continuum® Security

# Key Factors in Successfully Onboarding Customers and Managing Incident Response

Drew Sanford
Drew.Sanford@Continuum.net

Austin Roberts
Austin.Roberts@Continuum.net

# Our Agenda

01 Current Security Trends

02 War Stories

03 Power of Preparation (Onboarding)

04 Incident Response

05 Risk Tolerance

# Speaker Introduction

Director of SOC Operations, Continuum Security

## Drew Sanford

- 25+ years of experience providing IT and security solutions to businesses of all sizes
- Former owner of a Nashville-based MSP and CARVIR, his recently acquired cyber security company.
- Served as Outsourced CIO of multiple global manufacturing and distribution organizations
- As the Director of SOC Operations at Continuum Managed Services, he continues to work closely with organizations to provide insight and best practices for securing business networks.
- Currently manages multiple SOC teams in the US and India
- Regularly speaks at countless industry events for helping organizations understand the risks lack of preparation for cyber threats poses.
- Coached hundreds of companies on marketing and selling IT solutions and security packages.

# Current Security Trends

continuum® Security

# What the SMB Said is Compelling

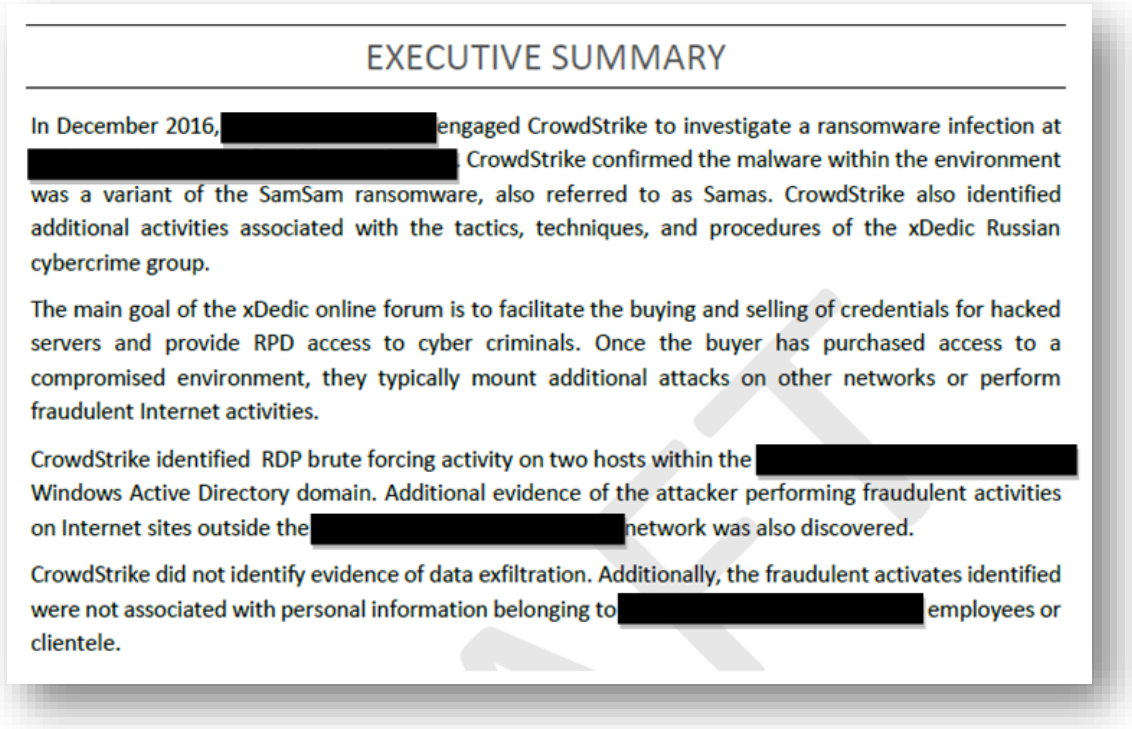
In this survey of 850 global organizations, 64% of respondents have reported that their organization has suffered a cyber-attack.

- Impact on respondents who suffered through a cyber attack was **an average cost of $53,987**.

# War Stories

continuum® Security

# SMB Example – Law Firm



EXECUTIVE SUMMARY

In December 2016, [redacted] engaged CrowdStrike to investigate a ransomware infection at [redacted]. CrowdStrike confirmed the malware within the environment was a variant of the SamSam ransomware, also referred to as Samas. CrowdStrike also identified additional activities associated with the tactics, techniques, and procedures of the xDedic Russian cybercrime group.

The main goal of the xDedic online forum is to facilitate the buying and selling of credentials for hacked servers and provide RPD access to cyber criminals. Once the buyer has purchased access to a compromised environment, they typically mount additional attacks on other networks or perform fraudulent Internet activities.

CrowdStrike identified RDP brute forcing activity on two hosts within the [redacted] Windows Active Directory domain. Additional evidence of the attacker performing fraudulent activities on Internet sites outside the [redacted] network was also discovered.

CrowdStrike did not identify evidence of data exfiltration. Additionally, the fraudulent activates identified were not associated with personal information belonging to [redacted] employees or clientele.

- 2 MSPs that had no idea how to proceed
- 5,000,000 Encrypted Files
- Paid $25,360 Ransom (Total Recovery over $225,000)
- Backups Were Corrupted
- Down for 2 Weeks
- 39 Hours to Restore per TB

# Power of Preparation (Onboarding)

continuum® Security

# Before An Attack: Onboard with the End in Mind?

**Onboarding for security** is similar and yet very different from Managed Services.

**Managed Services**

- Internal Systems
- Backup Recovery Plans
- Employee Roles
- Stability of Systems (Patching, Performance, etc.)
- Taking the noise out of the system
- Use Policies

**Managed Security**

- Attack Surfaces
- Points of Entry
- User Habits
- Security Policies
- HR Procedures
- Legal Impact (Do you know your clients coverage and process?)

# Reduce Your Attack Surface

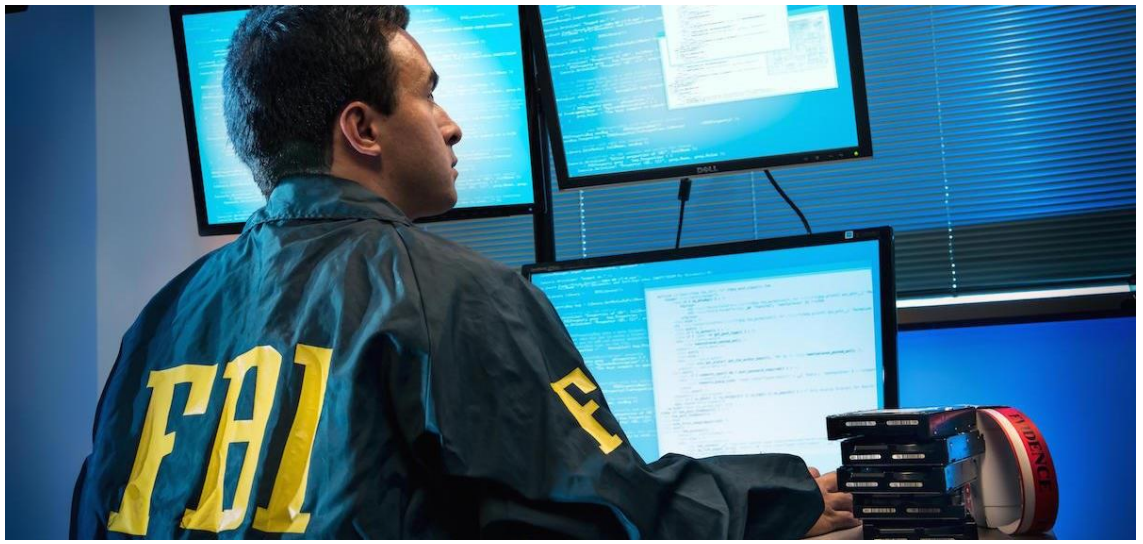
## Prep Stage Checklist

- ☐ Schedule a vulnerability assessment
- ☐ Check backup routines (test at least twice monthly)
- ☐ Prevent spam from entering the network
- ☐ Apply security-minded group policies
- ☐ Lock down application data & windows/temp folders
- ☐ Setup Active Directory account lockout policy
- ☐ Increase password complexity requirements
- ☐ Auto-expire inactive accounts after X days
- ☐ Establish unknown USB device policy
- ☐ Setup OS updates and patch management
- ☐ Deploy anti-virus/advanced enpoint security
- ☐ Deploy mobile devices security capabilities
- ☐ Configure web/DNS gateway security
- ☐ Setup/configure logging & SIEM console
- ☐ Test and update firewall rules/engine
- ☐ Review finding from vulnerability scan
- ☐ Close unnecessary ports
- ☐ Close RDP/require VPN for remote access
- ☐ Geo-Block international traffic
- ☐ Set up intrusion prevention/intrusion detection
- ☐ Set up multi-factor authenication/SSO
- ☐ Setup dark web scanning for stolen credentials
- ☐ Setup encryption on mobile devices and email
- ☐ Establish employee security awareness training
- ☐ Collect a copy of clients cyber insurance policy
- ☐ Review/update existing policies & procedures
- ☐ Verify data owner(s) and emergency processes
- ☐ Improve backup routine as needed
- ☐ Document ALL information in internal systems

# Before An Attack: Communication

## Communication Plan With Outside

- Law Enforcement
- ISPs
- Software/Hardware Vendors
- The Media
- Other Incident Response Teams
- Legal and Insurance

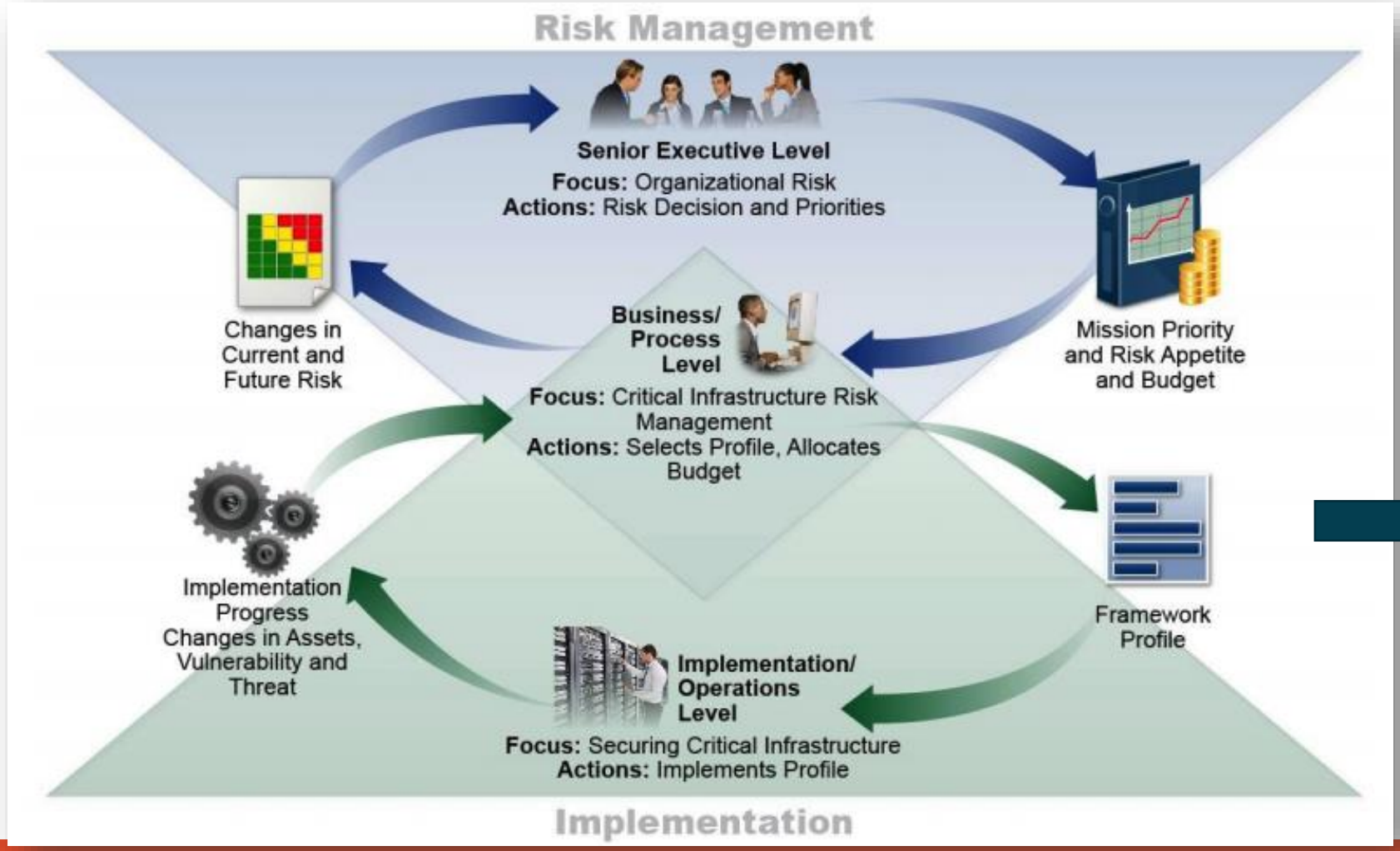


# Before An Attack: Who's In Charge?

## Communication Plans Should Document

- **Who is authorized** what can (and cannot) be shared
- **When** you should hire an outside communication management firm and/or legal firm
- Required staff training and **processes** for handling the media if/when necessary
- Importance of not revealing sensitive information
- **How to handle contact, communication and interactions with authorized team members**
- A statement of the current status of an incident so all interactions are up to date and consistent

# National Institute of Science & Technology (NIST)




Identify
Protect
Detect
**Respond**
Recover

# Incident Response

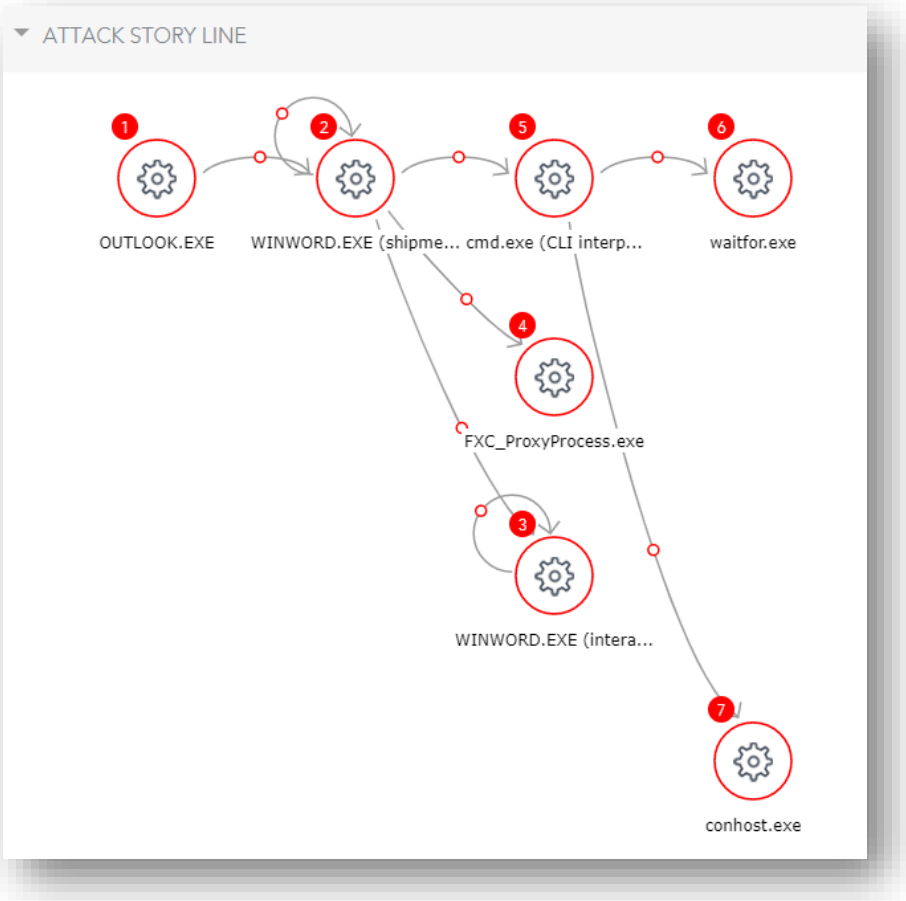
continuum® Security

# What is an Incident?

- What is an Event?
  - Any observable occurrence in a system or network
  - Adverse event – events with negative consequences
- What is a Security Incident?
  - A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices

# What is an Incident?

- Examples of a Security Incident
  - Users are **tricked into opening a "UPS Notice"** sent via email that is actually malware; running the tool has infected their computers and established connections to an external host
  - An **attacker** obtains sensitive data and **threatens** that the details will be released publicly **if the organization does not pay**
  - A **user exposes sensitive information** on social or sharing sites
  - An attacker uses a botnet to send high volumes of connections at a web server, causing it to crash (**Denial of Service**)

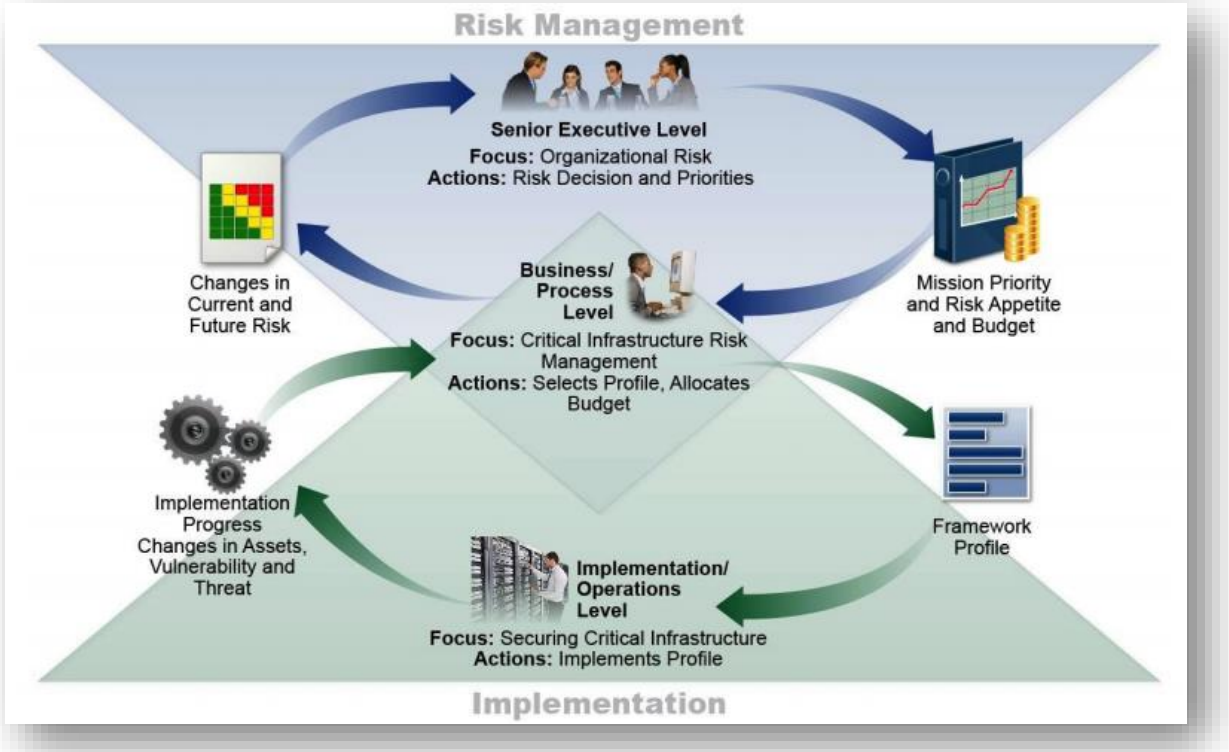


# What is an Incident Response Plan?

- In an attack, it is critical to respond quickly in an **organized manner**. (Muscle Memory)
- Supports **responding to incidents systematically** so the appropriate actions are taken
- Helps **minimize the loss or theft of information** and disruption of services
- Allows for the information gathered to help further **secure you against future incidents**

# Incident Response Plan Development

- 3 Parts to an Incident Response Program
  - Incident Response **Policy**
  - Incident Response **Plan**
  - Individual **Procedures**

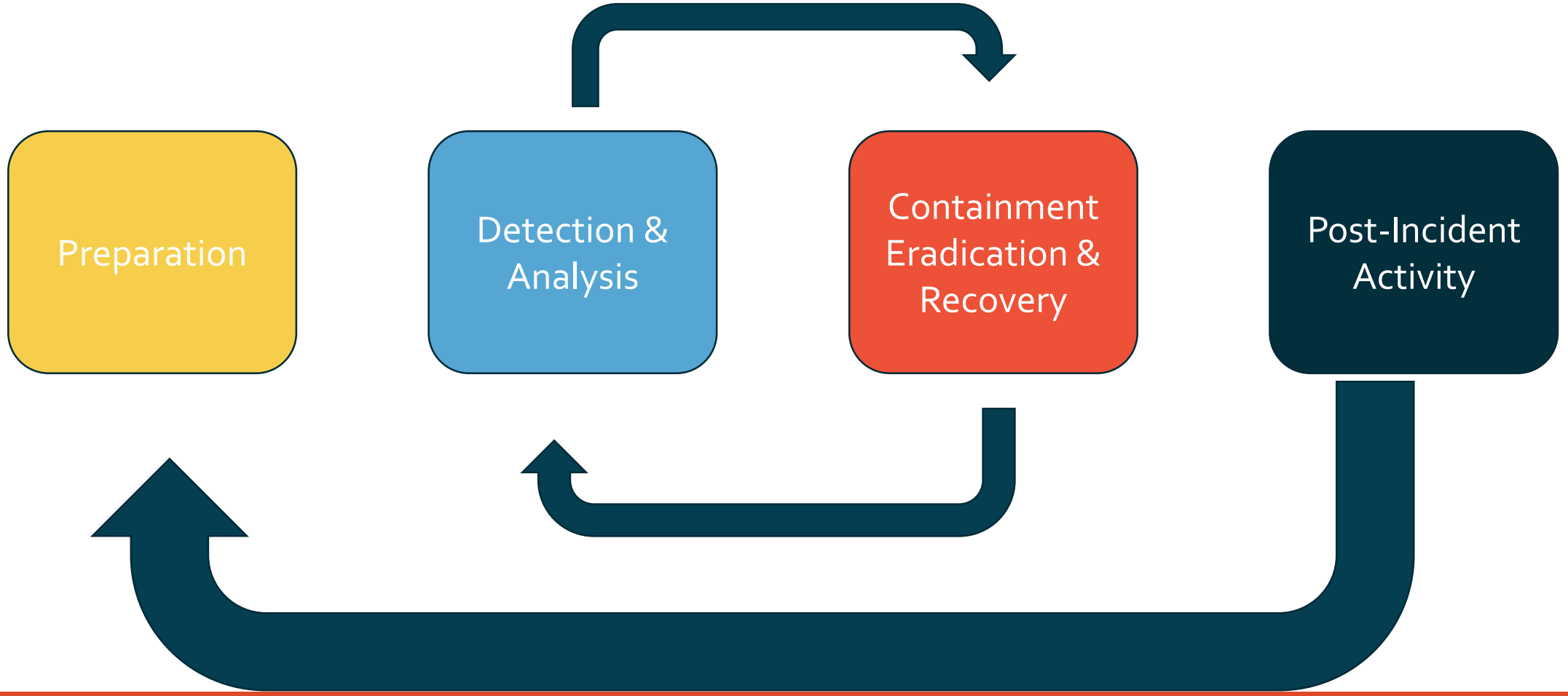



https://www.nist.gov/sites/default/files/documents/itl/preliminary-cybersecurity-framework.pdf

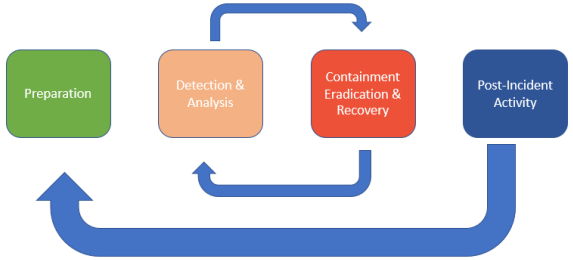
# During An Attack: Responding To Crisis

continuum® Security

# Incident Response Life Cycle (NIST)

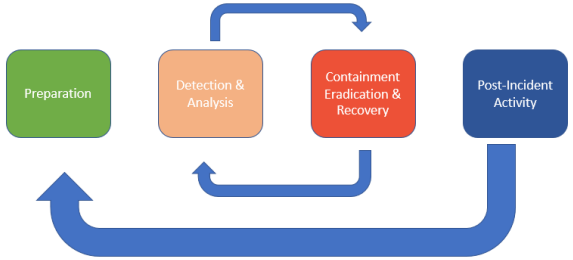


# Detection & Analysis



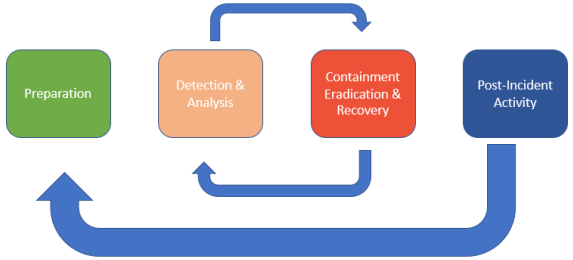

- Attack Vectors
  - Know the common ones and develop responses to each
    - Removeable/External Media, Attrition (brute force methods), Web, Email, Impersonation, Improper Usage (violation of the acceptable use policies), Theft, Document Responses to Unknown or New Threat Types
- Validate the reported incident. User reports can be inaccurate.
- Declare an Incident (Critical)
- Assemble the response Team

# Detection & Analysis



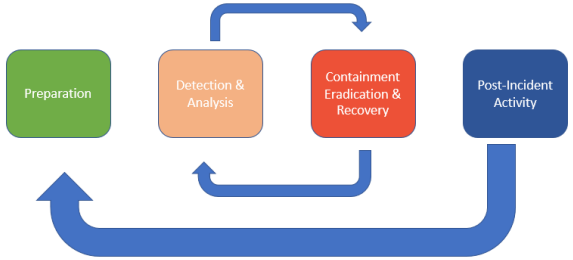

- Sources and Indications of an Incident
  - Alerts
    - IDPSs, SIEMs, AV/EDR software, File Integrity software, Third-party monitoring services
  - Logs
    - Operating System, Service, Application, Network Device, Network Flows
  - People
    - People within the organization
    - People from other organizations

# Detection & Analysis



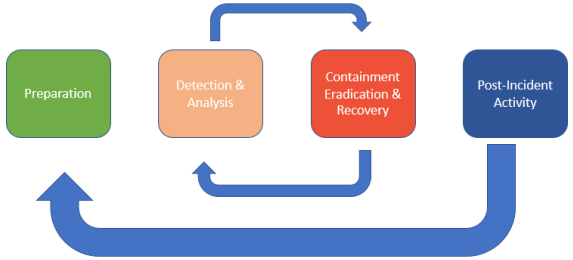

- Analysis
  - Profile Systems
    - Understand Normal Behavior
  - Create a Log Retention Policy
  - Perform Event Correlation
    - You many need to compare logs from differing sources to see the scope of an attack
    - An AV or EDR may see an infection on a system and point to a cause
    - The Firewall logs may show the full source and scope of an intrusion.
  - Keep all Clocks Synchronized

# Detection & Analysis



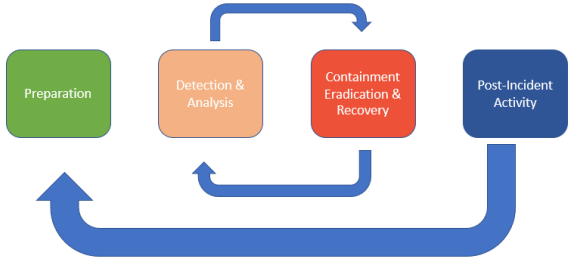

- Analysis
  - Use Internet Search Engines for Research
  - Run Packet Sniffers, Vulnerability Scans and Know how to Use Them
  - Seek Help from Others
- Documentation
  - Document All Findings
  - **Start immediately on suspicion of an incident**

# Containment Eradication & Recovery



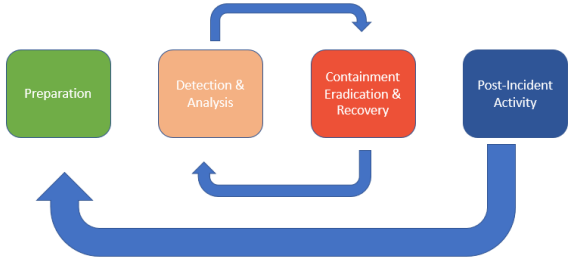

- Considerations for Containment
  - Potential Damage to and theft of resources
  - Need for **Evidence Preservation** (Legal and Insurance)
  - Service Availability
  - Time and Resources Needed to Implement
  - Effectiveness of the Strategy
  - Duration of the Solution (Emergency Workaround vs. Permanent Solution)

# Containment Eradication & Recovery




- Some Thoughts for Emergency Containment
  - Run scans to document as much information as possible
  - **Deny all international traffic in the firewall**
  - **Deny all inbound traffic across RDP and other remote access tools to the client site *Open RDP is a massive security risk***
  - Check all security and system logs for unusual activity
  - Test your backups
  - **Check for stolen credentials on the Dark Web *Should be done regularly as part of a maintenance plan***

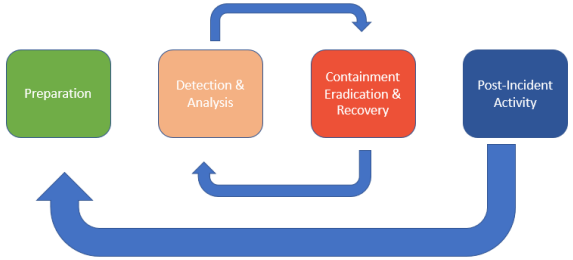
# Containment Eradication & Recovery




Immediately Following a Cyber Attack

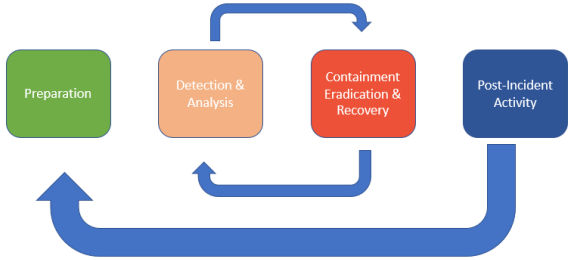
- Call your insurance company and the company attorney
- Review the Incident Response Plan, Business Continuity, or Disaster Recovery Plan
- Communicate or reiterate the company's rules of disclosure to its employees
- **Back up everything** before remediation begins

# Containment Eradication & Recovery




- Containment Activities
  - Isolate Infected Machines
  - **Do not power down machines unless you have made specific plans for it** (malicious autorun commands could cause the spread of threats on boot up)
  - Scan All Machines with Multiple Tools
  - Lock Down Firewalls and Verify All Rules
  - Monitor Firewall and Network Logs for Additional Intrusions

# Containment Eradication & Recovery

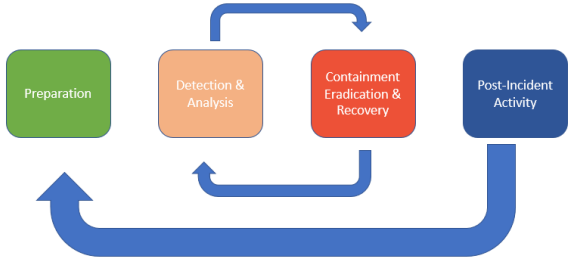



- Eradication and Recovery

*Before beginning these steps, unplug the internet connection and either unplug the switches to the network or disconnect all machines (including servers). Consider also removing the gateway IP address from DNS temporarily.*

  - Clean a domain controller of the infection
  - **Disable Autorun** on all systems
  - **Disable Windows Task Scheduler** on all systems
  - Reset all device passwords (Not just force password change)
  - Bring up one server at a time

# Containment Eradication & Recovery




- Eradication and Recovery
  - Rebuild any system that was infected and could not be cleaned
    - Any system with activity that looks like a threat and could not be identified should be wiped and rebuilt
  - Maintain forensic data needed by insurance and investigators
  - Tighten down network to restrict the same attack from happening again (Restart backup routine ASAP)
  - Use a phased approach so that remediation steps are prioritized – For a large organization this can take weeks or months – Do not rush

# During An Attack: Responding To Crisis

## Debrief

- Review and document entire incident
- Root cause analysis
- Steps to prevent in the future
- **Steps to reduce the impact in the future**

# After An Attack: Media & PR Response

# After An Attack: Media & PR

## Cost of Poorly Managed Crisis

- Loss of a good reputation and strong brand
- Loss of market value
- Loss of key relationships
- Loss of credibility
- Increased regulation

# After An Attack: Media & PR

**What to Say, What Not to Say, and How to Say it.**

**Tips for Managing the Media / Press.**

# After An Attack: Media & PR

**Be Prepared for Standard Questions**

- Were you not protected from this?!
- How did this happen?
- What about the firewall and anti-virus?
- What data did they get?
- How do we keep this from happening again?

# After An Attack: Media & PR

## What Makes Effective Key Messages

- Limit key messages to 3-5 that address the issue at hand
- Keep them short and to the point
- Repeat your key messages throughout
- Messaging is not a script; it's a tool
- When in doubt use this:

**"We are unable to respond to that question until we complete our investigation."**

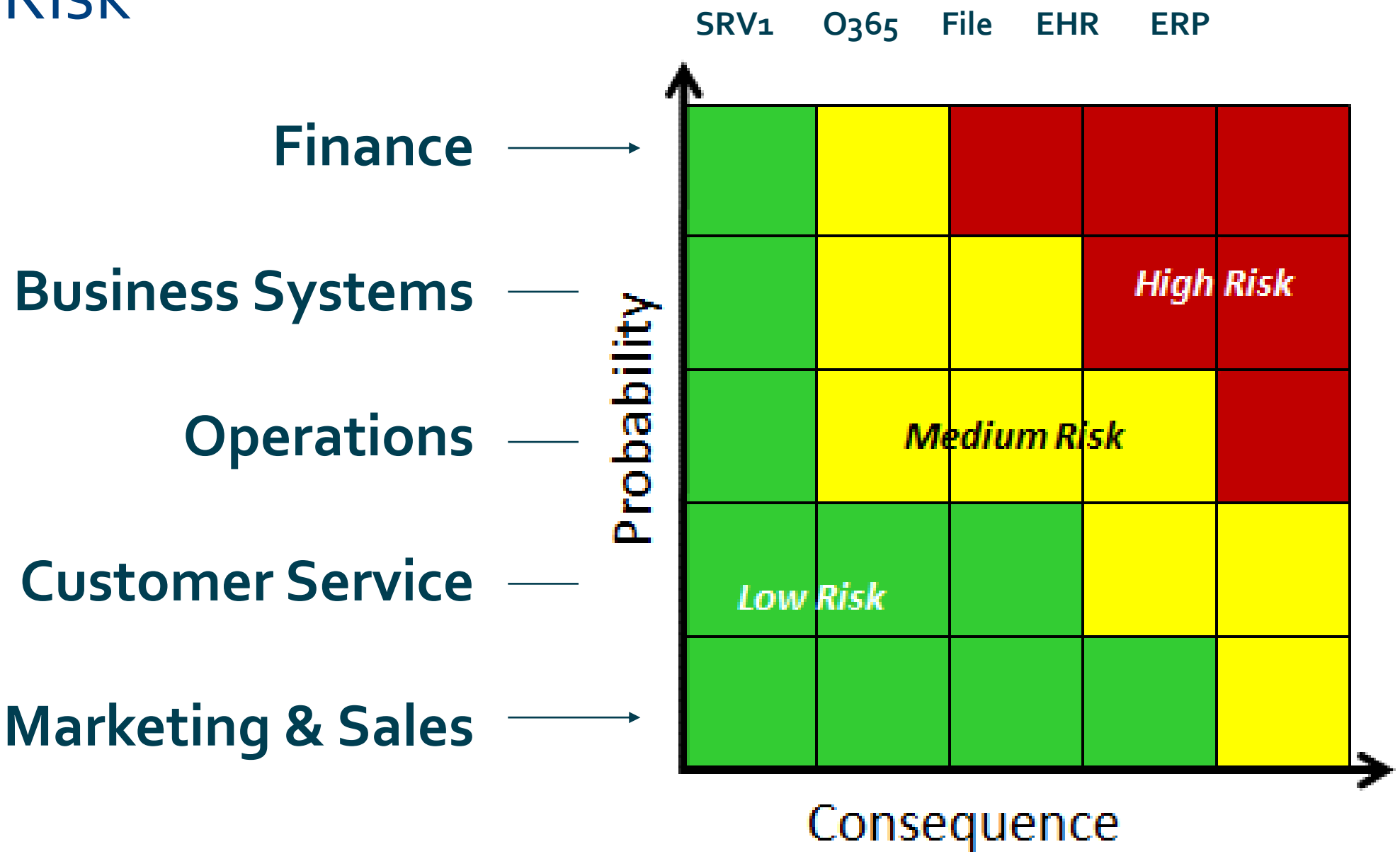
# Risk Tolerance

continuum® Security

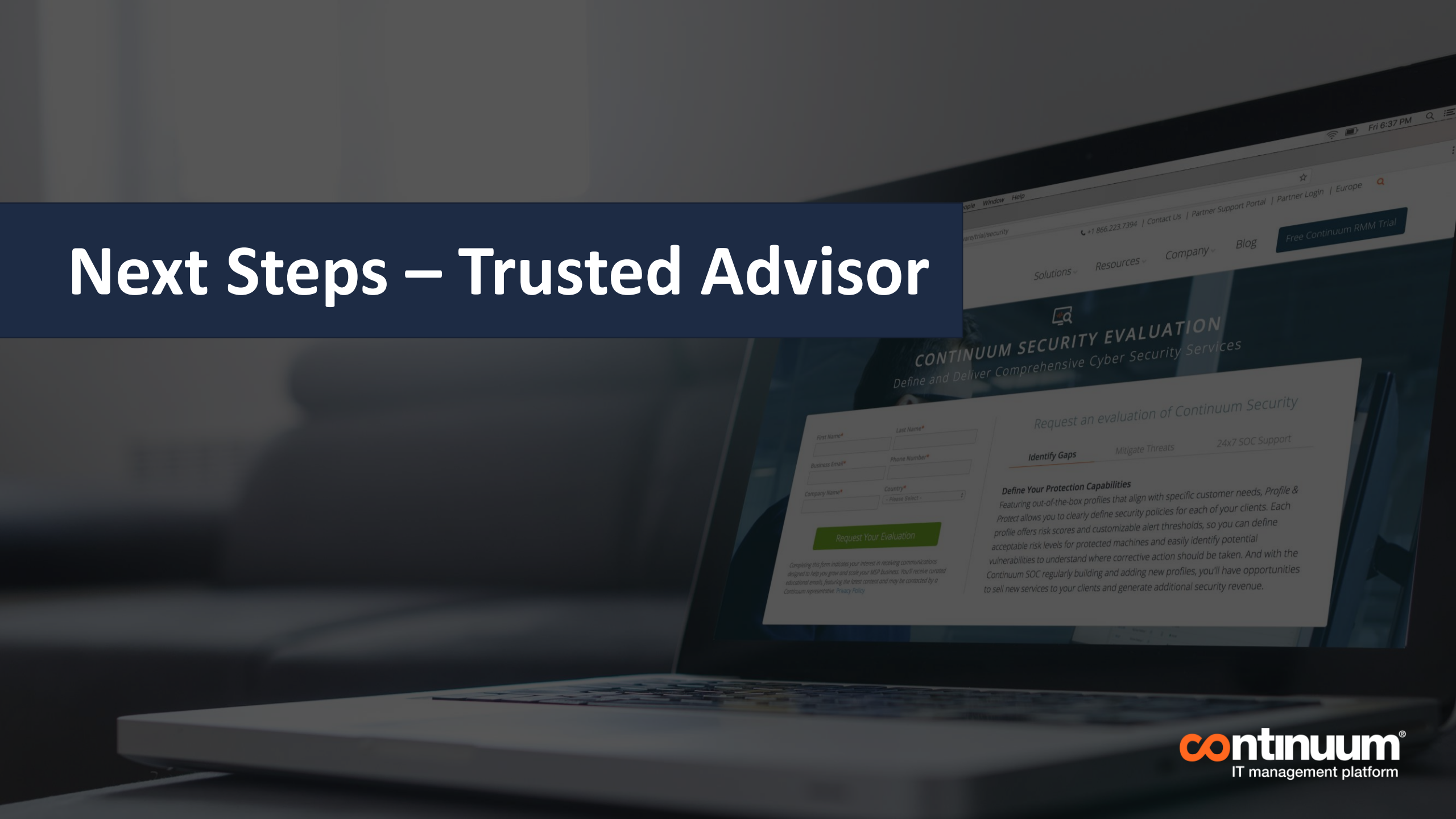
# NIST Security Framework

| Identify | Protection | Detection | Response | Recover |
|---|---|---|---|---|
| | Doors<br>Windows | Alarm | Dog | |
| | Locks | Motion Sensor | Insurance | |
| | Fence | Doorbell Camera | Police | |
| | Yard Signs | Neighborhood Watch | Baseball Bat | |

# Risk


SRV1
O365
File
EHR
ERP
Finance
Business Systems
Operations
Customer Service
Marketing & Sales
Probability
High Risk
Medium Risk
Low Risk
Consequence

# Next Steps – Trusted Advisor




continuum®
IT management platform

# Thank You

Drew Sanford
Drew.Sanford@Continuum.net

Austin Roberts
Austin.Roberts@Continuum.net