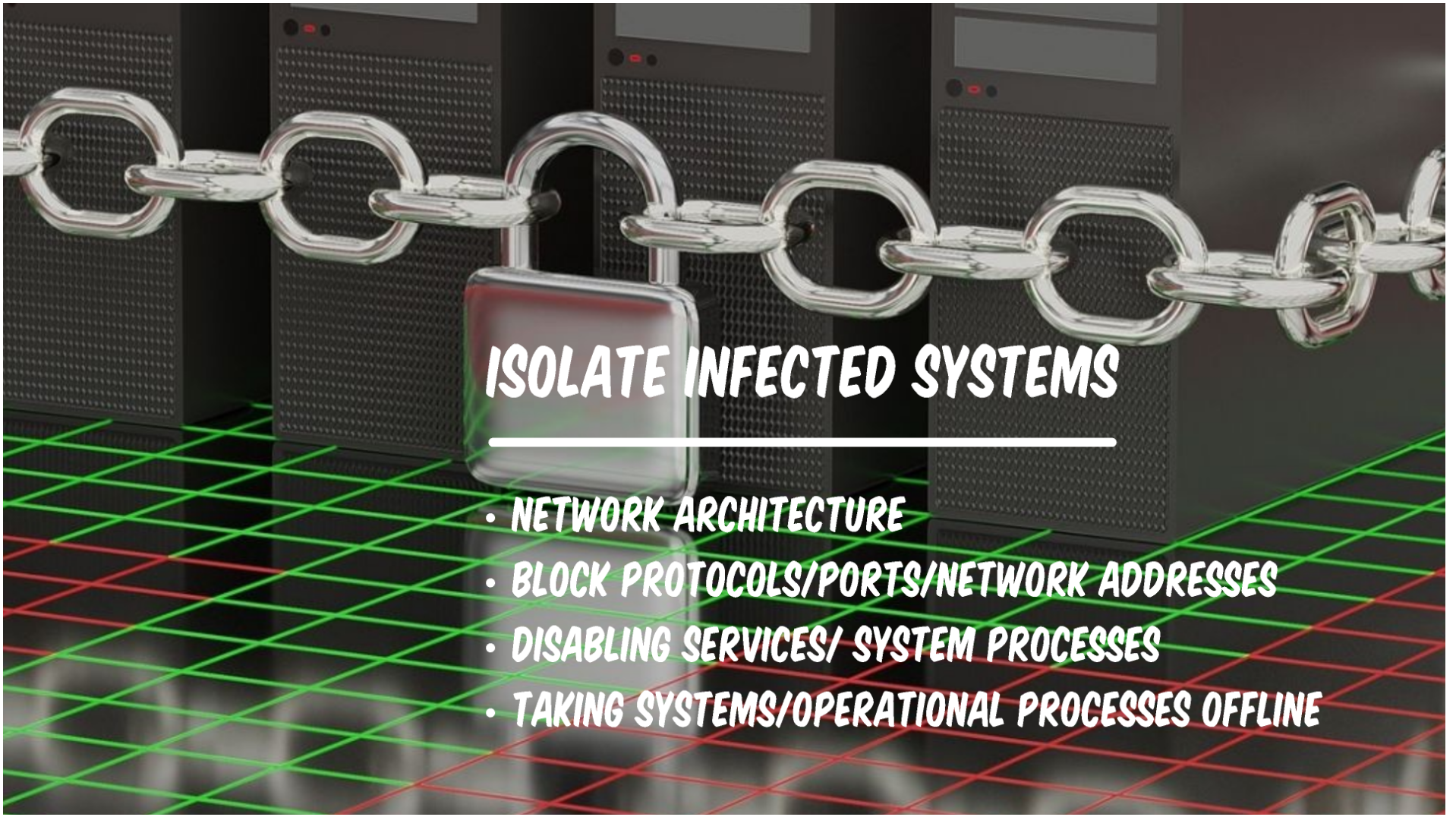

TRAIN EMPLOYEES
• SECURITY IS EVERYONE'S RESPONSIBILITY
• DEVELOP SECURE BEHAVIORS
• WHAT TO REPORT - ROLE BASED INDICATORS
• HOW TO REPORT
• REGULAR PHISHING/VISHING TESTS


INFRASTRUCTURE: LOOK BENEATH THE SURFACE
• AUDIT AND LOG SUFFICIENT DETAILS
• DEFINE SYSTEM ACTIVITY AND CONFIGURATIONS TO MONITOR
• PERIMETER, NETWORKS, APPS, DATABASES, HOSTS
• EVENT CORRELATION/ALERTING THRESHOLD


EMERGENCY
DETERMINE SEVERITY
• IMPACT ON CRITICAL SYSTEMS/PROCESSES
• COMPLIANCE IMPACT ON PROTECTED DATA
• SEVERITY MATRIX

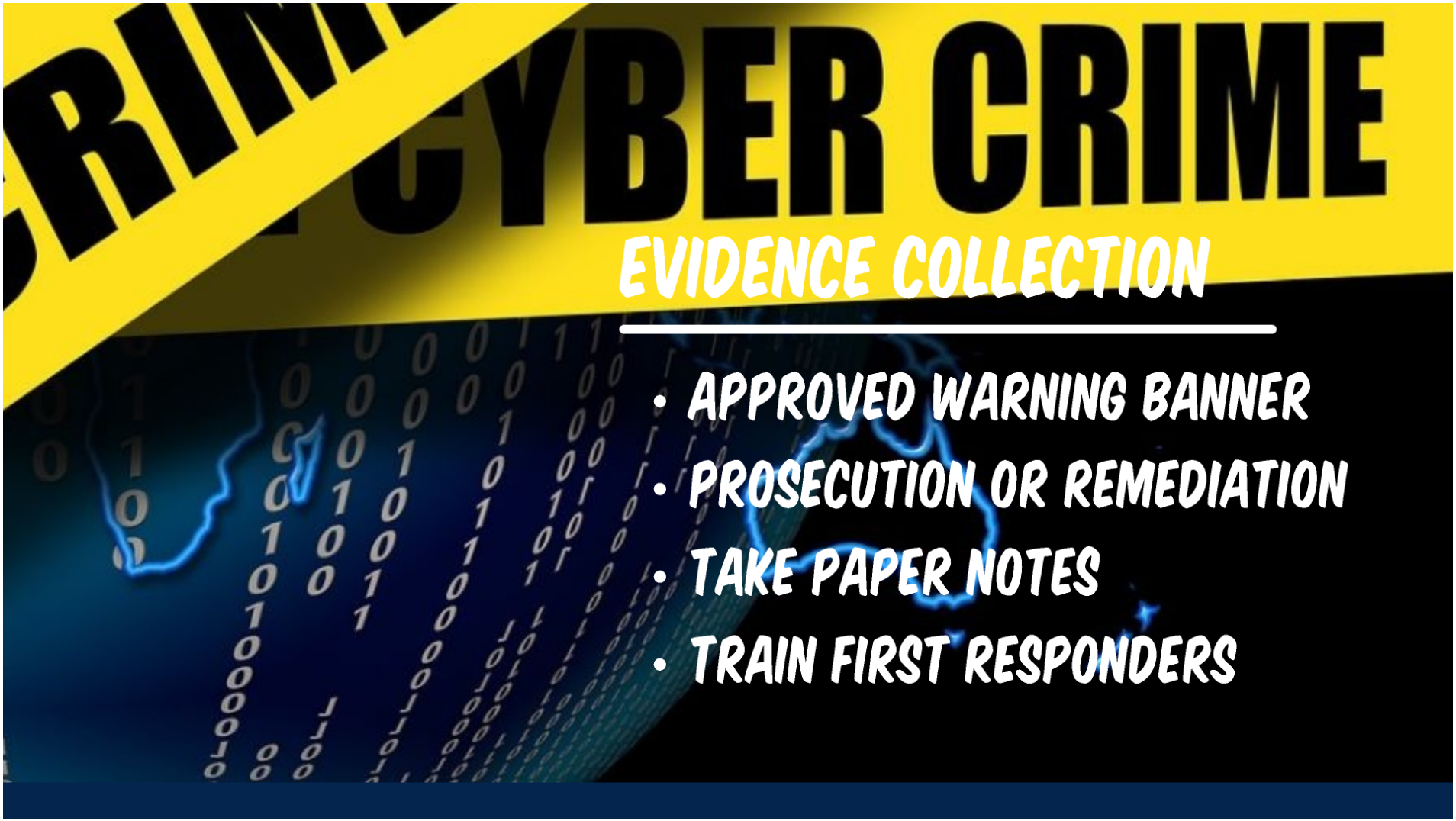

CYBER INCIDENT RESPONSE PLANNING
INTRODUCTION
WHY INCIDENT RESPONSE
GETTING STARTED
QUESTIONS?
NYSTEC
YOUR INDEPENDENT TECHNOLOGY ADVISOR
PAUL ROMEO, CISSP, CISA
ROB ZELGEN, CISSP, CCSFP
CONTACT
PROMEO@NYSTEC.COM
RZEGLEN@NYSTEC.COM
518-368-4277
INCIDENT MANAGEMENT LIFE-CYCLE
1 PREPARATION
2 IDENTIFICATION
3 CONTAINMENT
4 ERADICATION
5 RECOVERY
6 POST INCIDENT ACTIVITY

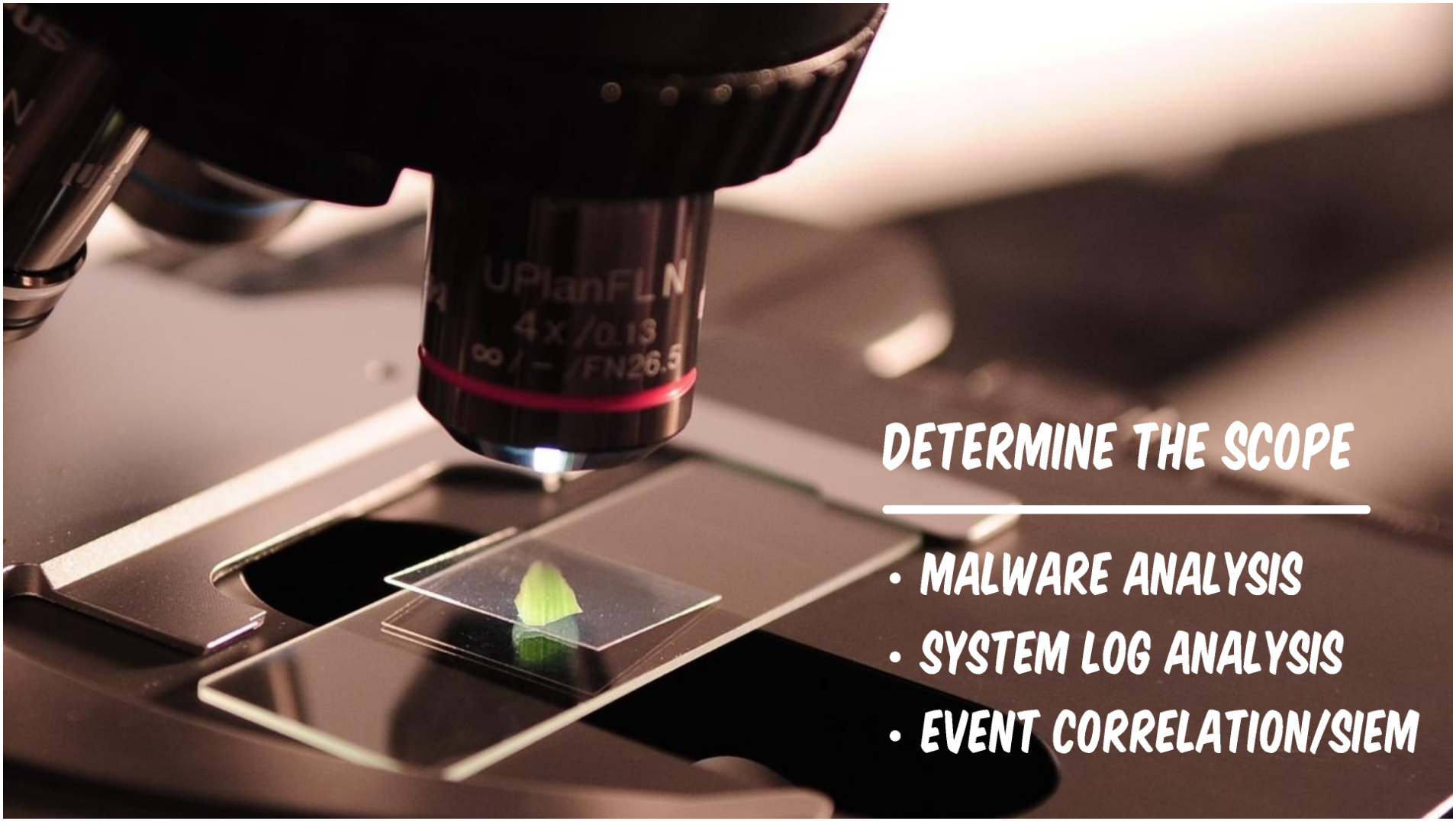

CONTAINMENT: LIMIT THE IMPACT
ISOLATE SYSTEMS
CONTROL COMMUNICATION
EVIDENCE COLLECTION
DETERMINE FULL SCOPE

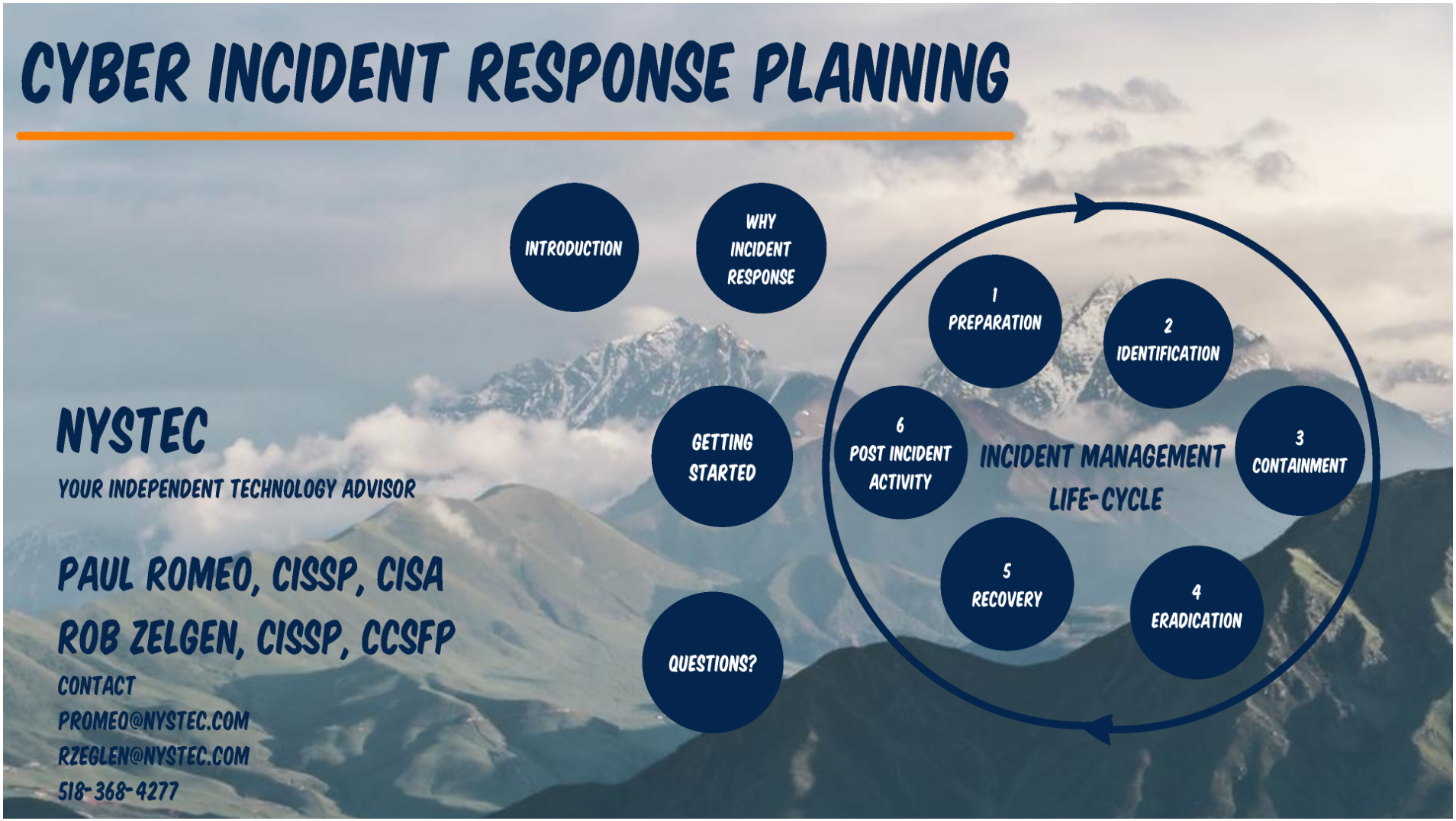

ISOLATE INFECTED SYSTEMS
• NETWORK ARCHITECTURE
• BLOCK PROTOCOLS/PORTS/NETWORK ADDRESSES
• DISABLING SERVICES/ SYSTEM PROCESSES
• TAKING SYSTEMS/OPERATIONAL PROCESSES OFFLINE

COMMUNICATION

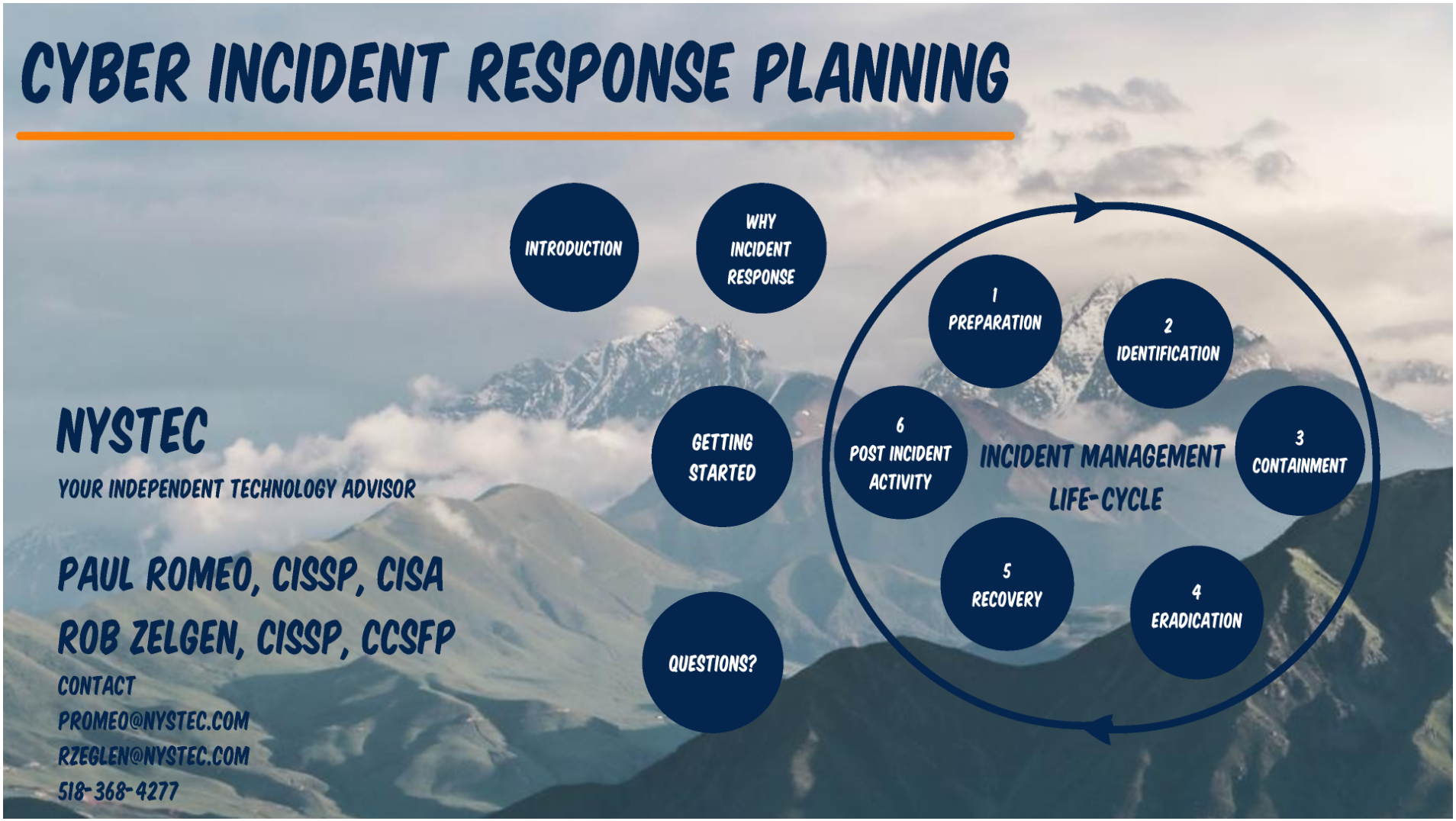
- HAVE A PLAN
- TRAIN EMPLOYEES
- APPROVED SOURCE/CHANNEL
- CONSISTENT MESSAGE
- INTERNAL/EXTERNAL
- REGULAR CADENCE
- REDUNDANT CHANNELS


CYBER CRIME
EVIDENCE COLLECTION
• APPROVED WARNING BANNER
• PROSECUTION OR REMEDIATION
• TAKE PAPER NOTES
• TRAIN FIRST RESPONDERS

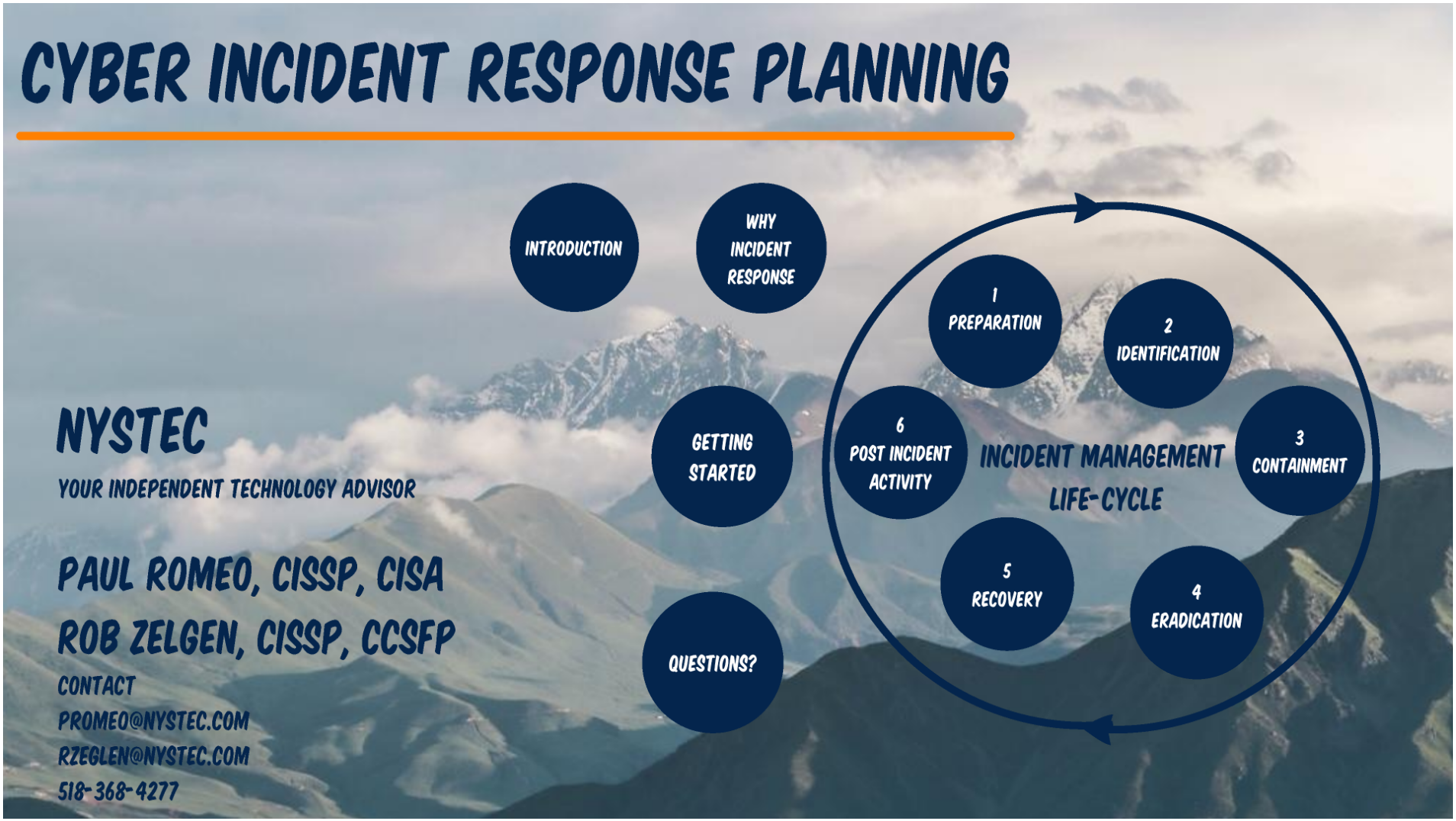

UPlanFL N
4x /0.13
∞ / – /FN26.5
DETERMINE THE SCOPE
• MALWARE ANALYSIS
• SYSTEM LOG ANALYSIS
• EVENT CORRELATION/SIEM


CYBER INCIDENT RESPONSE PLANNING
INTRODUCTION
WHY INCIDENT RESPONSE
GETTING STARTED
QUESTIONS?
NYSTEC
YOUR INDEPENDENT TECHNOLOGY ADVISOR
PAUL ROMEO, CISSP, CISA
ROB ZELGEN, CISSP, CCSFP
CONTACT
PROMEO@NYSTEC.COM
RZEGLEN@NYSTEC.COM
518-368-4277
INCIDENT MANAGEMENT LIFE-CYCLE
1 PREPARATION
2 IDENTIFICATION
3 CONTAINMENT
4 ERADICATION
5 RECOVERY
6 POST INCIDENT ACTIVITY

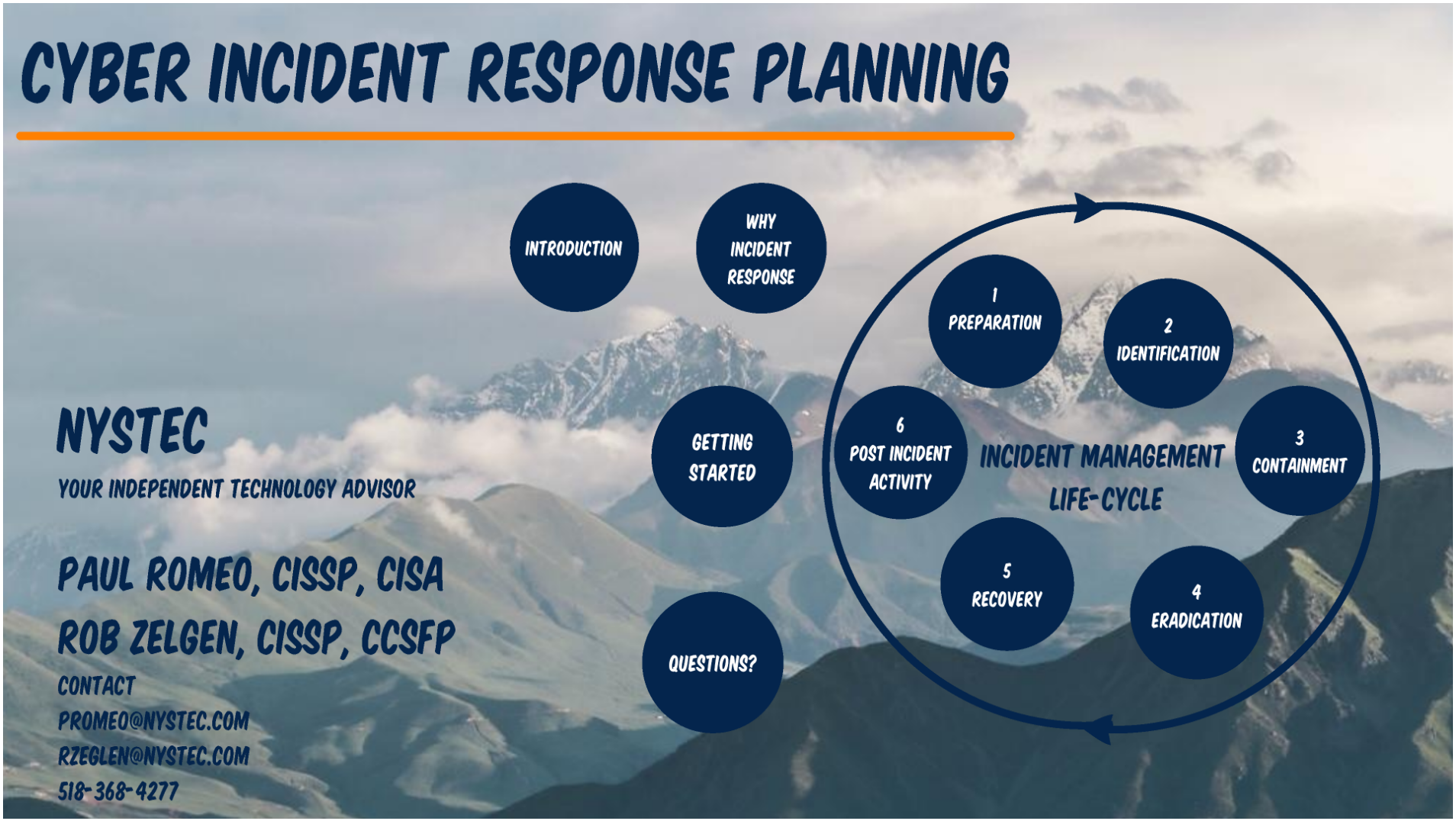

ERADICATION: REMOVE THE THREAT
• SANITIZE/WIPE SYSTEMS
• ENHANCED DETECTION ON SECURITY TOOLS
• UPDATE FIREWALL/ROUTER FILTER RULES
• PATCH/FIX VULNERABILITIES


CYBER INCIDENT RESPONSE PLANNING
INTRODUCTION
WHY INCIDENT RESPONSE
GETTING STARTED
QUESTIONS?
NYSTEC
YOUR INDEPENDENT TECHNOLOGY ADVISOR
PAUL ROMEO, CISSP, CISA
ROB ZELGEN, CISSP, CCSFP
CONTACT
PROMEO@NYSTEC.COM
RZEGLEN@NYSTEC.COM
518-368-4277
1 PREPARATION
2 IDENTIFICATION
3 CONTAINMENT
4 ERADICATION
5 RECOVERY
6 POST INCIDENT ACTIVITY
INCIDENT MANAGEMENT LIFE-CYCLE


RECOVERY AND RESTORATION OF SERVICES
• ENSURE ERADICATION COMPLETE
• AFTER HOURS
• REPAIR/REPLACE/REBUILD SYSTEMS
• RESTORING CLEAN BACKUPS

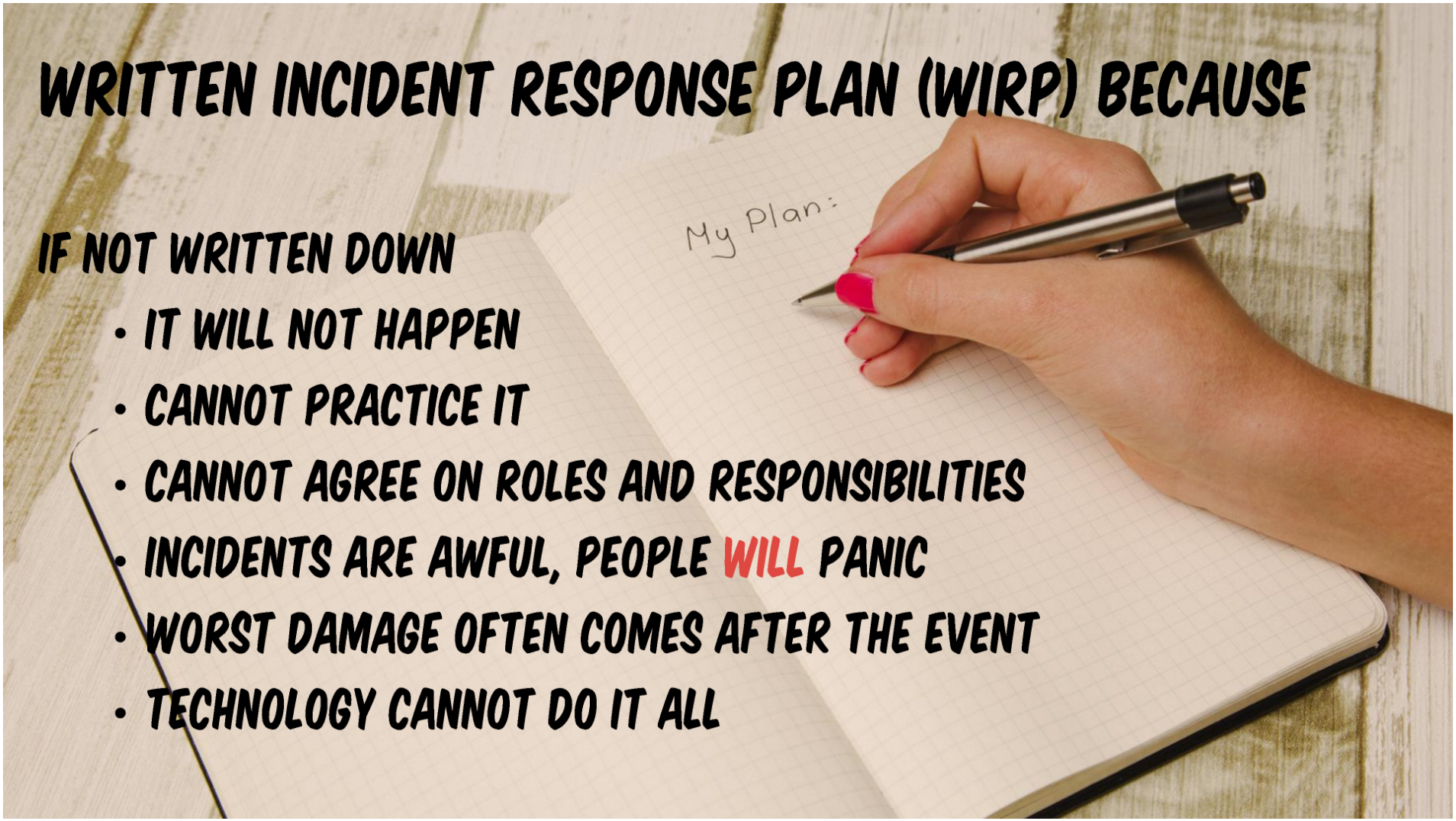

CYBER INCIDENT RESPONSE PLANNING
INTRODUCTION
WHY INCIDENT RESPONSE
GETTING STARTED
QUESTIONS?
1 PREPARATION
2 IDENTIFICATION
3 CONTAINMENT
4 ERADICATION
5 RECOVERY
6 POST INCIDENT ACTIVITY
INCIDENT MANAGEMENT LIFE-CYCLE
NYSTEC
YOUR INDEPENDENT TECHNOLOGY ADVISOR
PAUL ROMEO, CISSP, CISA
ROB ZELGEN, CISSP, CCSFP
CONTACT
PROMEO@NYSTEC.COM
RZEGLEN@NYSTEC.COM
518-368-4277


POST INCIDENT ACTIVITY
• MEET WITHIN 2 WEEKS OF INCIDENT CLOSURE
• LESSONS LEARNED
• MISSED INDICATORS/PRECURSORS
• MISSING OR INEFFECTIVE CONTROLS
• PROCESS/PROCEDURE CHANGES
• IDENTIFY TRAINING DEFICIENCIES
• PERFORMANCE MEASURES


CYBER INCIDENT RESPONSE PLANNING
INTRODUCTION
WHY INCIDENT RESPONSE
GETTING STARTED
QUESTIONS?
NYSTEC
YOUR INDEPENDENT TECHNOLOGY ADVISOR
PAUL ROMEO, CISSP, CISA
ROB ZELGEN, CISSP, CCSFP
CONTACT
PROMEO@NYSTEC.COM
RZEGLEN@NYSTEC.COM
518-368-4277
1 PREPARATION
2 IDENTIFICATION
3 CONTAINMENT
4 ERADICATION
5 RECOVERY
6 POST INCIDENT ACTIVITY
INCIDENT MANAGEMENT LIFE-CYCLE

WHERE DO I START?

- WRITTEN INCIDENT RESPONSE PLAN
- TIPS AND LESSONS LEARNED
- WIRP TEMPLATE

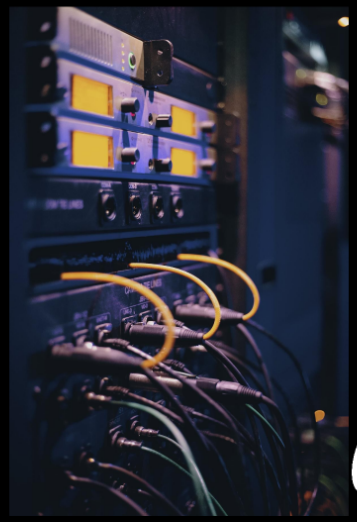

WRITTEN INCIDENT RESPONSE PLAN (WIRP) BECAUSE
My Plan:
IF NOT WRITTEN DOWN
• IT WILL NOT HAPPEN
• CANNOT PRACTICE IT
• CANNOT AGREE ON ROLES AND RESPONSIBILITIES
• INCIDENTS ARE AWFUL, PEOPLE WILL PANIC
• WORST DAMAGE OFTEN COMES AFTER THE EVENT
• TECHNOLOGY CANNOT DO IT ALL

KEY INCIDENT RESPONSE PLAN ELEMENTS

- TEAMS AND ROLES DEFINITION
- INTERNAL AND EXTERNAL CYBER SECURITY RESOURCES
- BREACH CLASSIFICATION
- ACTION ITEM CHECKLIST
- RUNBOOKS
- AUDIENCE: SECURITY, IT AND BUSINESS
- CONSIDER ALL INCIDENTS, NOT JUST IT

PRO TIPS AND LESSONS LEARNED

LESSONS LEARNED



HAVE A COMPREHENSIVE UNDERSTANDING OF YOUR CURRENT COMPUTING ENVIRONMENT AND NETWORKS

CREDENTIAL MANAGEMENT

ASSIGN AN INCIDENT COMMANDER

CREATE AN ACTION ITEM CHECKLIST

1) PREPARATION CHECKLIST
    - A. POLICIES & PROCEDURES
    - B. TOOLS
    - C. COMMUNICATION PLAN
    - D. LAW AND LEGAL
2) IDENTIFICATION CHECKLIST
    - A. WHO, WHEN, WHERE, IMPACT AND EXTENT
3) CONTAINMENT CHECKLIST
    - A. ISOLATION
    - B. BACKUPS
    - C. FORENSIC COPIES
    - D. REMOVAL
4) ERADICATION CHECKLIST
    - A. HARDENING & PATCHING
    - B. CONFIGURATION CHANGES
    - C. INGRESS
    - D. NEW CONTROLS
5) RECOVERY CHECKLIST
    - A. RECOVERY BACKUPS
    - B. RETURN TO PRODUCTION
    - C. TESTING
    - D. DOCUMENTATION
6) LESSONS LEARNED
    - A. HOTWASH

LOGGING AND FORENSICS

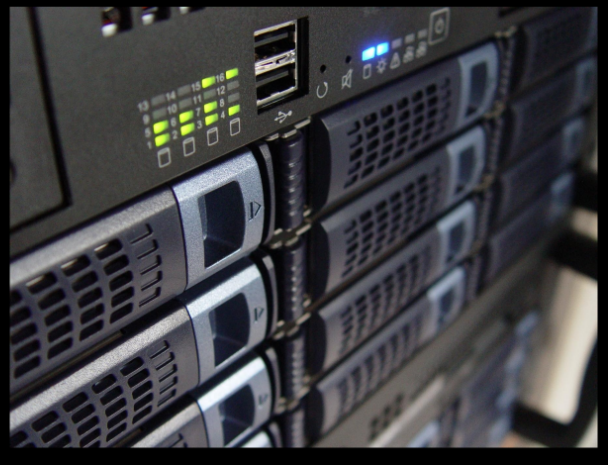
- AUDIT LOGS ARE CRITICAL ARTIFACTS
- TEST AUDITING CAPABILITIES
- WILL NEED LOG CORRELATION
- KEEP FORENSIC COPIES
- MAKE FORENSIC NOTES

CONSIDER OPPOSING FORCES

PRESERVE EVIDENCE FOR INVESTIGATION

VS

GET SYSTEMS BACK UP AND RUNNING ASAP

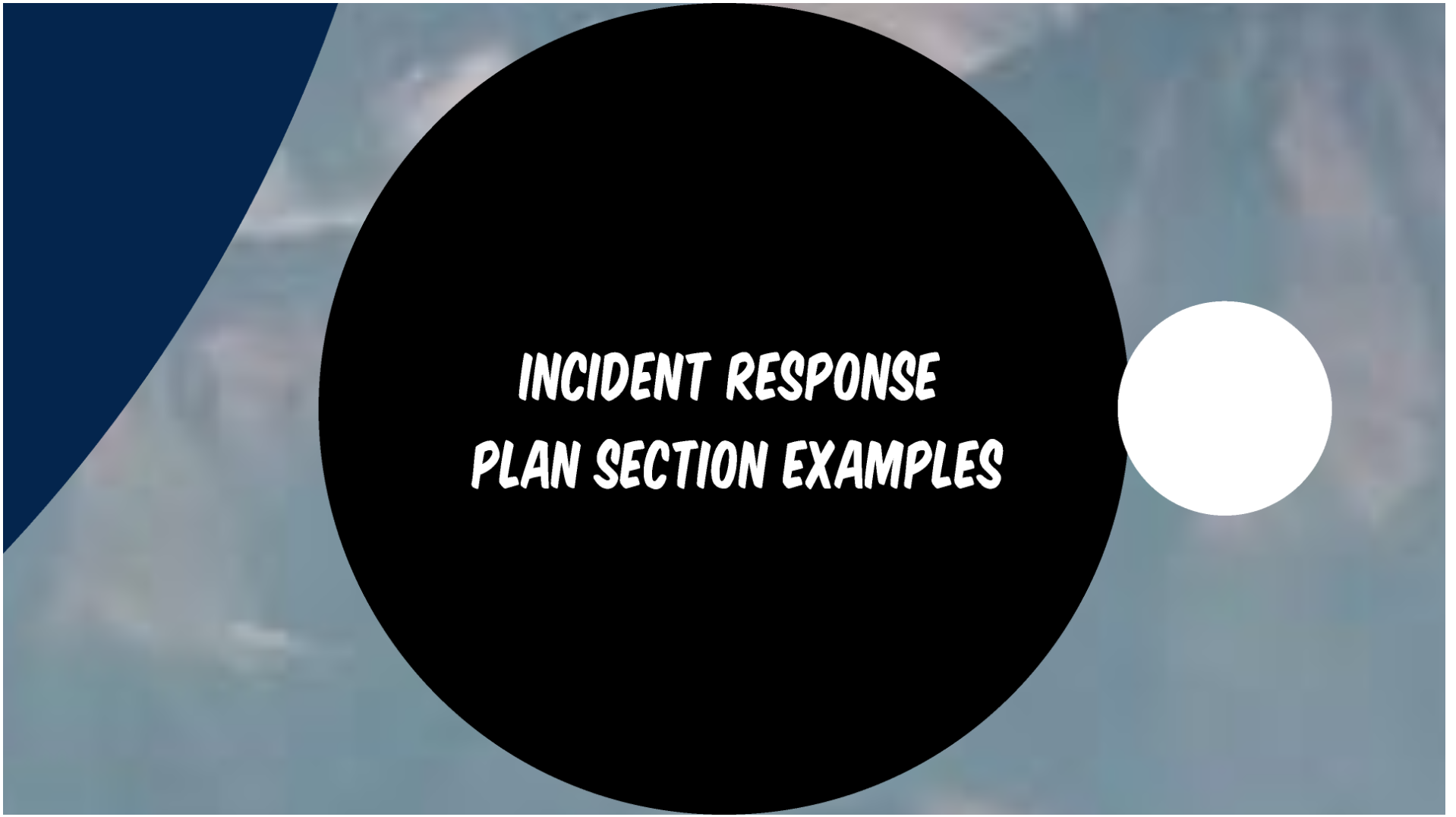


CONDUCT TABLETOP EXERCISES

HOTWASH

FAMOUS FAILURES

"First American has learned of a design defect in an application that made possible unauthorized access to customer data. **At First American, security, privacy and confidentiality are of the highest priority and we are committed to protecting our customers' information..."**


INCIDENT RESPONSE
PLAN SECTION EXAMPLES

Introduction

Mission/Purpose

- The purpose of this document is to define specific communications processes for managing information security incidents to minimize their impact on the organization, thus ensuring that the best possible levels of service quality and availability are maintained.
- To ensure that the incidents/requests are processed consistently and that none are lost.

Senior Management Approval

- Seek management approval for the plan
- Engage management in exercising the plan

Potential Supporting Documents

- Incident Response Process Flow
- Security Incident Response Communications Policy
- Security Incident Response Interdepartmental Communications Template
- Security Incident and Crisis External Communications Guidelines
- IR Procedures
    - Early Detection Runbook
    - Ransomware Runbook
    - Malware Runbook
    - Compromised Credential Runbook
    - Malicious Email Runbook
    - Distributed Denial of Service (DDoS) Runbook
    - Etc..

Definitions

Information security event: Identified occurrence of a system, service, or network state indicating a possible breach of information security policy or failure of controls, including false alarms.

Information security incident: Single or series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.

Incident Commander/Responder: Once MSSP/Security Operations has validated that an event is an incident, the Incident Responder manages the response process.

Forensic Team.....

NYSTEC
YOUR INDEPENDENT TECHNOLOGY ADVISOR

Communications Roles and Responsibilities

Individuals needed and responsible for responding to a security incident make up a security incident response team (SIRT), also known as the incident responders. Members may include the following:

- End Users
- Help Desk
- MSSP/Security Operations
- Customers and Partners
- Constituents
- Media
- Cybersecurity
- IT Operations
- CISO
- Legal
- Human Resources
- Public Relations
- Insurance Providers
- ISP
- Law Enforcement
- Senior Management
- External
- 3rd Party Partners

The RACI tool below is used to identify and avoid confusion in roles and responsibilities during an incident remediation. The acronym stands for:

- **Responsible.** The person(s) who does the work to accomplish the activity; they have been tasked with completing the activity, and/or getting a decision made.
- **Accountable.** The person(s) who is accountable for the completion of the activity. Ideally, this is a single person and is often an executive or program sponsor.
- **Consulted.** The person(s) who provides information. This is usually several people, typically called subject-matter experts (SMEs).
- **Informed.** The person(s) who is updated on progress. These are resources that are affected by the outcome of the activities and need to be kept up to date.

Legend: R – Responsible A – Accountable C – Consulted I – Informed	End Users	Help Desk	Developers System Admins	Cybersecurity/Security Operations	IT Operations	CISO	Legal	HR	PR	Senior Management	External			
Detection														
Report a service disruption, a suspicious email, or an unusual endpoint behavior.	A	R	C	C	C	I	-			-	-	-		
Review security events and determine if there is an incident.	I	I	R	A	-	-	-			-	-	-		
Analysis														
Open help desk ticket.	-	A	A	-	C	C	C			R	-			
Gather answers to incident-related	-	R	R	A	R	-	-			-				

Communications Plan

- Alternate sources for key contact information
  - Cell phones
  - Alternate web site
  - Hardcopy
  - Alternate emails
  - Key contact information
    - Customers
    - Insurance
    - Incident Responders
    - Those in above roles

Incident Reporting Responsibilities

Know reporting responsibilities

- IRS
- NYS ITS
- NYS Breach Reporting Law
- HIPAA
- Business Associate Agreements
- Data Use Agreements
- Privacy Policies
- Help Desk

Table 1. Threat Escalation Protocol

Threat Escalation Protocol			
Impact	Scope		
	High	Medium	Low
High	Tier 1	Tier 1	Tier 2
Medium	Tier 1	Tier 2	Tier 2
Low	Tier 2	Tier 2	Tier 3

Threat Escalation Protocol	Criteria	Stakeholders
Tier 1	• High impact, high scope • High impact, medium scope • Medium impact, high scope	• End User • Help Desk • Cybersecurity • IT Operations • CISO • Legal, HR, PR • Senior Management • External Third Parties
Tier 2	• High impact, low scope • Medium impact, medium scope • Medium impact, low scope • Low impact, high scope • Low impact, medium scope	• End User • Help Desk • Cybersecurity • IT Operations • CISO
Tier 3	• Low impact, medium scope • False positive	• End User • Help Desk • Cybersecurity

NYSTEC Incident Reporting Procedure

What to do?

All NYSTEC employees and contractors must promptly report a security event they observe or experience. By reporting security events early, you can help stop them from becoming incidents.

- Security events have the potential to negatively impact the confidentiality, integrity, or availability of NYSTEC or client information systems, devices, assets, or data.
- Security events can negatively impact the reputation of NYSTEC or our clients.
- Reportable security events require non-routine corrective actions.

What are reportable security events?

- Any event or condition that could impact physical security or safety, including unusual or concerning behavior.
- Any adverse event that threatens the confidentiality, integrity, or availability of NYSTEC or client resources.
- Lost or stolen computers, devices, or media, whether NYSTEC- or client-owned.
- Discovery of malware or attackers on a system.
- Criminal or unauthorized use or misuse of systems or data.
- Unusual or unexpected computer behavior.
- Observed unauthorized access to a secure location.

How to report:

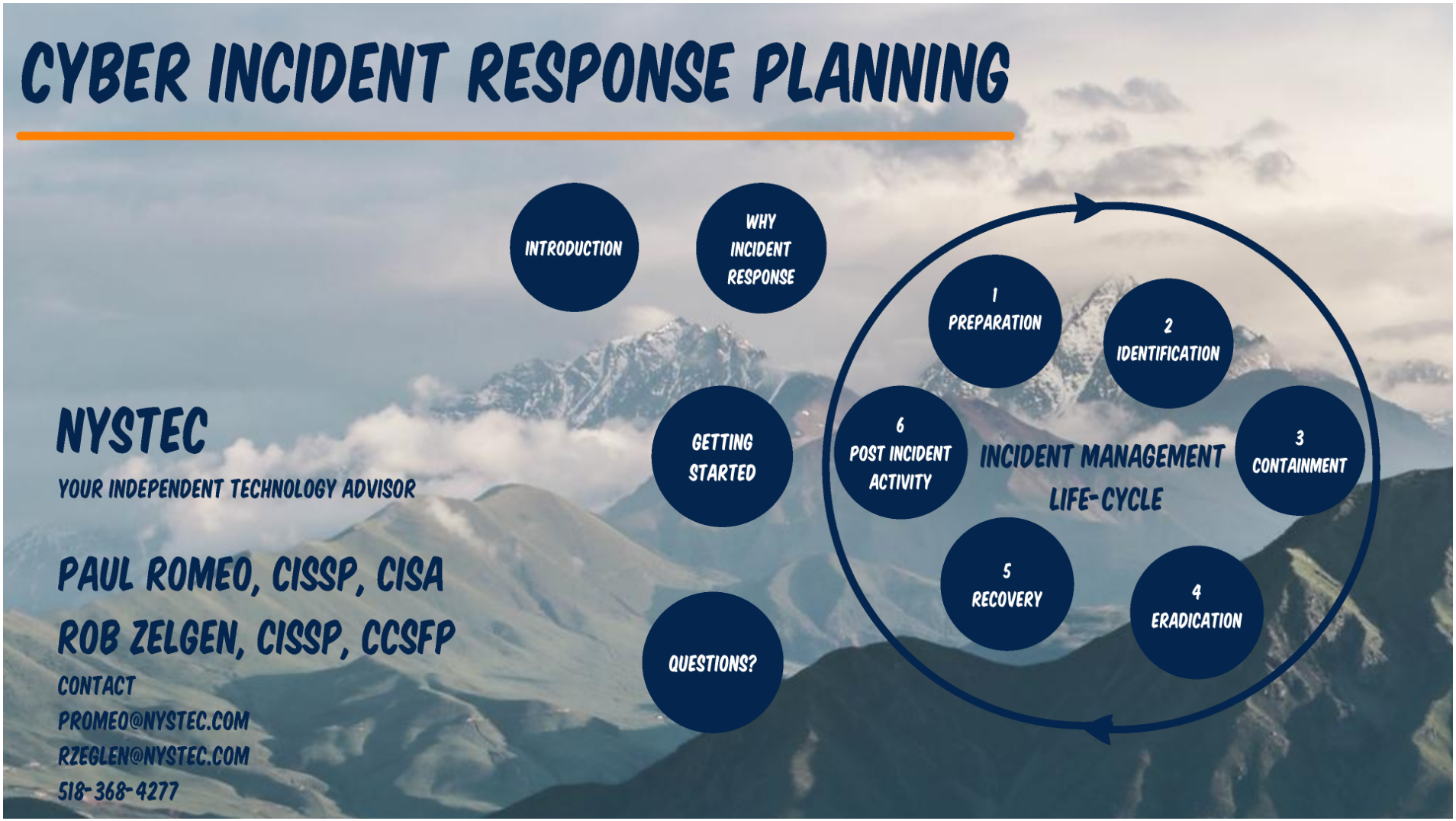
1: Ensure your own safety and the safety of others. Contact first responders, if appropriate.

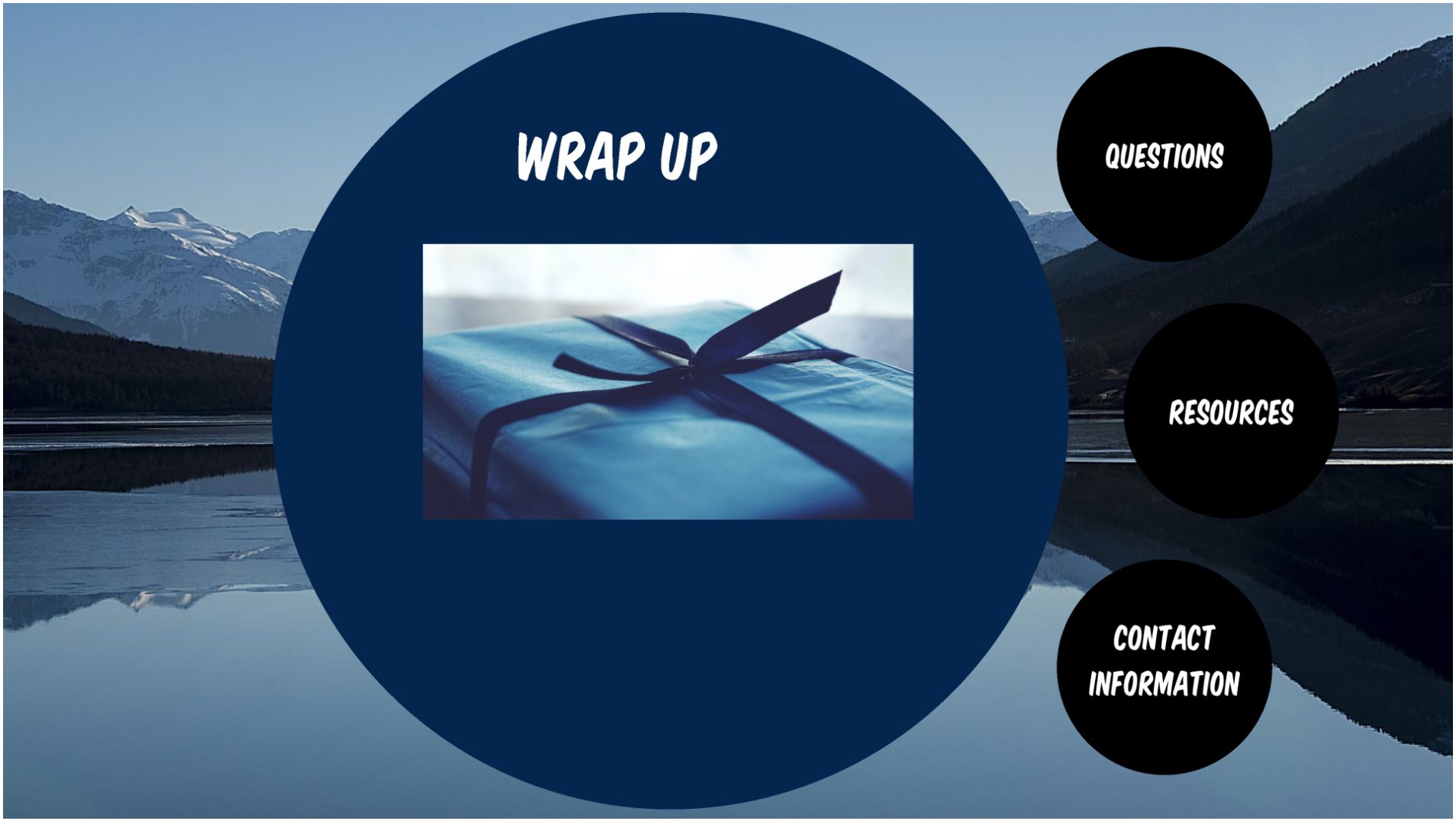
2: Call or text the NYSTEC Incident Response Team (NIRT): (518) [redacted]

NYSTEC
YOUR INDEPENDENT TECHNOLOGY ADVISOR

If you see something, say something.

Be observant. Report suspicious activity.


CYBER INCIDENT RESPONSE PLANNING
INTRODUCTION
WHY INCIDENT RESPONSE
GETTING STARTED
QUESTIONS?
1 PREPARATION
2 IDENTIFICATION
3 CONTAINMENT
4 ERADICATION
5 RECOVERY
6 POST INCIDENT ACTIVITY
INCIDENT MANAGEMENT LIFE-CYCLE
NYSTEC
YOUR INDEPENDENT TECHNOLOGY ADVISOR
PAUL ROMEO, CISSP, CISA
ROB ZELGEN, CISSP, CCSFP
CONTACT
PROMEO@NYSTEC.COM
RZEGLEN@NYSTEC.COM
518-368-4277


WRAP UP
QUESTIONS
RESOURCES
CONTACT INFORMATION


QUESTIONS


RESOURCES

INCIDENT REPONSE PLANNING 101

TOOLS AND RESOURCES

a. REPORTING CYBER CRIMES:

a. Federal Bureau of Investigation: https://www.ic3.gov/default.aspx
b. New York State Police: https://www.troopers.ny.gov/Criminal_Investigation/Computer_Crimes/

b. FRAMEWORKS

c. NIST RMF: https://csrc.nist.gov/Projects/Risk-Management/rmf-overview
d. ISO: https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final
e. PCI: https://www.iso.org/standard/54533.html
f. DHS Incident Response: https://www.dhs.gov/cisa/cyber-incident-response

c. HARDENING GUIDES

g. Center for Internet Security www.cisecurity.org
h. DOD Cyber Exchange: https://public.cyber.mil/stigs/downloads/

d. ONLINE TOOLS AND SITES

i. https://www.hybrid-analysis.com/
j. https://www.virustotal.com/#/home/upload
k. https://www.joesandbox.com/
l. http://ether.gtisc.gatech.edu/web_unpack
m. https://blog.didierstevens.com/programs/pdf-tools/
n. https://app.any.run/
o. https://mxtoolbox.com/
p. https://www.knowbe4.com/
q. https://www.phishing.org/
r. SANS:https://www.sans.org/

e. CENTRALIZED LOGGING/ORCHESTRATION

s. SYSLOG:
t. Sysmon: https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon
u. ELK: https://www.elastic.co/elk-stack
v. ELSA: https://github.com/Security-Onion-Solutions/security-onion/wiki/ELSA\
w. RSA's NetWitness Orchestrator: https://www.rsa.com/en-us/products/threat-detection-response/security-automation-orchestration

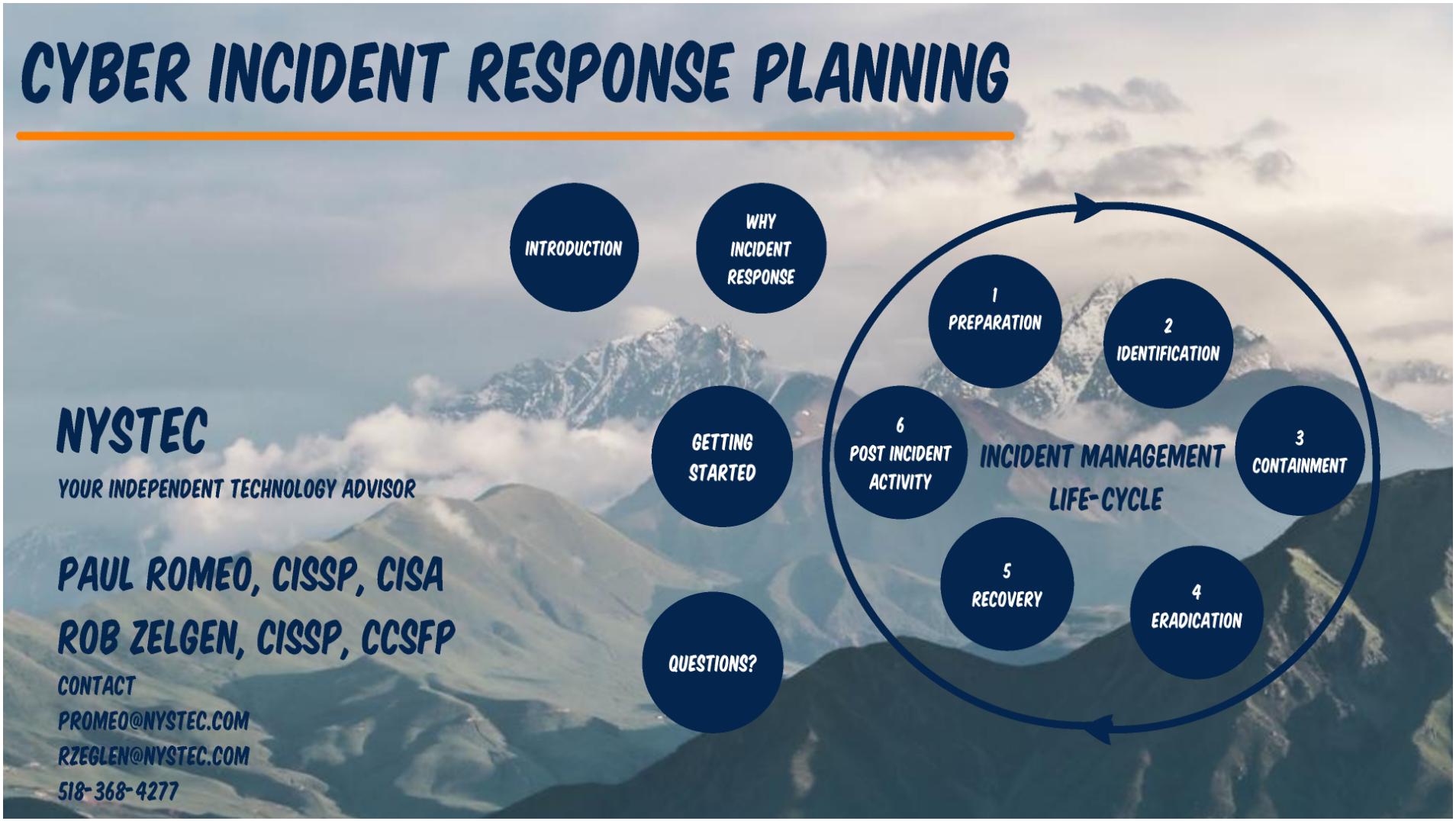
f. SECURITY INFORMATION AND EVENT MANAGEMENT

x. SNARE: https://www.snaresolutions.com/solutions/log-monitoring-and-management/
y. Splunk: https://www.splunk.com/
z. ArcSight: https://www.microfocus.com

g. INTRUSION DETECTION

aa. SNORT: https://www.snort.org/


CONTACT INFORMATION
ROB ZEGLEN CISSP
RZEGLEN@NYSTEC.COM
518-368-4277
PAUL ROMEO CISSP
PROMEO@NYSTEC.COM
518-859-2687


CYBER INCIDENT RESPONSE PLANNING
INTRODUCTION
WHY INCIDENT RESPONSE
GETTING STARTED
QUESTIONS?
NYSTEC
YOUR INDEPENDENT TECHNOLOGY ADVISOR
PAUL ROMEO, CISSP, CISA
ROB ZELGEN, CISSP, CCSFP
CONTACT
PROMEO@NYSTEC.COM
RZEGLEN@NYSTEC.COM
518-368-4277
1 PREPARATION
2 IDENTIFICATION
3 CONTAINMENT
4 ERADICATION
5 RECOVERY
6 POST INCIDENT ACTIVITY
INCIDENT MANAGEMENT LIFE-CYCLE