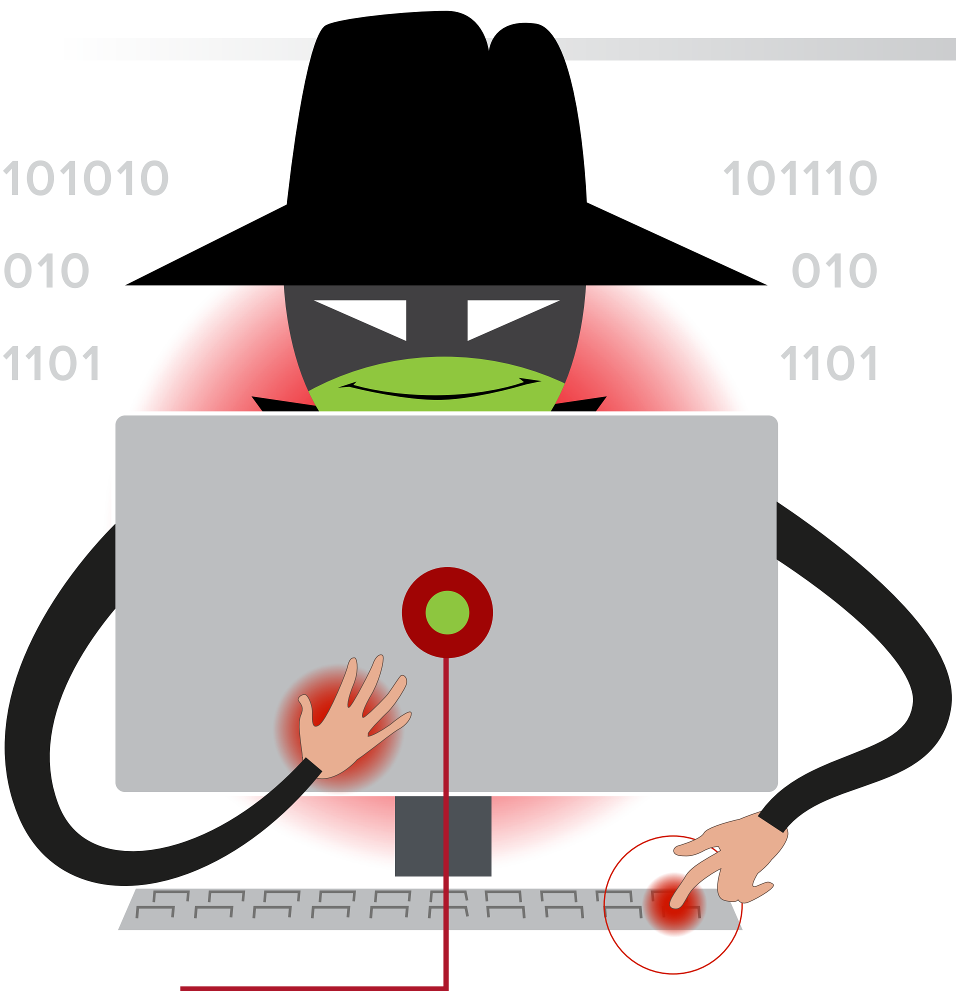
Best Practices for Improved Cyber-Attack Incident Response



The importance of having a set of policies in place to simplify and speed up incident response cannot be overstated. We have compiled this list of best practices as a result of discussion with numerous IT security professionals

Steps to take

1

What Data & Where

Know the type and location of your business critical assets

- What applications data bases and files?
- What sites, what IP address ranges or subnets?

2

Watch Data

Tune your threat detection system(s) to watch these devices

- Monitor log-ins and/or connections to these devices for these applications
- Using devices like Firewall and N-IDS/IPS or SIEMs if you have them

3

Record Conversations

Capture and record all conversations involving these applications

- On these particular devices

4

Extract Critical Conversations

Use a firewall/IDS alert to extract the relevant conversations

- From the threat detection systems (see step 2)

5

Automate

Set up the process with as little human interaction as possible

- Runs 24 x 365

Visit **cspi.com/nVoy** to learn how you can dramatically reduce your incident response time.

CSPi