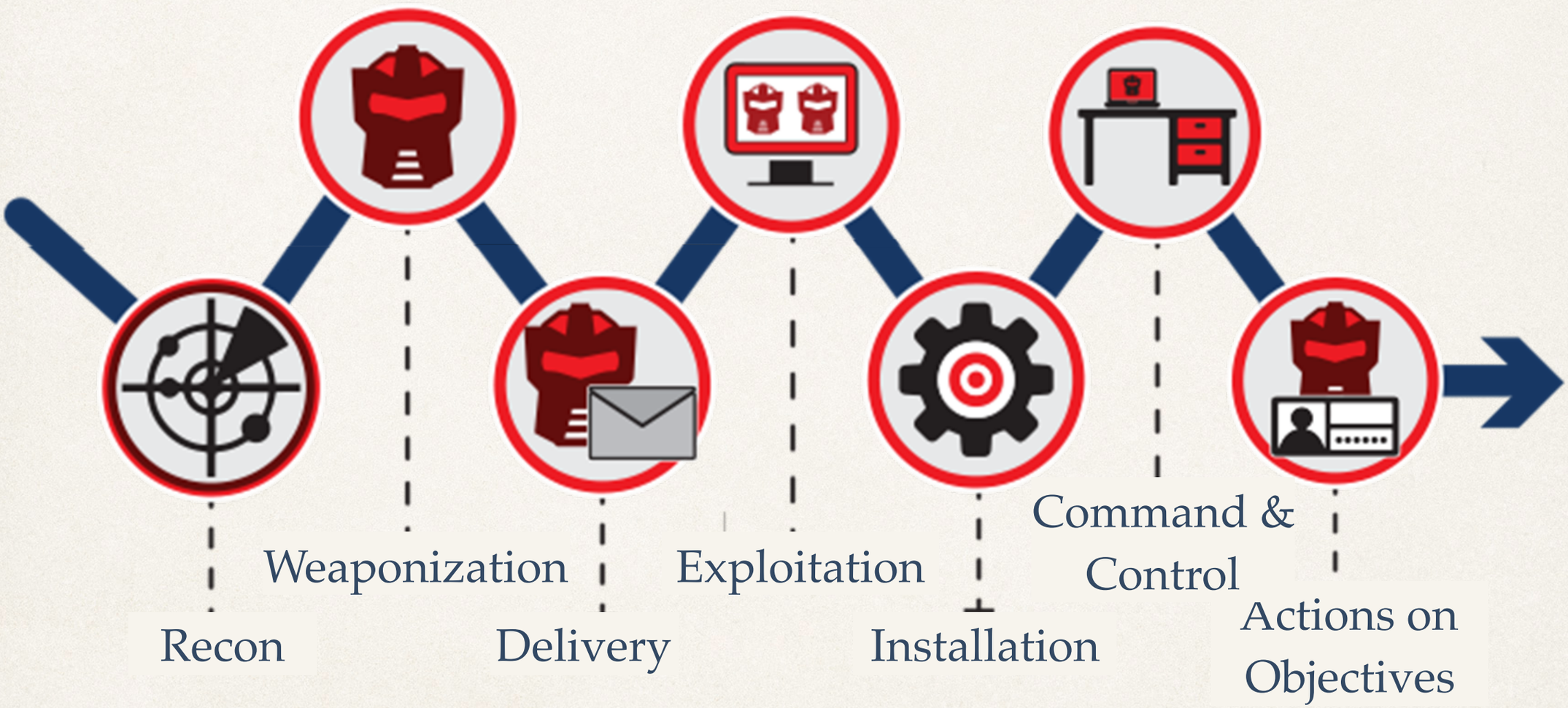
Reversing the Kill Chain

An Actionable Framework for defending against common threats

Amanda Berlin

NetWorks GROUP

Intrusion Kill Chain



Common Threats

Malicious Action

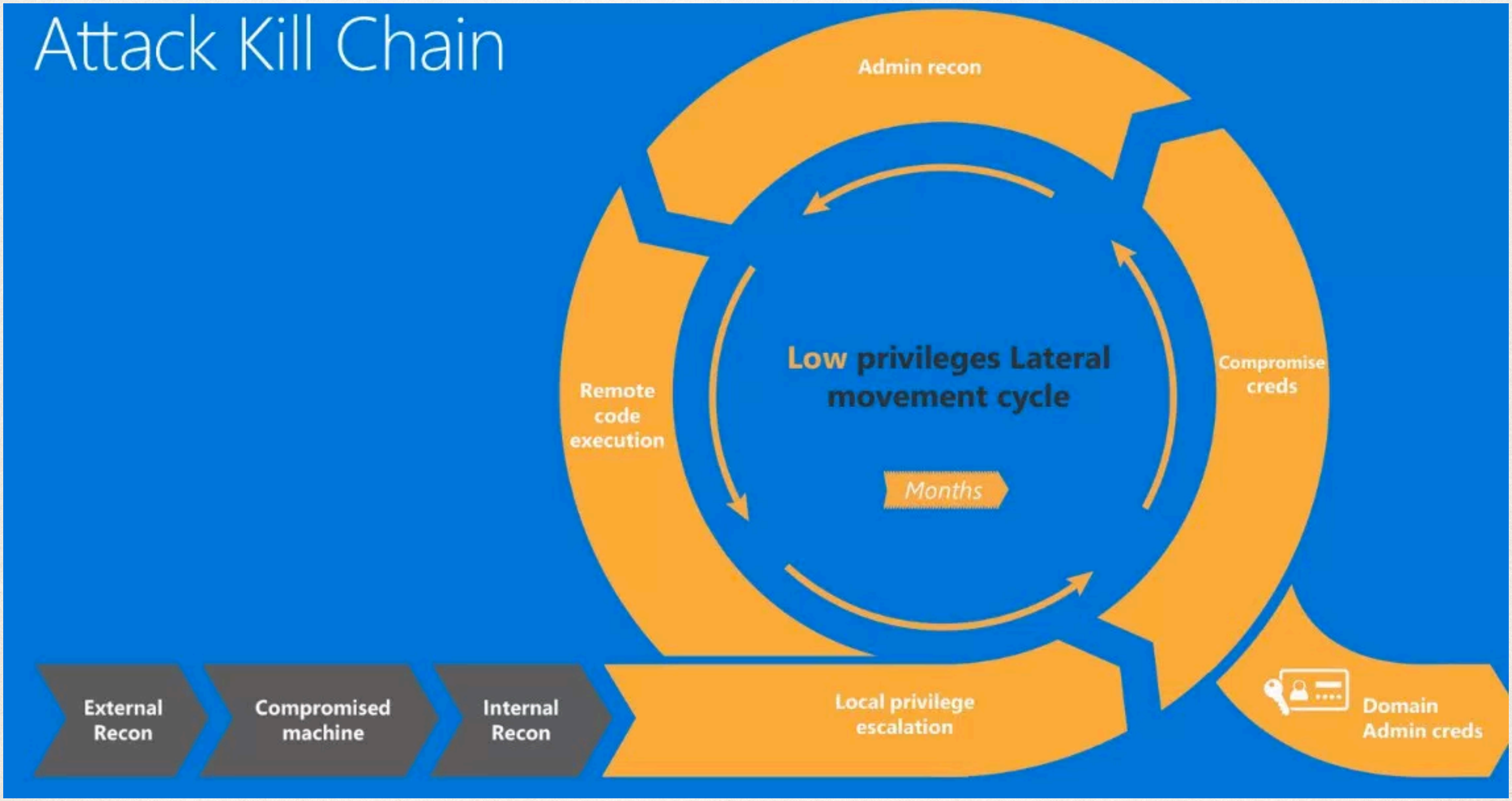
Defensive Mitigation

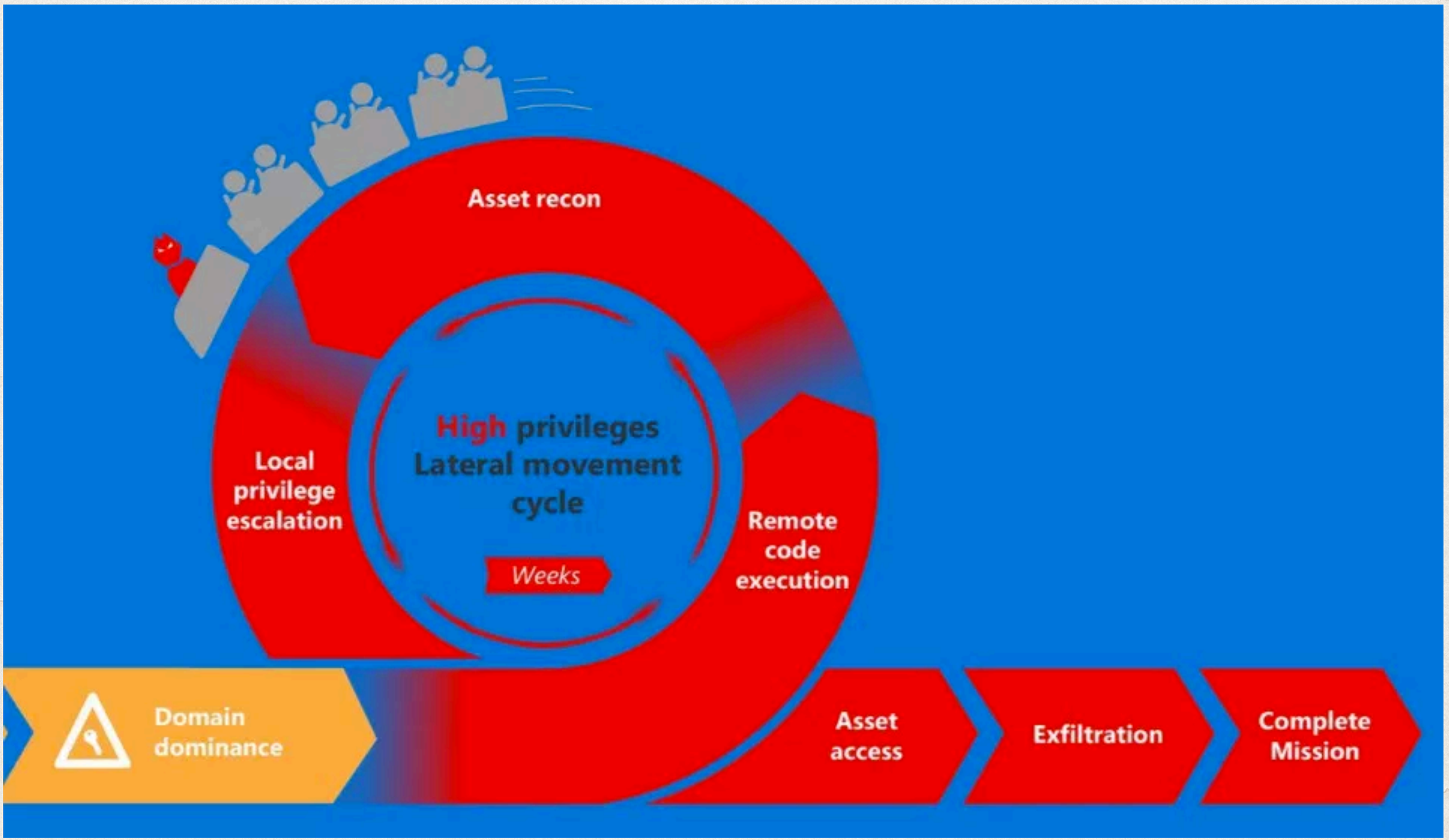
Ease of Deployment

Potential Monitoring

Specific Alerting

Attack Kill Chain




Asset recon
High privileges
Lateral movement
cycle
Weeks
Local
privilege
escalation
Remote
code
execution
Domain
dominance
Asset
access
Exfiltration
Complete
Mission


ransomware

Reconnaissance

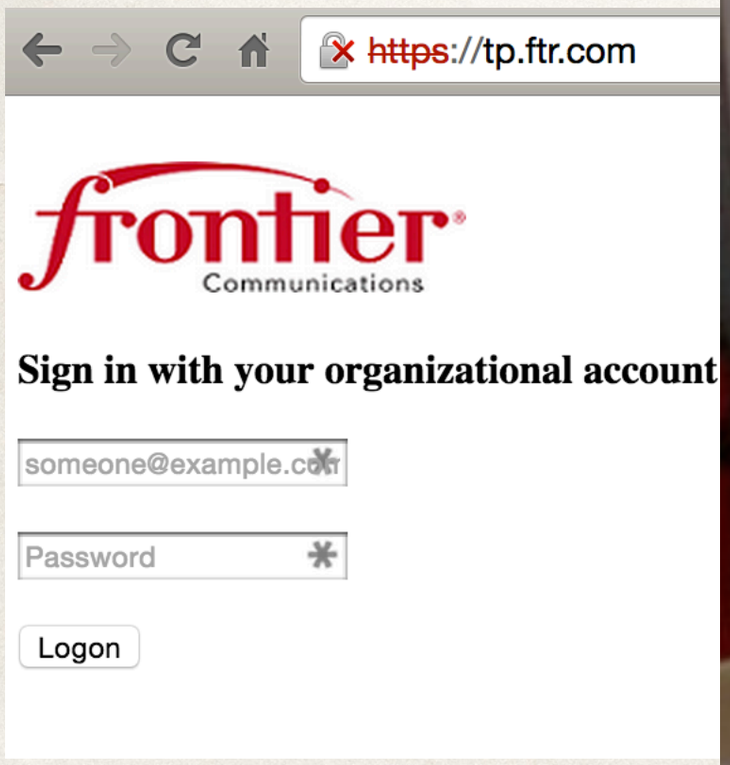
Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting



Reconnaissance

Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting

Reconnaissance

Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting

Reconnaissance

Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting

DEMO

Delivery

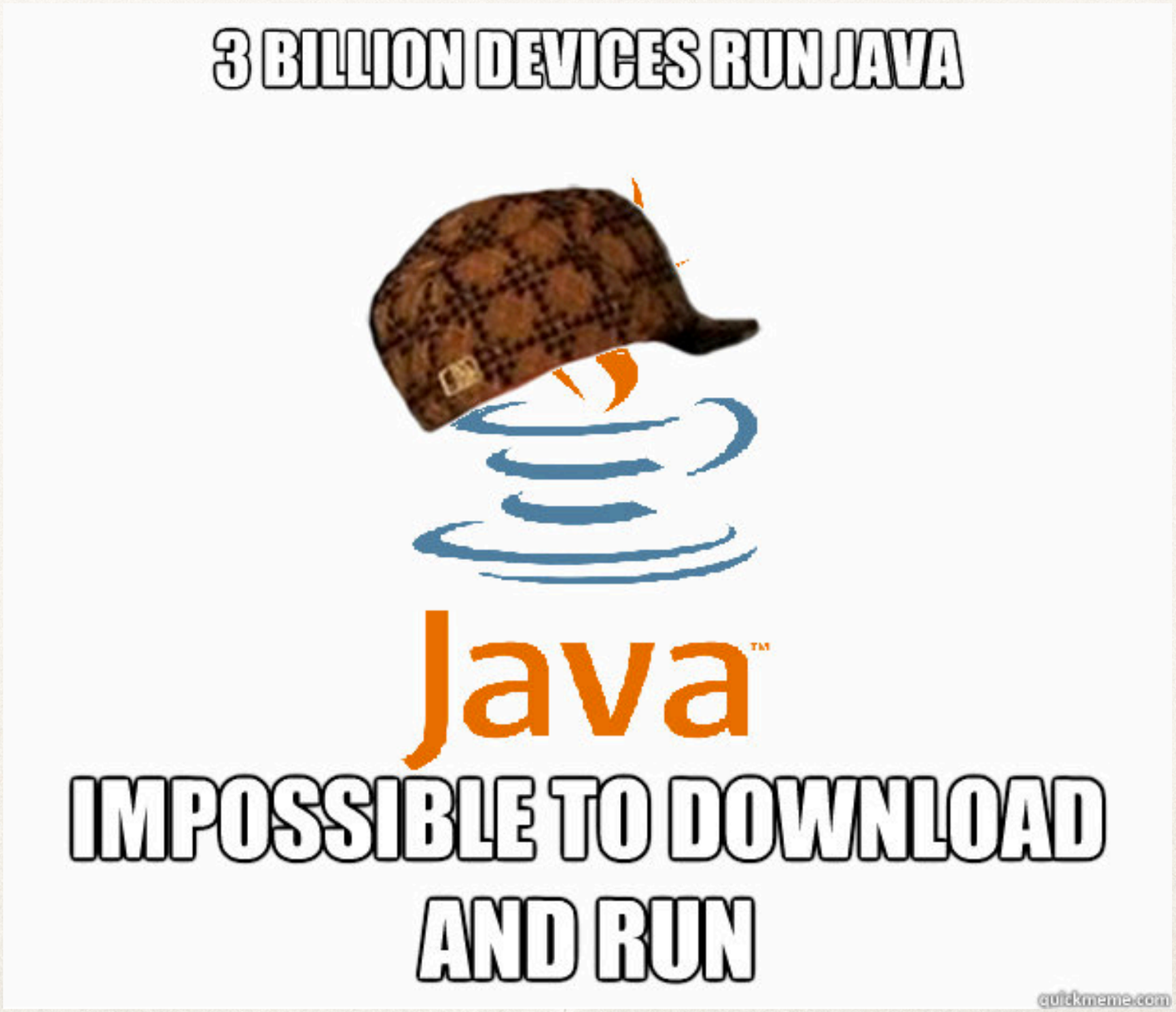
Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting



Delivery

Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting

DEMO

.hta	HTML Scripting Application
.js	JavaScript
.jse	JavaScript Encoded
.pif	Program Information File
.scr	ScreenSaver
.wsf	Windows Script File
.wsh/.wsc	Windows Script Host
.vbe	Visual Basic Encoded
.vbf	Visual Basic File

Delivery

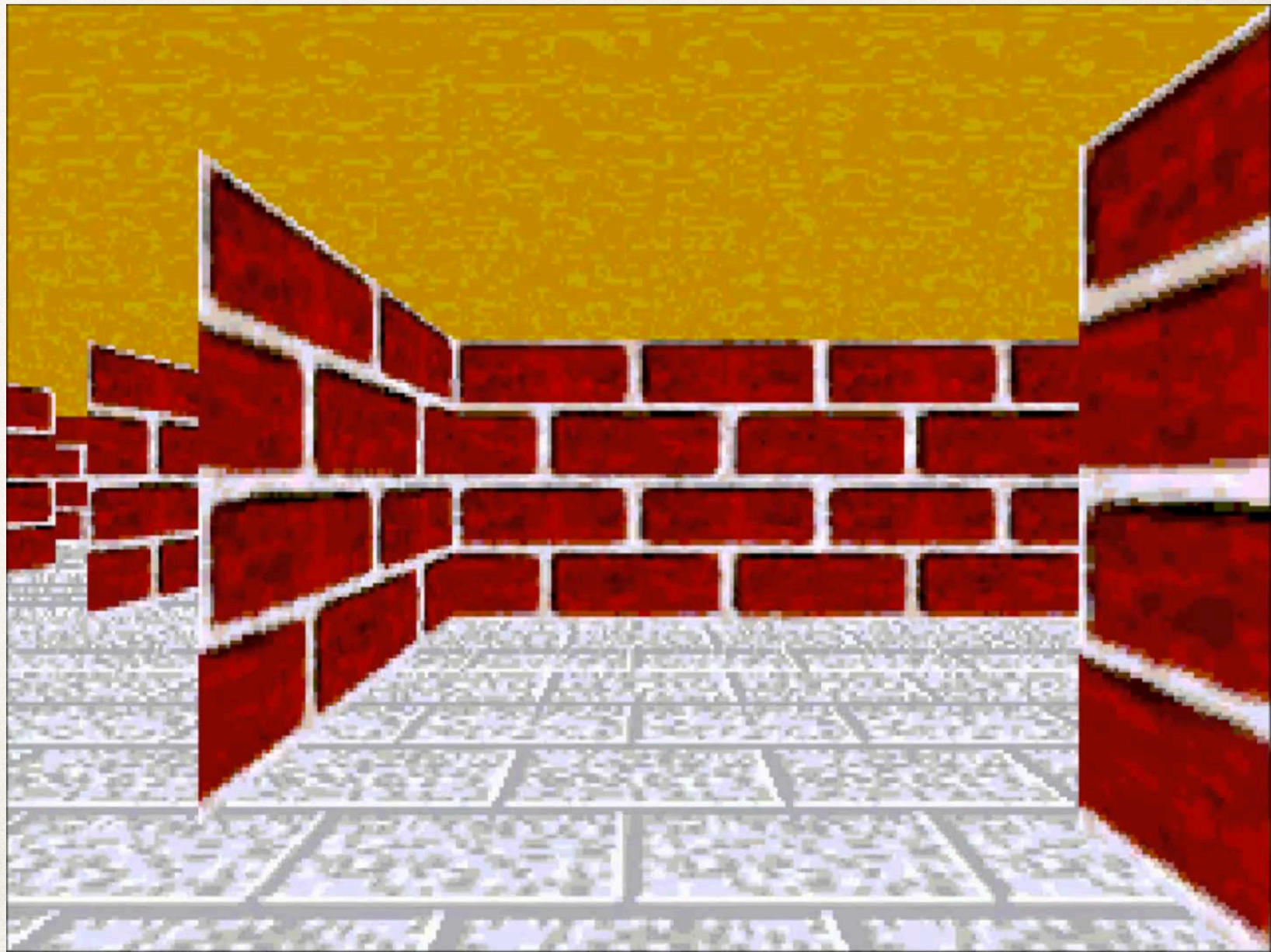
Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting



Exploitation

Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting

Exploitation

Malicious Action

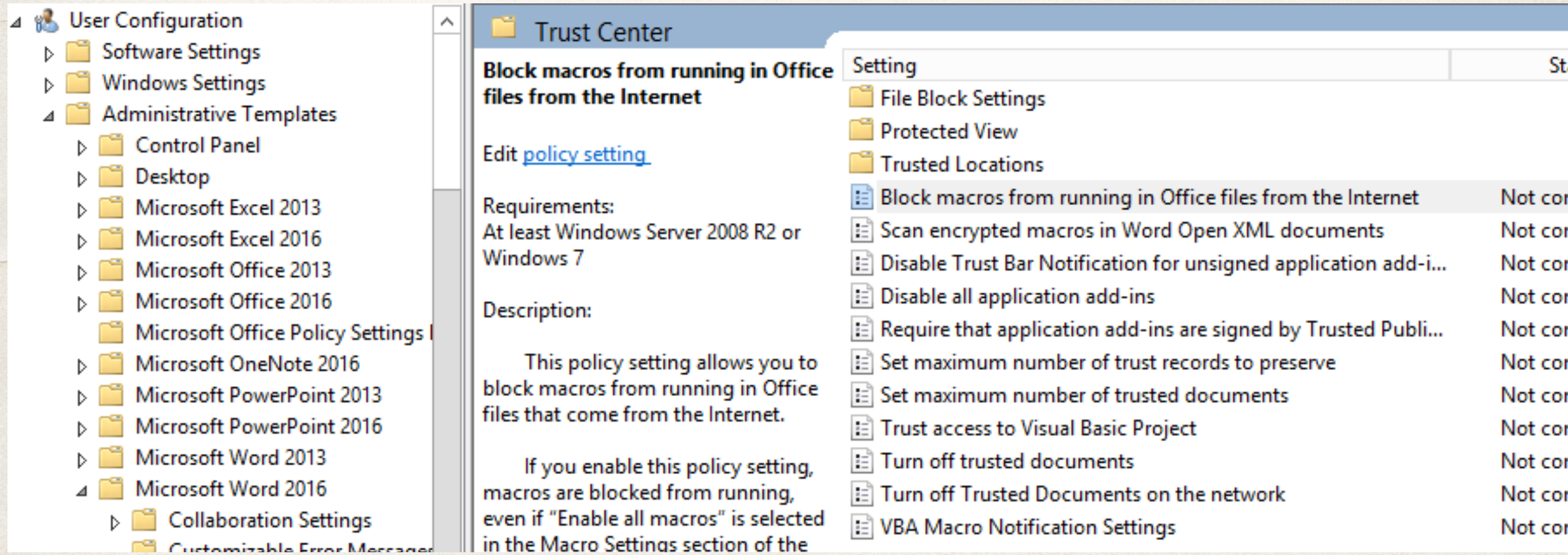
Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting

DEMO



Exploitation

Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting

```
char *decode(char *s, size_t len) {
  for (int i = 0; i < len; i++)
    s[i] ^= 0x15;
  return s;
}

int main(int argc, char *argv[]) {
  struct hostent *addr =
      gethostbyname(decode("}aaef/::lz`a`;wp:qDb!b,BrMvD", 28));
  return 0;
}
```

Installation

Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting

Installation

Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting

Installation

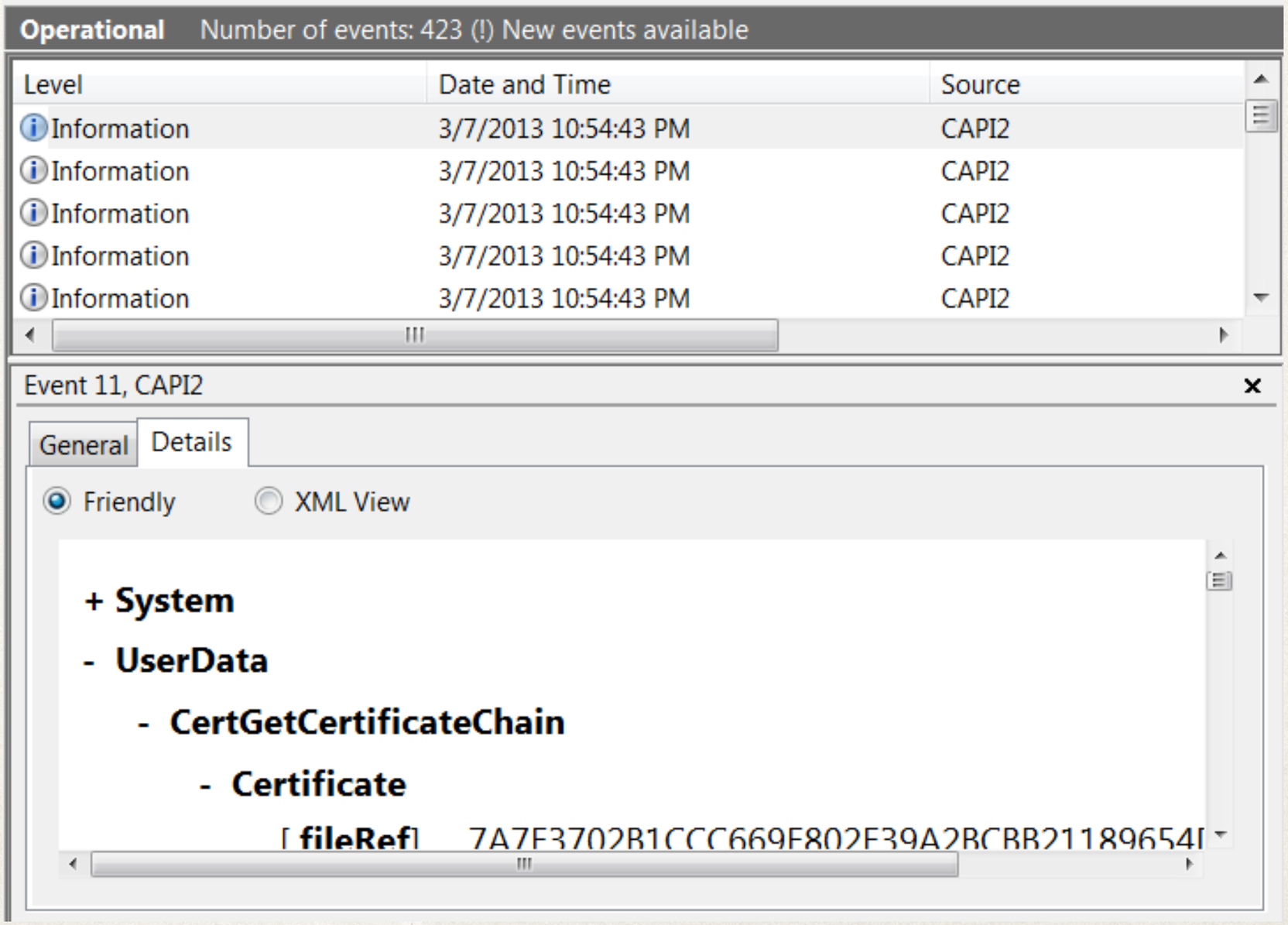
Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

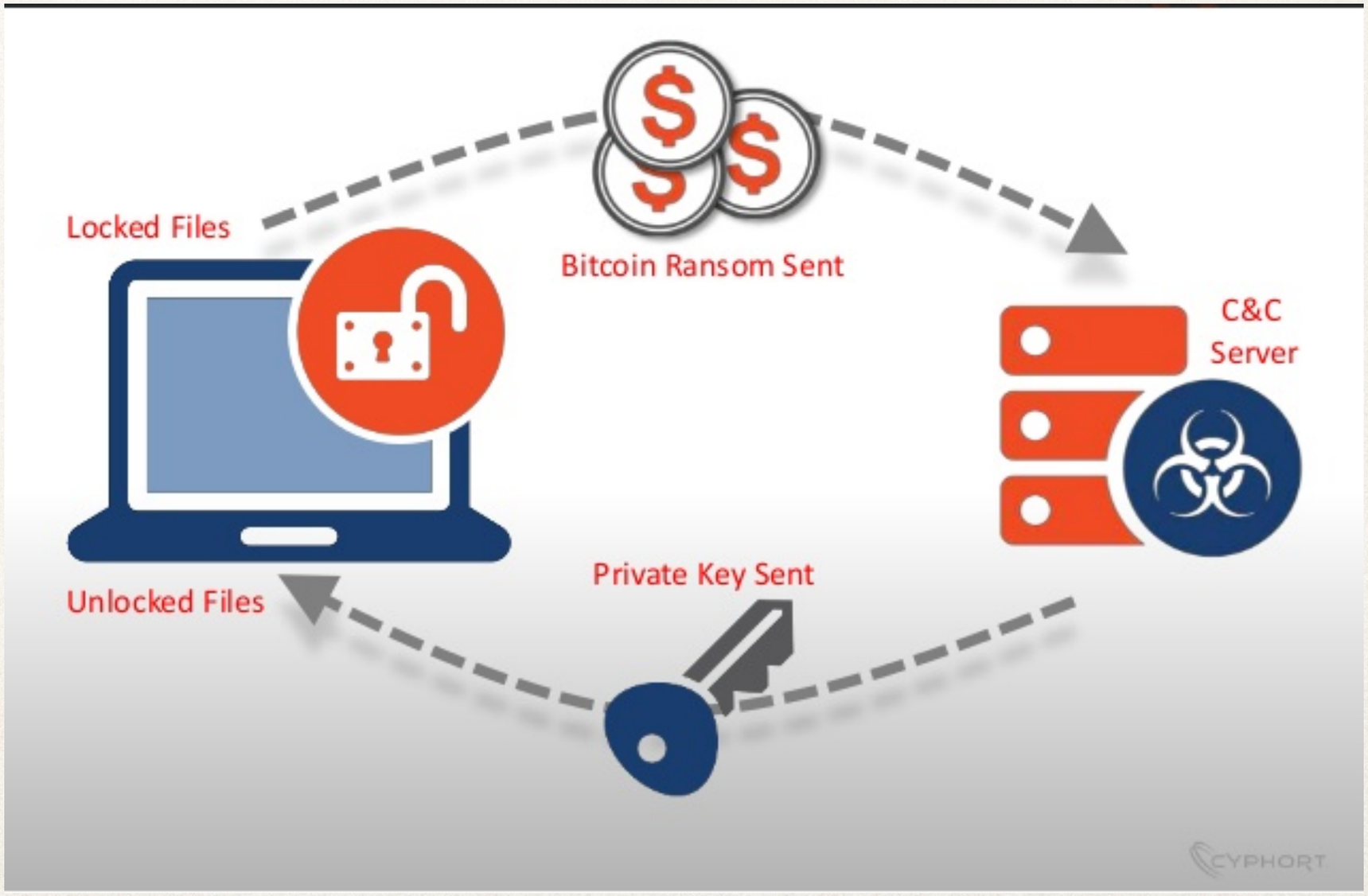
Detailed Alerting



Command & Control

Malicious Action

Defensive Mitigation
Ease of Deployment
Potential Monitoring
Detailed Alerting



Command & Control

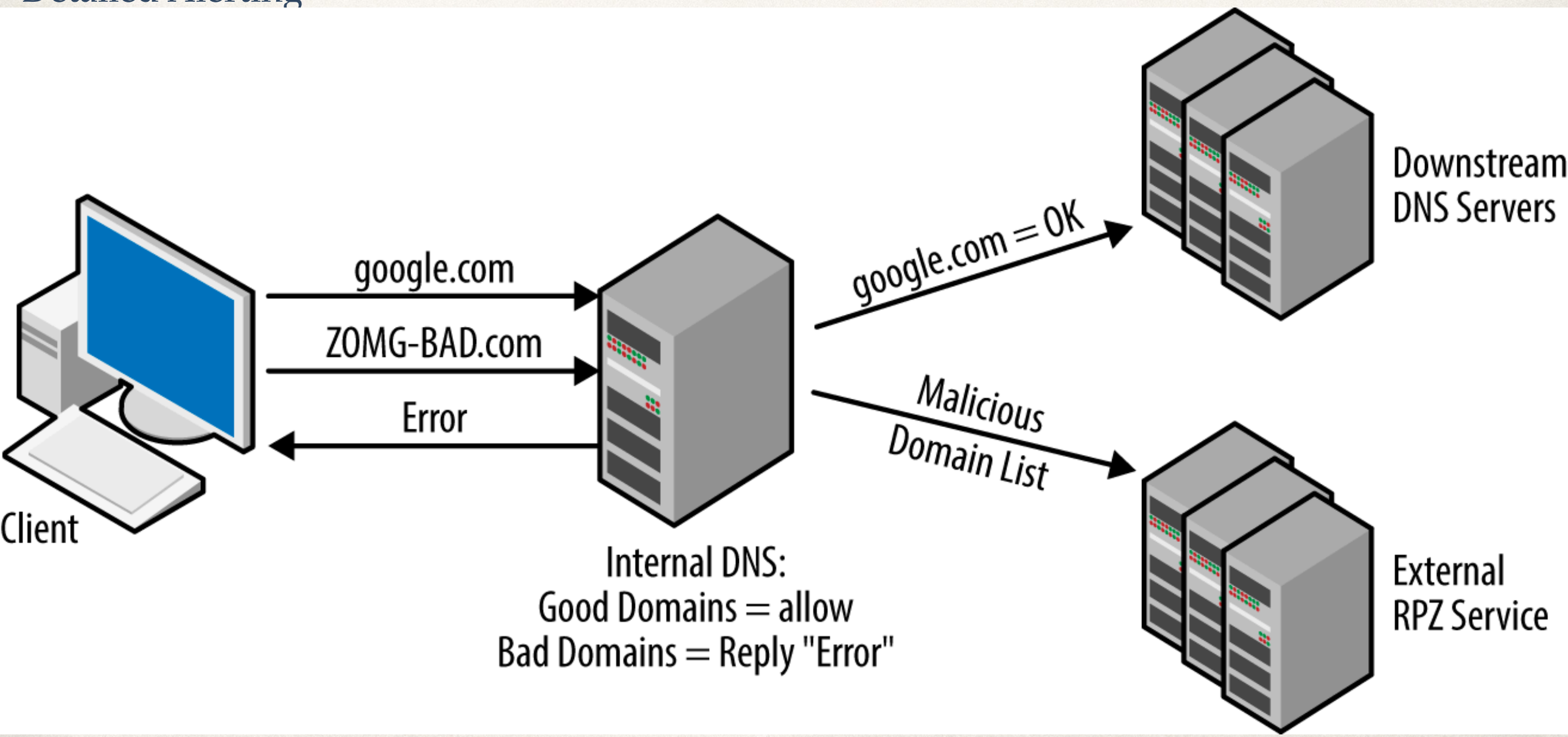
Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting



Command & Control

Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting

THREAT FEEDS

BOTS	MALWARE	OTHERS	PORT SCANNERS
bebloh C&C server	Malwaredomainlist	CI Army List	Port 110 Scanner
Cryptowall C&C server	Malwaredomains	Emergingthreats	Port 143 Scanner
Dyreza Servers	Threatexpert	Forum Spammers	Port 21 Scanner
Hesperbot C&C server		Malc0de Blacklist	Port 22 Scanner
matsnu C&C server		TLD Name Servers	Port 25 Scanner
Palevo C&C IP		Tor Exit Node ✓	Port 443 Scanner
qakbot C&C server			Port 80 Scanner
ramnit C&C server			Port 993 Scanner
Ransomdomains			Apache Web Server Scanner
Ransomips			Asterisk VoIP Scanner
Spyeye C&C server			Suspect Bots/Infected
Symmi C&C server			Bruteforce
TinyBanker C&C server			courier imap attacker
Upatr Servers			courier pop3 attacker
WebIron Bots			OpenBL FTP Scanners
Zeus C&C server			OpenBL HTTP Scanners
Zeus C&C server			OpenBL MAIL Scanners
			OpenBL SMTP Scanners
			OpenBL SSH Scanners

Command & Control

Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting

packets_20130913_020904.pcap [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: (ip.addr eq 127.0.0.2 and ip.addr eq 127.0.0.1) and (udp.port eq 2308 anc Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
31	145.489203	127.0.0.2	127.0.0.1	DNS	58	Standard query 0x02c9 A www.bing.com
723	218.013488	127.0.0.2	127.0.0.1	DNS	77	Standard query 0x0cfe A kvbqxktzlhyrolzmonqwcqheoov.net
583	202.891744	127.0.0.2	127.0.0.1	DNS	72	Standard query 0x13e4 A swijdmljofmrskeohzgjnnr.ru
351	178.726997	127.0.0.2	127.0.0.1	DNS	72	Standard query 0x17db A abmciduijgifuhqoknktw.info
1227	272.201407	127.0.0.2	127.0.0.1	DNS	77	Standard query 0x1a9e A upnkflbmkzmbpzhzxtrstdipjei.biz
555	199.867395	127.0.0.2	127.0.0.1	DNS	76	Standard query 0x1be9 A eahrkeuemlmzhainkjmbljyhon.net
751	221.037837	127.0.0.2	127.0.0.1	DNS	75	Standard query 0x1bf8 A qijdeqpkzhexyqctcuyxnjgeso.ru
485	192.306523	127.0.0.2	127.0.0.1	DNS	78	Standard query 0x1eed A vkgymfvshjbxohatgldamknydwpr.com
513	195.330872	127.0.0.2	127.0.0.1	DNS	78	Standard query 0x21ee A usfugqfbmmrskmfcywkaivvlrzpr.com
1423	293.231647	127.0.0.2	127.0.0.1	DNS	74	Standard query 0x2293 A aqwgqkukizoznzaufmyxprkmb.ru
1255	275.205727	127.0.0.2	127.0.0.1	DNS	70	Standard query 0x249f A xozammrhacmtlhiznfxkh.ru
863	233.115203	127.0.0.2	127.0.0.1	DNS	78	Standard query 0x26f0 A hyvxgusqscacqhycqwkrhmnrorp.info
625	207.428267	127.0.0.2	127.0.0.1	DNS	77	Standard query 0x28e0 A ojyhqpndraqbaqcpeapfzdtucgu.org
891	236.129538	127.0.0.2	127.0.0.1	DNS	76	Standard query 0x2af2 A ugrcusdibdqquuhehitwldrwbi.net
695	214.989139	127.0.0.2	127.0.0.1	DNS	76	Standard query 0x2efd A ivhpnjzlhutfedscxwvvovgaq.info
737	219.525663	127.0.0.2	127.0.0.1	DNS	77	Standard query 0x2fff A obzpjbrojfhxivskfmvgjnsonvv.biz
267	169.663965	127.0.0.2	127.0.0.1	DNS	76	Standard query 0x32de A gqeuibzfwsvwjzijinydlhylxg.net
457	189.282175	127.0.0.2	127.0.0.1	DNS	76	Standard query 0x35d3 A hbeiffydekzjbprwpscpeikbop.biz
1073	255.677647	127.0.0.2	127.0.0.1	DNS	76	Standard query 0x3787 A hygqpjusibxvhyvghhxccunjjb.com
989	246.664687	127.0.0.2	127.0.0.1	DNS	72	Standard query 0x3789 A vcithyrkdmbmdlbclvgexc.com
1171	266.192767	127.0.0.2	127.0.0.1	DNS	76	Standard query 0x3a9c A aqdeufircjvfejbtpzuovkdeazh.ru
231	166.649631	127.0.0.2	127.0.0.1	DNS	75	Standard query 0x3adc A xqficegmkvwoxkptmjcyrcxwqt.ru

Action & Objectives

Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting

Action & Objectives

Malicious Action

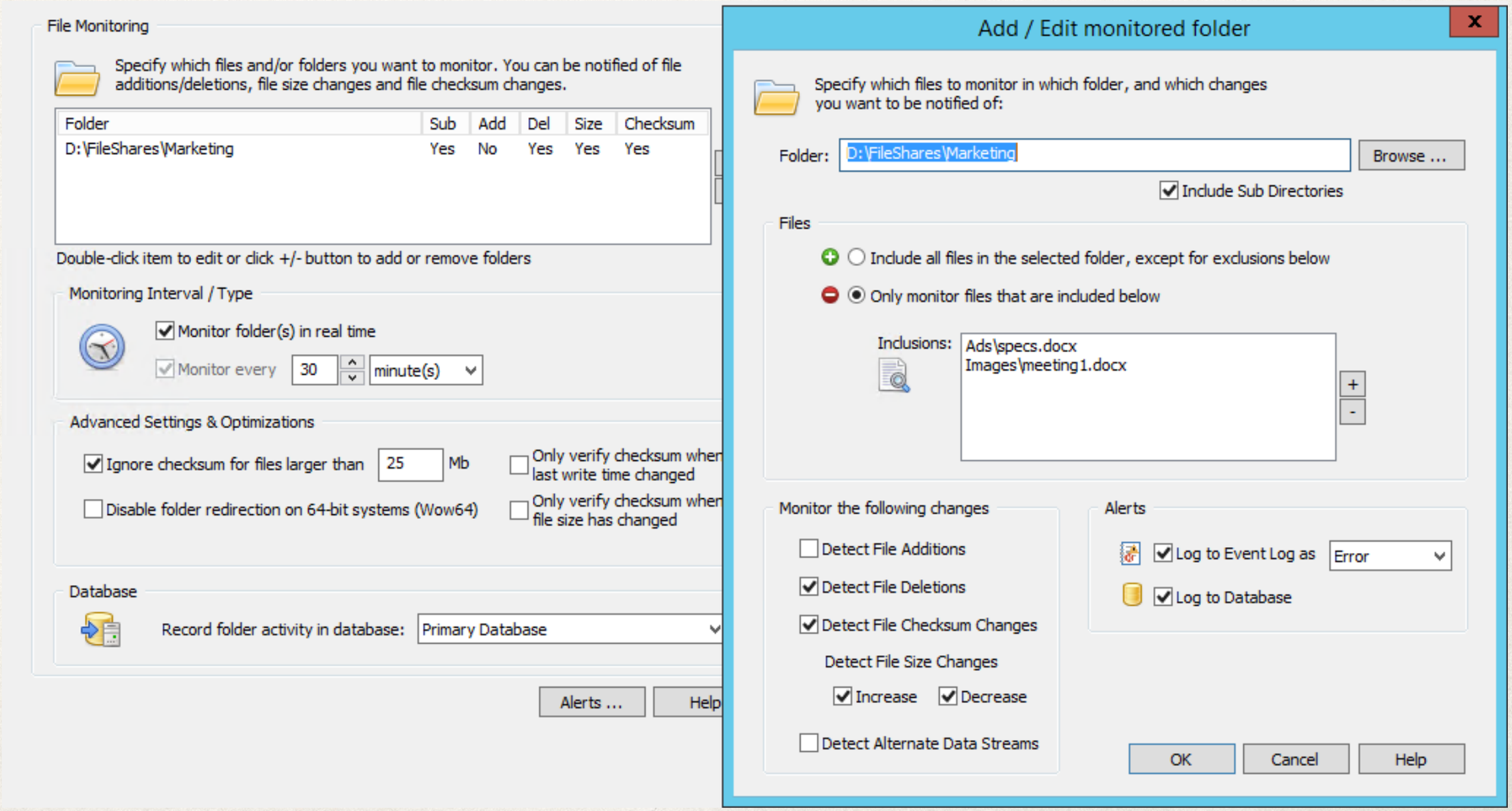
Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting

DEMO



Action & Objectives

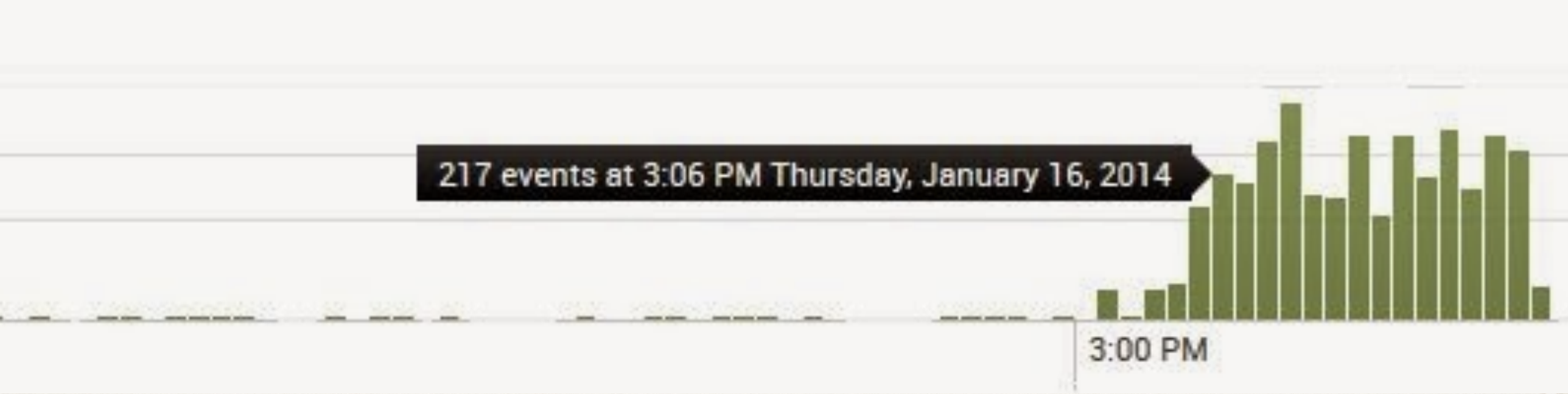
Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting



Theft, Loss, & Data Exfiltration

The Notorious DLP

Data Classification

—5 steps—

Identify Sources

Information Classes

Map Protections

Classify & Protect

Repeat

Map Data
—3 Types—

Data at Rest

Data in Motion

Data in Use

Implementation

Reconnaissance

Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting

Reconnaissance

Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting

```
node "c2950.domain.com" {

  Interface {
    duplex => auto,
    speed => auto
  }

  interface {
    "FastEthernet 0/1":
      description => "--> to end-user workstation",
      mode => access,
      native_vlan => 1000
  }
```

Reconnaissance

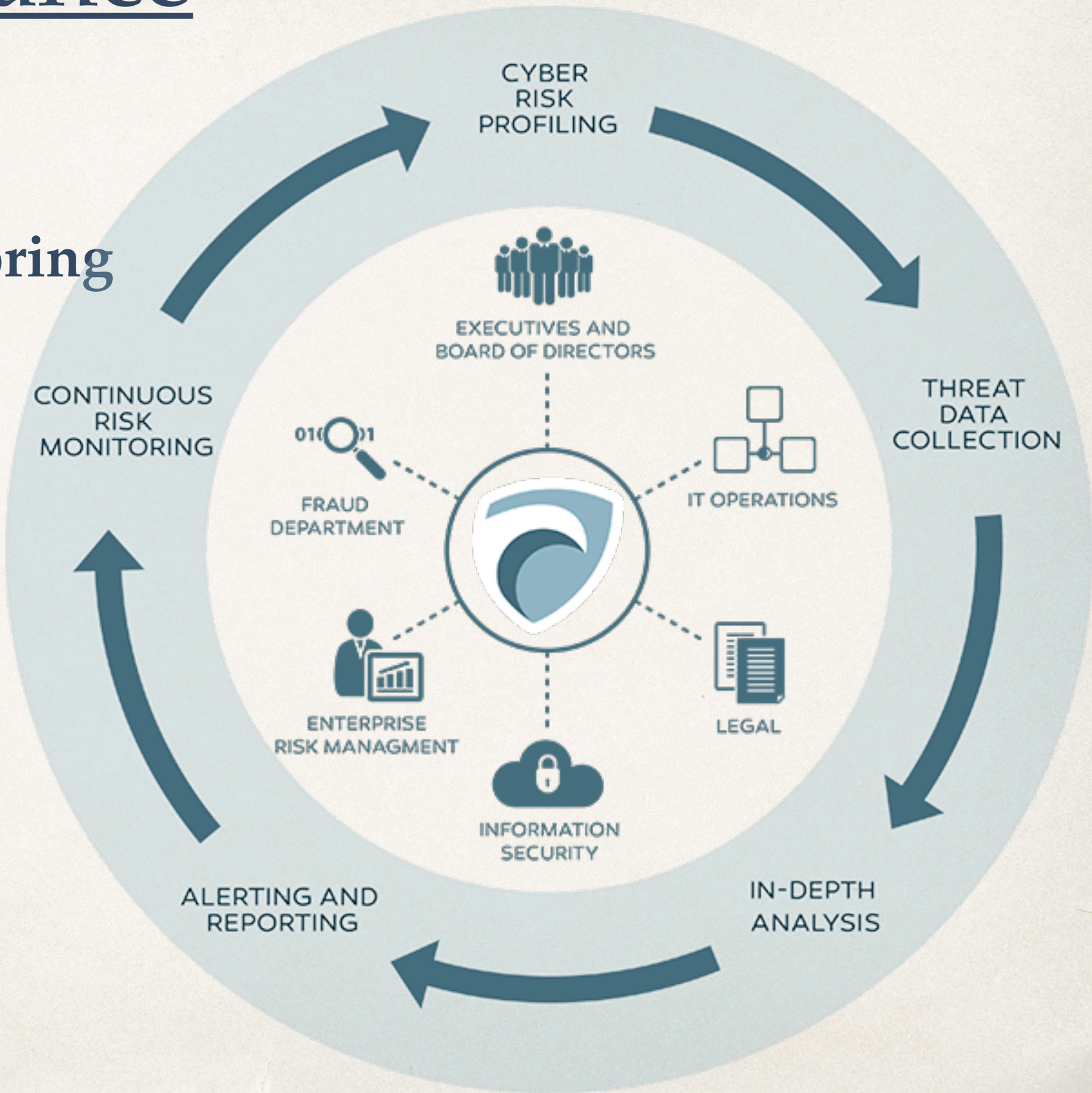
Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting



Reconnaissance

Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting

Exploitation

Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting

Exploitation

Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting

LastPass •••|
AUTHENTICATOR

Installation

Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting

Installation

Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting

Installation

Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting

Action & Objectives

Malicious Action

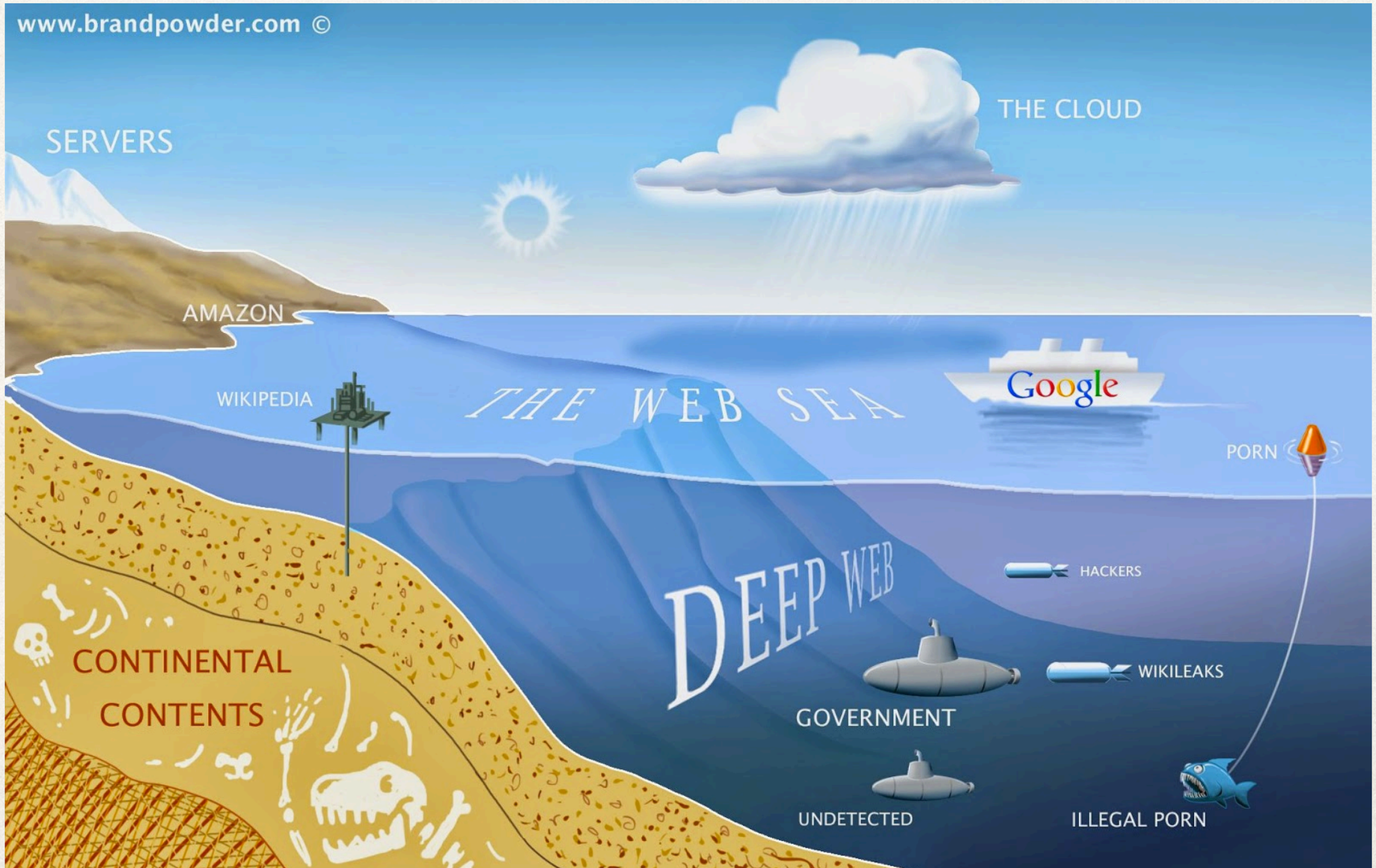
Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting

DEMO



Lateral Movement & Privilege Misuse

Reconnaissance

Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting

DEMO

Reconnaissance

Malicious Action

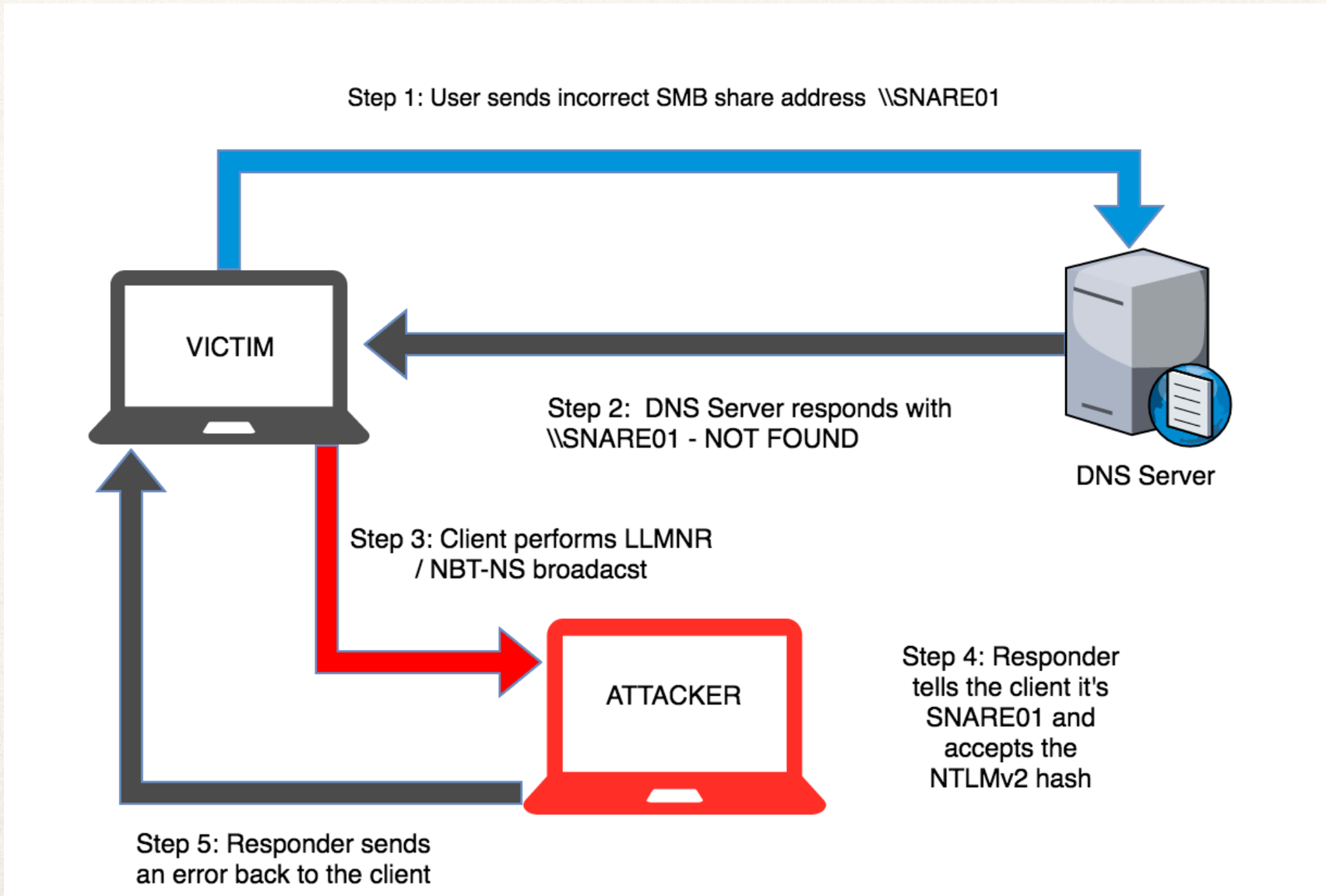
Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting

DEMO



Reconnaissance

Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting

DEMO

8 characters at only lowercase equals 26^8. Extremely easy, will crack in < 2 minutes.	baseball
8 characters at upper- and lowercase equals 52^8. Still not the best, will crack in < 6 hours.	Baseball
8 characters at uppercase, lowercase, and numbers equals 62^8. A little better, will crack in < 24 hours.	Bas3ball
10-character passphrase with uppercase, lowercase, numbers, and symbols 94^10. Approximately 600 years.	Base64b@ll

Reconnaissance

Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting

DEMO

Operational Number of events: 93

Level	Date and Time	Source	Event ID	Task Category
Information	9/7/2017 10:50:14 AM	PowerShell (Micros...	4103	Executing Pipeline
Information	9/7/2017 10:50:14 AM	PowerShell (Micros...	4103	Executing Pipeline
Information	9/7/2017 10:50:14 AM	PowerShell (Micros...	4103	Executing Pipeline
Information	9/7/2017 10:50:14 AM	PowerShell (Micros...	4103	Executing Pipeline
Information	9/7/2017 10:50:10 AM	PowerShell (Micros...	4103	Executing Pipeline
Information	9/7/2017 10:50:07 AM	PowerShell (Micros...	4103	Executing Pipeline
Information	9/7/2017 10:50:07 AM	PowerShell (Micros...	4103	Executing Pipeline
Information	9/7/2017 10:50:07 AM	PowerShell (Micros...	4103	Executing Pipeline
Information	9/7/2017 10:50:07 AM	PowerShell (Micros	4103	Executing Pipeline

Event 4103, PowerShell (Microsoft-Windows-PowerShell)

General | Details

```
ParameterBinding(Write-Verbose): name="Message"; value="Enumerated global catalog location: GC://"


Context:
        Severity = Informational
        Host Name = ConsoleHost
        Host Version = 4.0
        Host ID = 470eda8e-4f72-432c-8cbf-3d3a10f2d9de
        Engine Version = 4.0
        Runspace ID = b9e47a76-7718-4aca-b652-1ec7c88ae49d
        Pipeline ID = 30
        Command Name = Write-Verbose
        Command Type = Cmdlet
        Script Name = C:\Users\Administrator\Downloads\BloodHound-master\BloodHound-master\PowerShell\BloodHound.ps1
        Command Path =
        Sequence Number = 150
        User = WIN-I2RGFJQ3QJU\Administrator
        Shell ID = Microsoft.PowerShell
```

Weaponization

Malicious Action

Defensive Mitigation
Ease of Deployment
Potential Monitoring
Detailed Alerting

Exploitation

Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting

Exploitation

Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting

DEMO

Testing & Proof of Concept


HITACHI
DEWALT
18V XR LI-ION
Makita


Natural
Cherry
Mahogany
Walnut

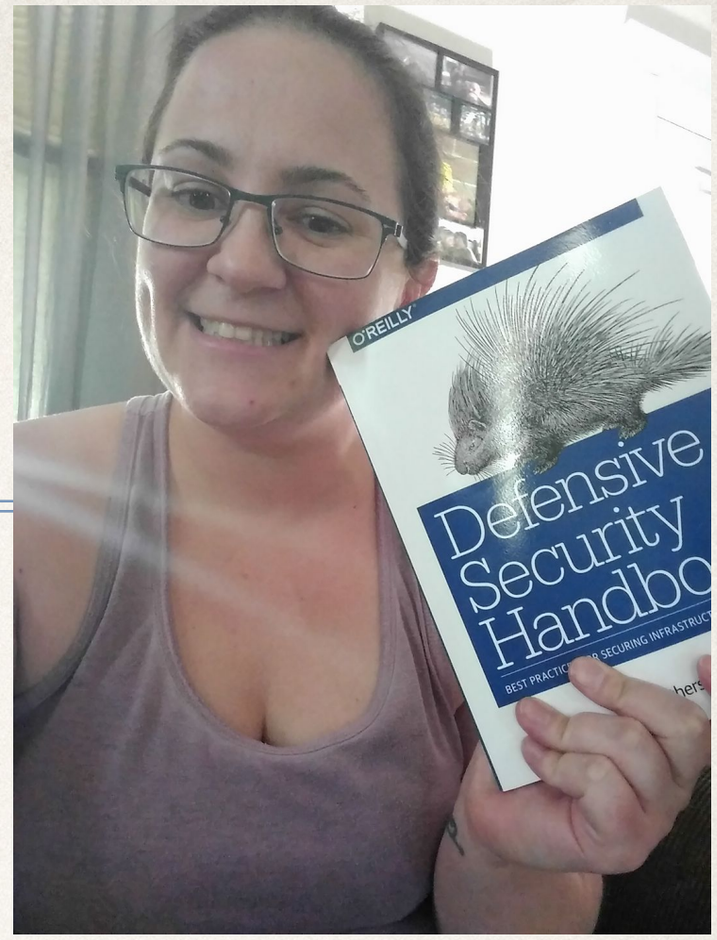
What to include in the tabletop:

- A handout to participants with the scenario and room for notes.
- Current runbook of how security situations are handled.
- Any policy and procedure manuals.
- List of tools and external services.

Post-exercise actions and questions:

- What went well?
- What could have gone better?
- Are any services or processes missing that would have improved resolution time or accuracy?
- Are any steps unneeded or irrelevant?
- Identify and document issues for corrective action.
- Change the plan appropriately for next time.

Me



- Amanda Berlin
- @Infosystir
- Co-Author of “Defensive Security Handbook”
- Co-host on the Brakeing Down Security podcast
- Blogger
- Mom of 3 kick ass boys
- Lover of unicorns and lock picking

- https://www.fireeye.com/blog/threat-research/2016/06/automatically-extracting-obfuscated-strings.html
- http://hackerhurricane.blogspot.com/2016/09/avoiding-ransomware-with-built-in-basic.html
- https://isc.sans.edu/threatfeed.html
- https://www.eventsentry.com/blog/2015/11/trapping-cryptolockercryptowall-with-honey.html
- https://www.sans.org/reading-room/whitepapers/dns/detecting-dns-tunneling-34152
- http://www.freeforensics.org/2016/03/proactively-reacting-to-ransomware.html
- https://blogs.technet.microsoft.com/secguide/2014/09/02/blocking-remote-use-of-local-accounts/
- https://attack.mitre.org/wiki/Main_Page