SLAIT Consulting

Maryland Education Enterprise Consortium - 2017

INNOVATIVE SOLUTIONS FOR
FORWARD THINKING COMPANIES

About SLAIT

SLAIT is an Information Technology Consulting Services Company specializing in delivering customized IT Services and Solutions to clients in the Commercial, State\Local Government and Education sectors.

- Serving clients for over 26 years
- $100M revenue
- 350+ Resources
- Headquartered in Virginia Beach, VA with regional offices in:
  - Richmond, VA
  - Greenbelt, MD
  - Charlotte, NC
  - Raleigh, NC

Innovative Solutions for Forward Thinking Companies

Some of SLAIT's Technology Partners

paloalto NETWORKS
the network security company™

NetApp®
Star Partner
Professional Services and Support Services Certified

PURESTORAGE

peak 10™
DATA CENTER SOLUTIONS

CISCO™ PARTNER
Premier Certified

COMMVAULT®

Quantum®

citrix® partner
Solution Advisor

Microsoft®
GOLD CERTIFIED
Partner

FORTINET®

vmware® PARTNER
ENTERPRISE SOLUTION PROVIDER

Infoblox®

riverbed®

aruba
a Hewlett Packard Enterprise company

Blue Coat

IBM

NUTANIX.

CARBON BLACK
ARM YOUR ENDPOINTS

splunk>

DELL

FireEye®

nimble storage

REDSEAL

Aerohive®

veeam
IT JUST WORKS!™

JUNIPer NETWORKS
ELITE PARTNER
ENTERPRISE SOLUTION PROVIDER

VARONIS

QTS
Data Centers without Compromise®

EXAGRID™

COMMVAULT®

EQUINIX

hp® invent

f5®

symantec™

Tintri

SLAIT Consulting

SLAITCONSULTING.com

SLAIT Consulting

Ransomware – Your Data Held Hostage

SLAIT Consulting

Ransomware By the numbers

- Prior to attack 4 out of 5 organizations are confident backup can provide them complete recovery
  - Less than half of victims fully recover their data
- Email is the #1 delivery vehicle for ransomware
- Nearly two-thirds of exploit kits have ransomware payloads
  - Ransomware is the most popular payload
- 600% growth in new ransomware families in 2016
- 4x jump in Android ransomware
- 230% percent jump in JavaScript ransomware payloads

"In my day, kids didn't build massive, ransomware-spewing botnets. They got a paper route."

brianmooredraws.com

Big Business

Business Model

- Very skilled groups maintain and sell exploit kits
  - Maintain list of exploits including zero-day exploits
  - Package the ability to automatically identify vulnerabilities and deliver payload of your choice
- Ransomware groups use EK to deploy their variant
- Ransomware as a service – Some ransomware groups even subcontract their combined package for a share of the profits

Profits

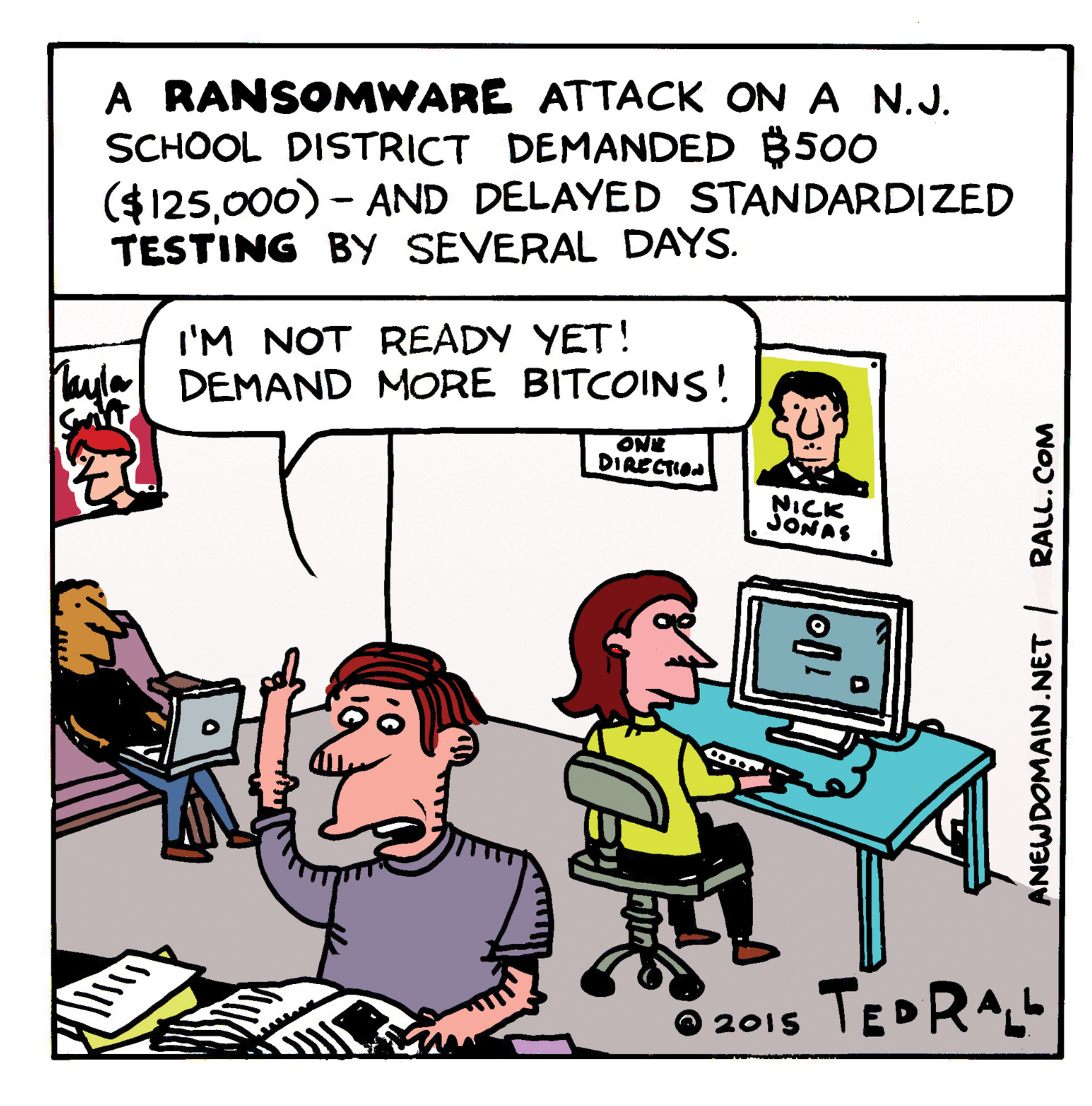
- 209 million paid to cyber criminals in Q1 - 2016
- Angler Exploit Kit
  - $60 million per year
- Cryptowall 3 – $321 million per year
- Locky – 90,000 victims per day
  - Research indicates around 2.9% of victims pay the ransom of between .5 and 1 bitcoin ($450). This works out to between $200-$400 million dollars a year

"In my day, kids didn't build massive, ransomware-spewing botnets. They got a paper route."

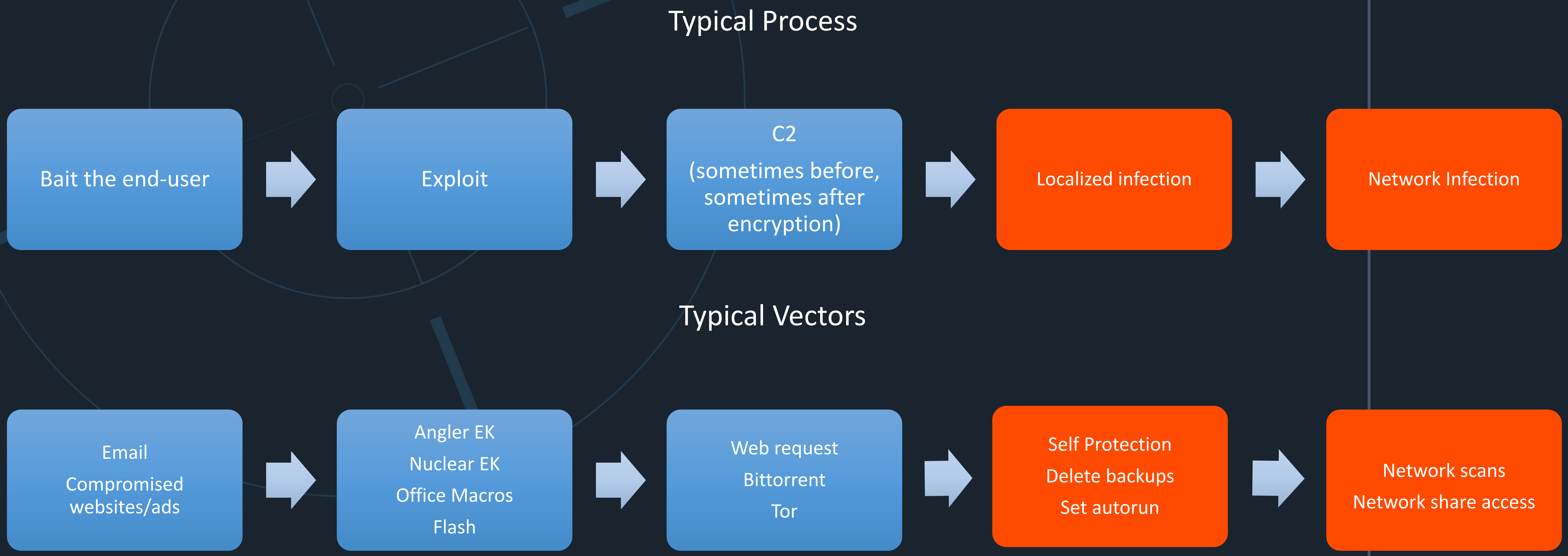
brianmooredraws.com

Evolutionary Capitalism

- Every ransom paid is an investment in the R&D process of the ransomware economy
- Threat groups track what methods are successful and what methods are not
- Threat groups also track the success of competitors, copying and avoiding as appropriate
- Continual process whereby unsuccessful methods die-off and successful methods proliferate
- Expect future ransomware to
  - Be more automated with a greater prevalence of self-propagation
  - Have an increased focus on lateral movement and reducing C2 dependency
    - Encrypt what C2 is necessary
  - Include time delay features to inhibit data restore options


A RANSOMWARE ATTACK ON A N.J. SCHOOL DISTRICT DEMANDED ₿500 ($125,000) – AND DELAYED STANDARDIZED TESTING BY SEVERAL DAYS.
I'M NOT READY YET! DEMAND MORE BITCOINS!
Tayla Swift
ONE DIRECTION
NICK JONAS
ANEWDOMAIN.NET / RALL.COM
© 2015 TED RALL

Ransom Family Commonalities (AKA Kill Chain)



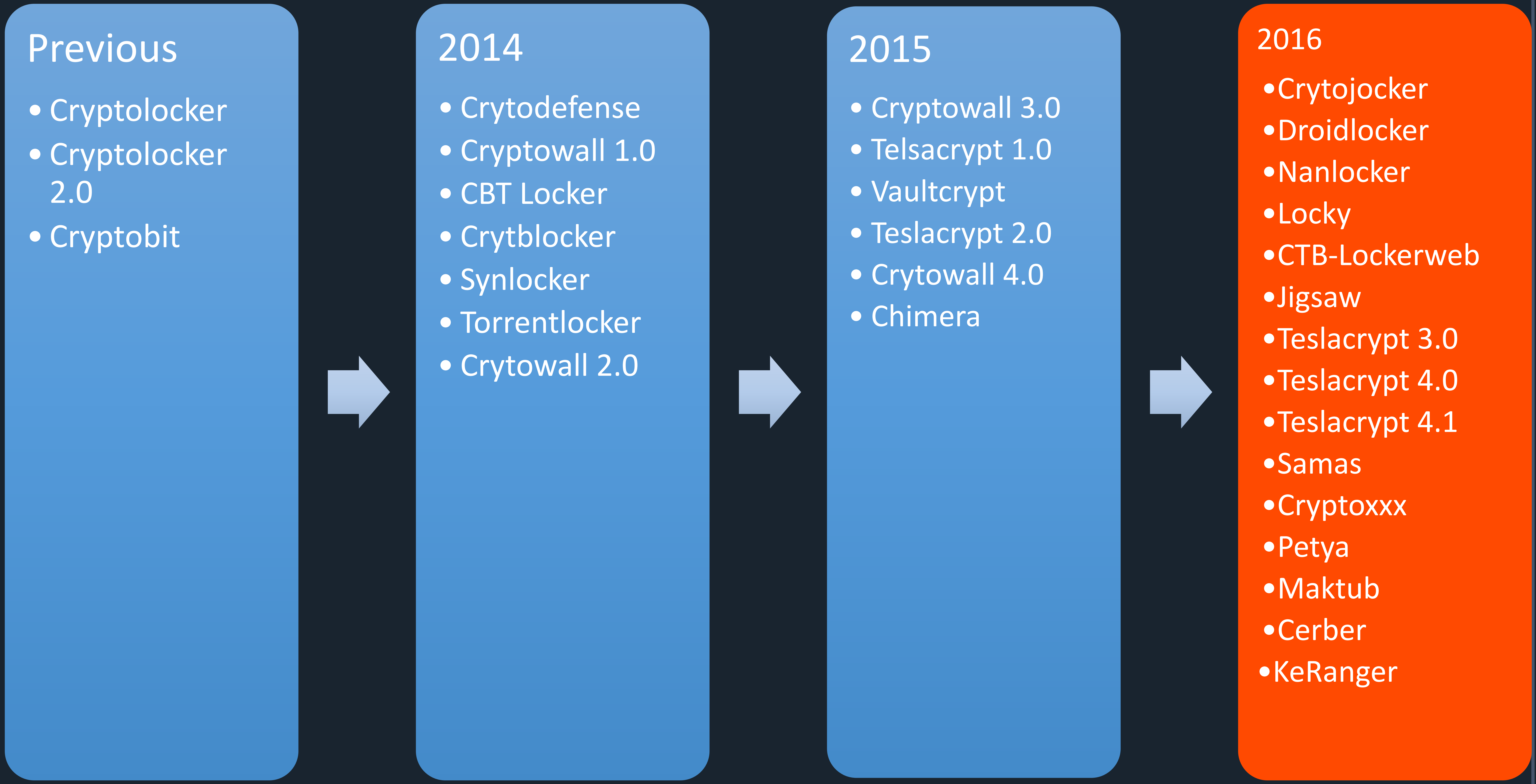
Typical Process

Bait the end-user → Exploit → C2 (sometimes before, sometimes after encryption) → Localized infection → Network Infection

Typical Vectors

Email
Compromised websites/ads → Angler EK
Nuclear EK
Office Macros
Flash → Web request
Bittorrent
Tor → Self Protection
Delete backups
Set autorun → Network scans
Network share access

Evolution of Ransomware



Previous

- Cryptolocker
- Cryptolocker 2.0
- Cryptobit

2014

- Crytodefense
- Cryptowall 1.0
- CBT Locker
- Crytblocker
- Synlocker
- Torrentlocker
- Crytowall 2.0

2015

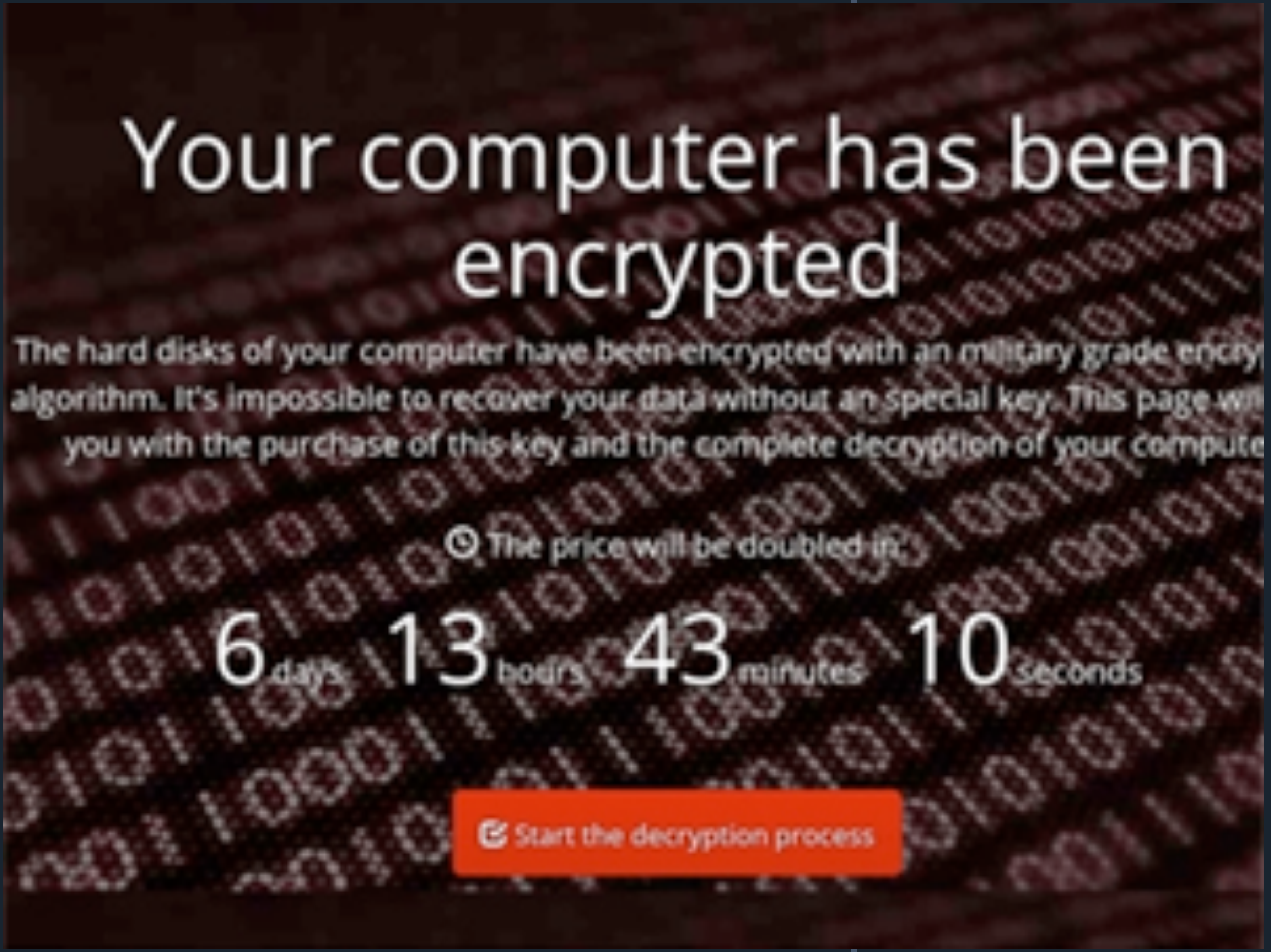
- Cryptowall 3.0
- Telsacrypt 1.0
- Vaultcrypt
- Teslacrypt 2.0
- Crytowall 4.0
- Chimera

2016

- Crytojocker
- Droidlocker
- Nanlocker
- Locky
- CTB-Lockerweb
- Jigsaw
- Teslacrypt 3.0
- Teslacrypt 4.0
- Teslacrypt 4.1
- Samas
- Cryptoxxx
- Petya
- Maktub
- Cerber
- KeRanger

Trending

- Increase in targeted attacks against
  - → Healthcare organizations
  - → Law firms
  - → Payment processing firms
- Attacker seeking soft targets with high impact
- Critical systems/data → expectation higher payout
- Payment per infected system
- Ransomware seeking local backups
- Exploit expanded attack surface
- Encryption of MBR
- Change in delivery methodology attacking previously compromised systems
- Drops bootloader then crashes system to force reboot – encrypts upon reboot



Your computer has been encrypted

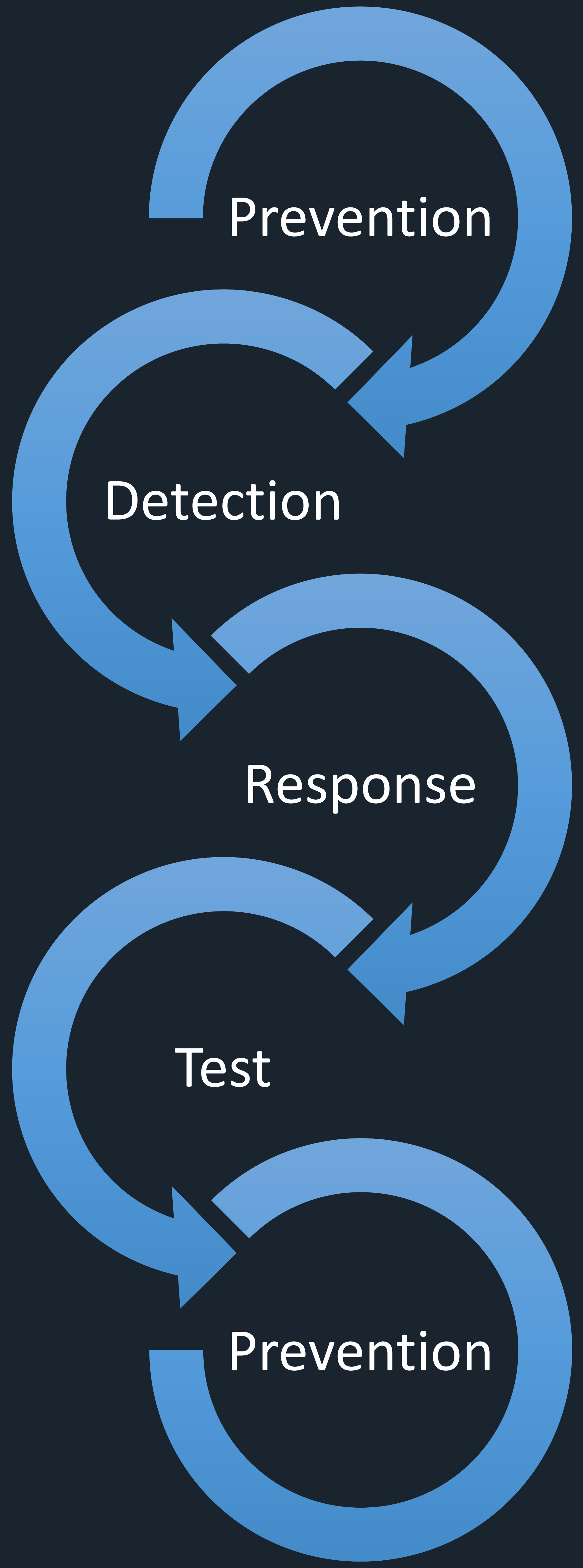
The hard disks of your computer have been encrypted with an military grade encry
algorithm. It's impossible to recover your data without an special key. This page wi
you with the purchase of this key and the complete decryption of your compute

The price will be doubled in:

6 days 13 hours 43 minutes 10 seconds

What the future holds - Predictions

- More platforms targeted
  - All flavors of windows and Android exist
  - Targeted OSX attacks - 2016
- Higher ransoms – success begets success
- MORE targeted attacks – Seeking critical networks
- Internet of Things = Significant expansion of attach surface



What to do

Email Gateway Filtering

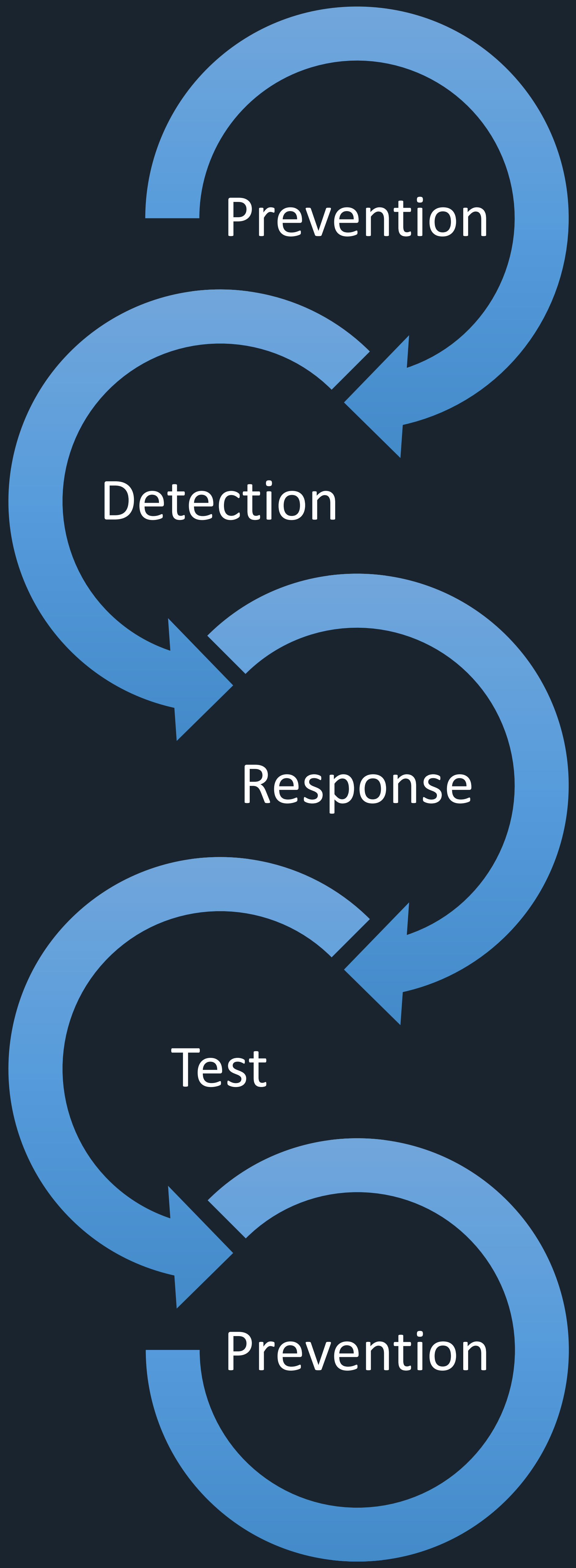
- .exe, .bat, .ps1, .js, .jse, .scr, .com, .osx, .jar, .vb, .vbs, .bas, .ws, .wsf, .shs, .pif, .hta, lnk
  - .doc, .xls, .rft

Domain group policies

- Block macros
  - Open downloaded documents in “protected view”
  - Open downloaded documents and block all macros
- Restrict program execution
  - Disable execution from temporary and/or user data folders
- Disable Windows Script Host
- Show file extensions
  - (****.PDF.EXE)

Restrict access to network shares

Maintain excellent backup practices



SLAIT Consulting

What to do

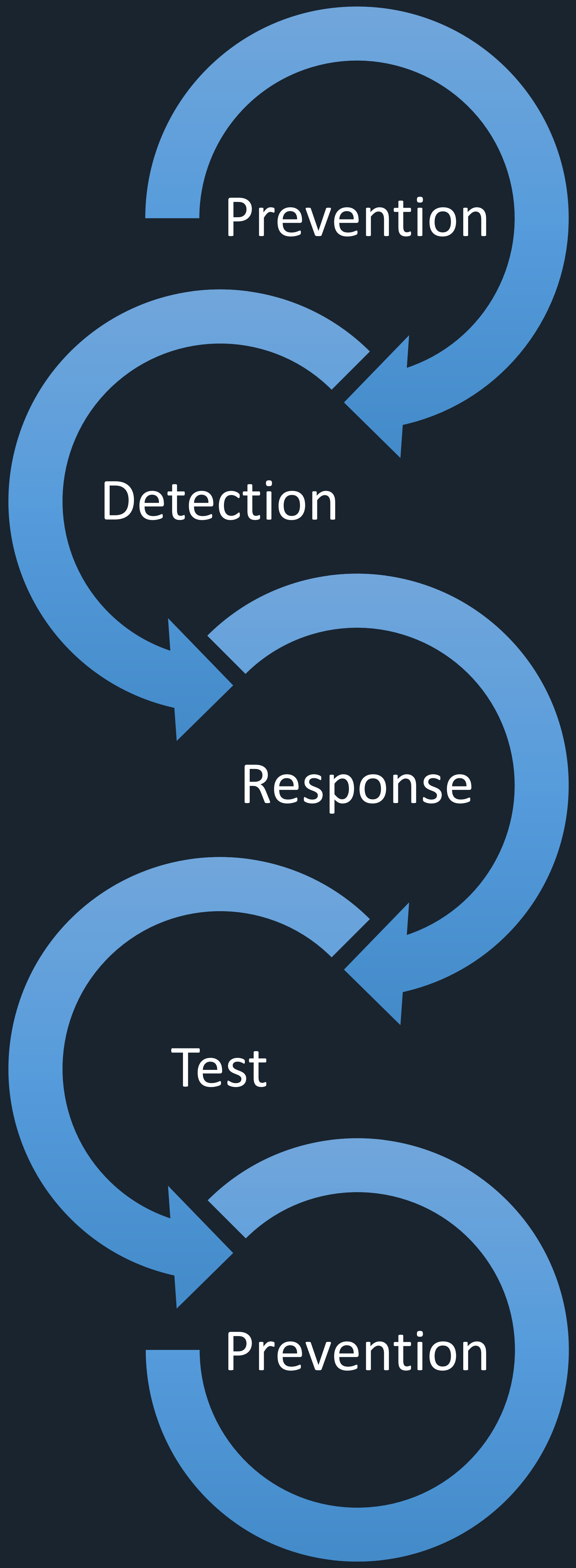
Maximize visibility

- Effective security at the perimeter
- Effective security at the endpoint

Increased user awareness

Resources

- ID Ransomware: Ransomware identification:
  - https://id-ransomware.malwarehunterteam.com/
- Anti-Petya Live CD
  - https://hshrzd.wordpress.com/2016/20/anti-peyta-live-cd-the -fastest-stage1-key-decoder/
- No Ransom: Decryptors for CoinVault, CrytXXX, etc.
  - https://noransom.kaspersky.com
- Ransomware overview: Ransomware IOCs
  - https://goo.gl/SfU0hv
  - https://docs.google.com/spreadsheets/d/1TWS238xacAto-fLKh1n5uTsdijWdCEsGIM0Y0Hvmc5g/htmlview?pli=1



Prevention

Detection

Response

Test

Prevention

Six Security Pillars in the SLAIT ThreatManage USM Platform

SLAIT ThreatManage USM

SIEM & LOG MANAGEMENT

- Log Collection & Correlation
- OTX Threat Data
- SIEM Event Correlation
- Incident Response

BEHAVIORAL MONITORING

- Network IDS
- Netflow Analysis
- Full Packet Capture
- ThreatCloud Integration

ENDPOINT RESPONSE

- “Flight Data Recorder”
- Live Response
- Threat Actor Detection/Remediation

SLAIT
24x7 Security
Operations
Center

ASSET DISCOVERY & INVENTORY

- Active Network Scanning
- Passive Network Scanning
- Asset Inventory
- Software Inventory

VULNERABILITY ASSESSMENT

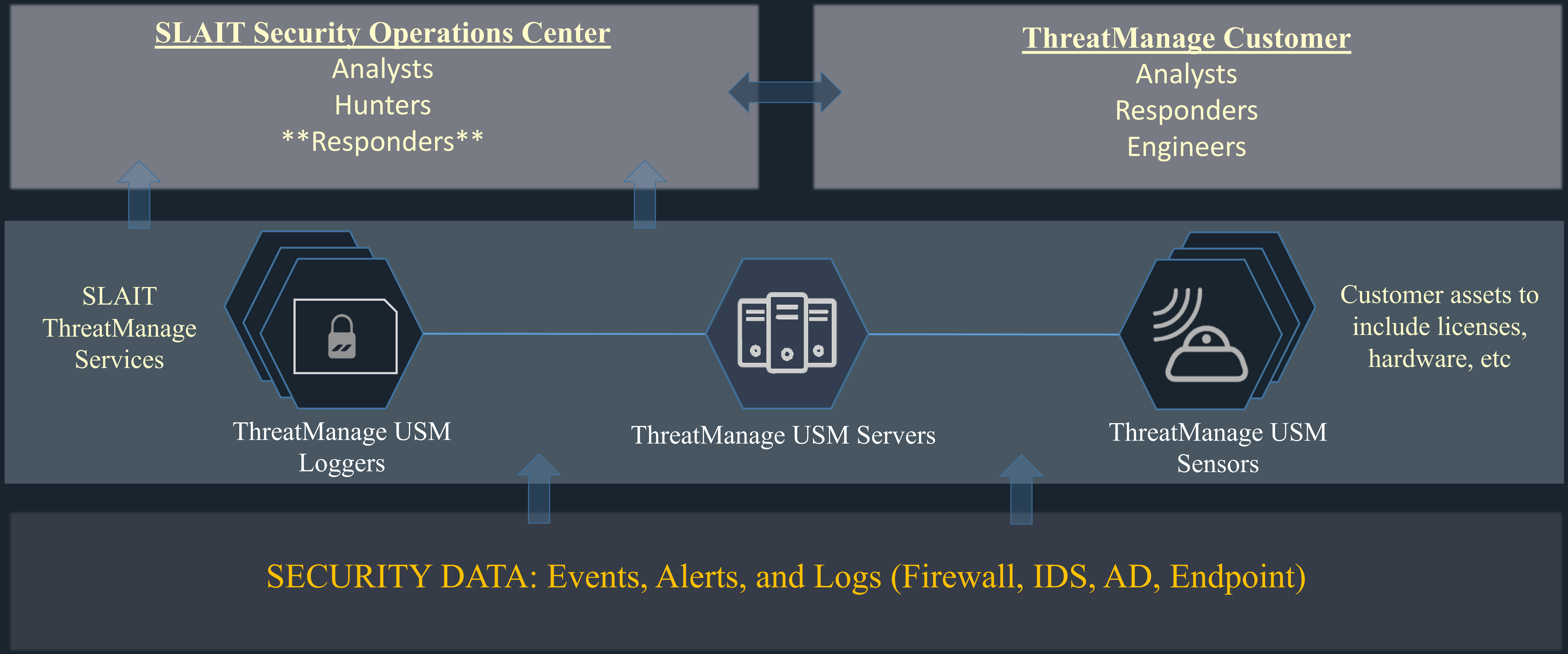
- Continuous Vulnerability Monitoring
- Authenticated & Unauthenticated Active Scanning

ADVANCED THREAT DETECTION

- Adaptive Threat Fabric
- Behavioral Analysis
- Dynamic Sandbox Analysis

Unified Security Management Framework

SLAIT ThreatManage USM



SLAIT Security Operations Center

Analysts

Hunters

Responders

ThreatManage Customer

Analysts

Responders

Engineers

SLAIT ThreatManage Services

ThreatManage USM Loggers

ThreatManage USM Servers

ThreatManage USM Sensors

Customer assets to include licenses, hardware, etc

SECURITY DATA: Events, Alerts, and Logs (Firewall, IDS, AD, Endpoint)

Center for Internet Security (CIS)

- SANS – CIS top 20 Critical Security Controls (CSC)

1) Inventory of authorized and unauthorized devices
2) Inventory of authorized and unauthorized software
3) Secure configurations for hardware and software on mobile devices, laptops, workstations and servers
4) Continuous vulnerability monitoring
5) Controlled use of administrative privileges
6) Maintenance, monitoring and analysis of audit logs
7) Email and Web Browser protection
8) Malware defense
9) Limitation and control of network ports, protocols, and services
10) Data recovery capability
11) Secure configurations for network devices such as firewalls, routers and switches
12) Boundary devices
13) Data protection
14) Controlled access based on need to know
15) Wireless access control
16) Account monitoring and control
17) Security skills and assessment and appropriate training to fill gaps
18) Application software security
19) Incident response and management
20) Penetration tests and Red team exercises

And when all else fail…Restore

- Implement frequent backups – Limit data lost by ensuring a recent restore point
- Limit access to these backups – A sufficiently advanced attacker could seek to eliminate the backups themselves

Innovative Solutions for Forward Thinking Companies

SLAIT Consulting

Arnold E. Bell - CISO
Arnold.Bell@slaitonsulting.com
6304 Ivy Lane, Greenbelt MD   T: (301) 987-1293 | (800) 761-6898
slaitconsulting.com

Follow Us On Our Social Sites

LinkedIn: slait.it/linkedinslait

Twitter: @slaitconsulting

Facebook: SLAITConsulting