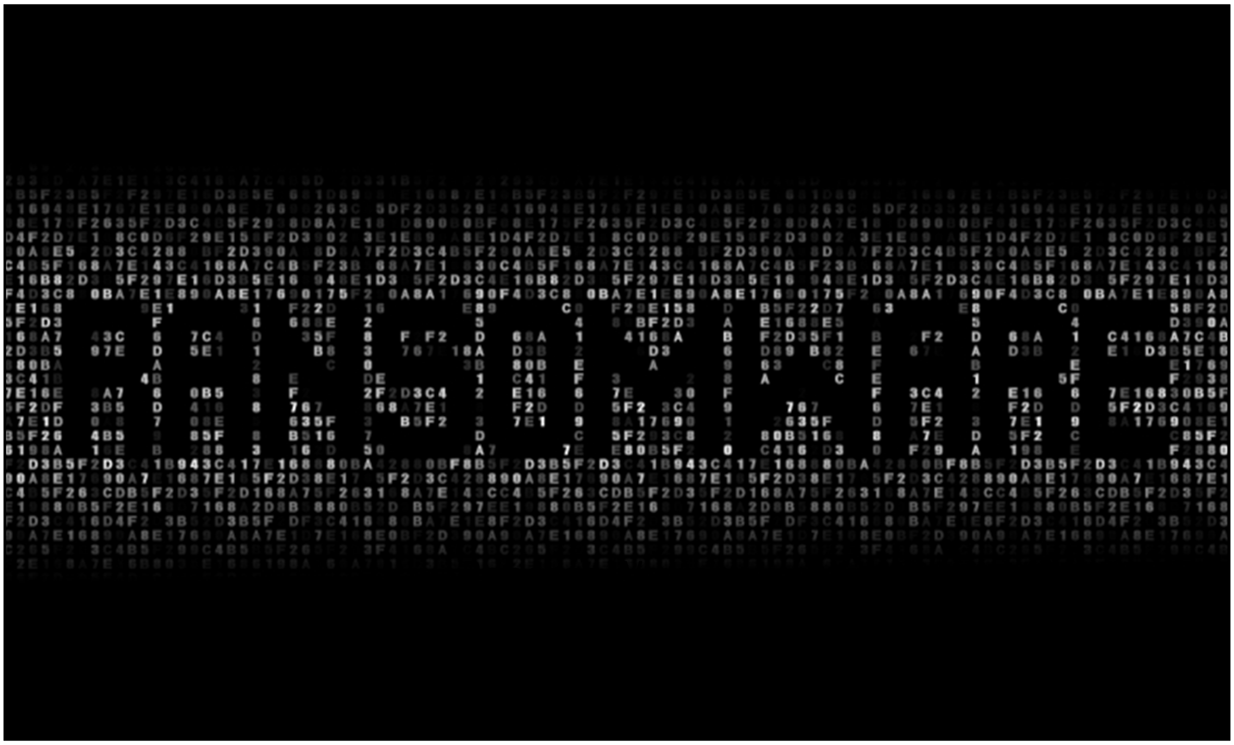


Discussion Points

- Health IT
- Security In Healthcare
- Ransomware
- Breach Risk Maturity
- Discussion

Delivery of Care Has Transformed

MORE TECHNOLOGY

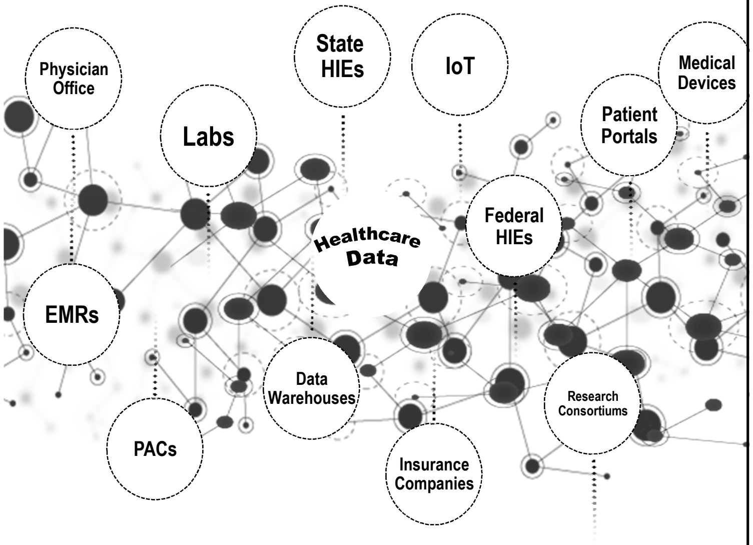
ENHANCED ACCESS

HIGHER AVAILABILITY

…YET HEALTHCARE IS STILL NOT SECURE

Provider / Patient Infrastructure

- Family physician / PCP / GP
- Specialist clinic
- Blood Lab
- X-Ray / Cat Scan provider
- Local hospital
- Rehab facility after hospital discharge
- Online patient portals
- Insurance company (payer)
- Health Information Exchanges
- EMR-to-like-EMR integration
- Data Warehouse(s)
- Data push to patients & other providers
- Push to the State, research consortiums
- Data push of lab results to providers
- Data pull from EMRs for visiting patients (Patient Portals)
- IoT
- Medical Devices

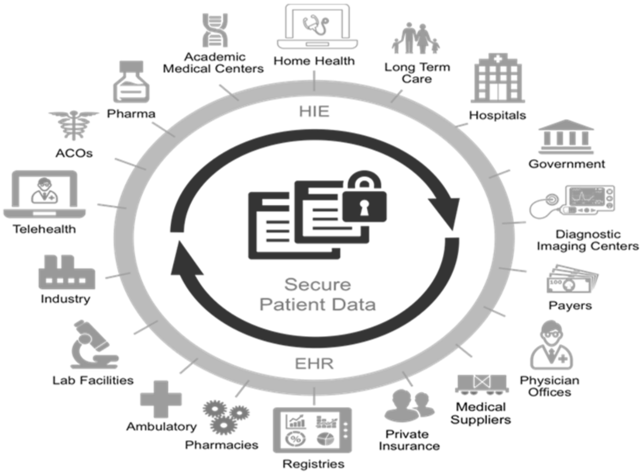


* Doug Copley data from SecureWorld 2014

Transformed Care is a Hotbed for CyberSecurity

- Digitizing patient record
- Sharing patient across HLS ecosystem
- Data-based collaborative care
- Analytics to enhance care
- Electronic registries for population health
- Personalized medicine

DATA EXPLOSION
Unprecedented Security Risk



“

WHAT THREAT VECTOR IS MOST CONCERNING TO YOU AND WHY.

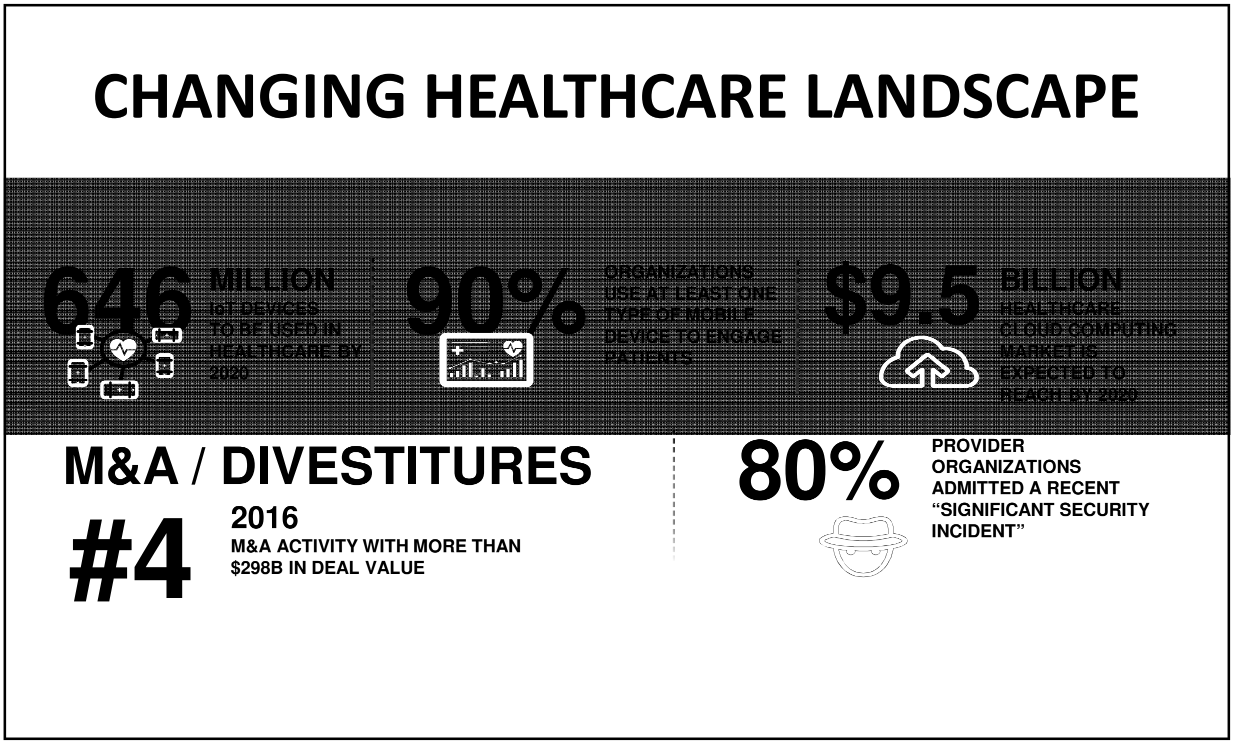
”

The Next Battleground

Mobile applications
Wearables
Remote health monitoring
Virtual care

THE NEXT THREAT

Forrester Research 2016 Cybersecurity Report – #1 prediction will be ransomware for medical devices or wearables



CHANGING HEALTHCARE LANDSCAPE

646 MILLION IoT DEVICES TO BE USED IN HEALTHCARE BY 2020

90% ORGANIZATIONS USE AT LEAST ONE TYPE OF MOBILE DEVICE TO ENGAGE PATIENTS

$9.5 BILLION HEALTHCARE CLOUD COMPUTING MARKET IS EXPECTED TO REACH BY 2020

M&A / DIVESTITURES

#4 **2016** M&A ACTIVITY WITH MORE THAN $298B IN DEAL VALUE

80% PROVIDER ORGANIZATIONS ADMITTED A RECENT “SIGNIFICANT SECURITY INCIDENT”

“

HAVE WE BEEN **HACKED**?

”

SECURITY INCIDENTS AND BREACHES

329 2016 & 51 2017 REPORTED BREACHES OF 500 OR MORE AFFECTED

16.6MM INDIVIDUALS AFFECTED
425K INDIVIDUALS AFFECTED

OVER $20MM IN FINES IN 2016

OVER $11MM IN FINES IN 2017

BREACH TYPE	AFFECTED ENTITIES	
	2016	2017
HACKING/ IT INCIDENT	113	14
IMPROPER DISPOSAL	7	2
LOST	16	4
THEFT	62	10
UNAUTHORIZED ACCESS/DISCLOSURE	130	21
TYPE NOT DISCLOSED	1	
TOTAL	329	51
BA	20	3
HEALTH PLAN	51	8
HEALTHCARE PROVIDER	256	40
NOT SPECIFIED	2	0
TOTAL	329	51

Source: U.S. Department of Health and Human Services
Office for Civil Rights Breach Portal
https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Notable Breaches in 2016

	REPORTED	AFFECTED INDIVIDUALS	CAUSE
Banner Health®	8/3/16	3,620,000	HACKING/ IT INCIDENT
newkirk® Communication Innovation	8/9/16	3,466,120	HACKING/ IT INCIDENT
21st Century Oncology	3/4/16	2,213,597	HACKING/ IT INCIDENT
VALLEY ANESTHESIOLOGY CONSULTANTS	8/12/16	882,590	HACKING/ IT INCIDENT
Health Services LOS ANGELES COUNTY	12/16/16	749,017	HACKING/ IT INCIDENT
BON SECOURS HEALTH SYSTEM	8/12/16	651,971	UNAUTHORIZED ACCESS/ DISCLOSURE
PEACHTREE ORTHOPAEDIC CLINIC	11/18/16	531,000	HACKING/ IT INCIDENT
Radiology Regional Center radiologyregional.com	2/12/16	483,063	LOSS
CALIFORNIA CORRECTIONAL HEALTH CARE SERVICES	5/15/16	400,000	THEFT
COMMUNITY HEALTH PLAN of Washington™	12/21/16	381,504	HACKING/ IT INCIDENT

14 Ransomware Incidents

BECKER'S HEALTH IT & CIO REVIEW

Hospitals are hit with 88% of all ransomware attacks

TRMC TITUS REGIONAL MEDICAL CENTER Our Passion. Our Promise. Your Care.

HOLLYWOOD PRESBYTERIAN MEDICAL CENTER

Lukaskrankenhaus GmbH

COUNTY OF LOS ANGELES Public Health

The Ottawa Hospital L'Hôpital d'Ottawa

DEKALB HEALTH Promote. Preserve. Restore.

Kansas Heart HOSPITAL

Keck Medicine of USC

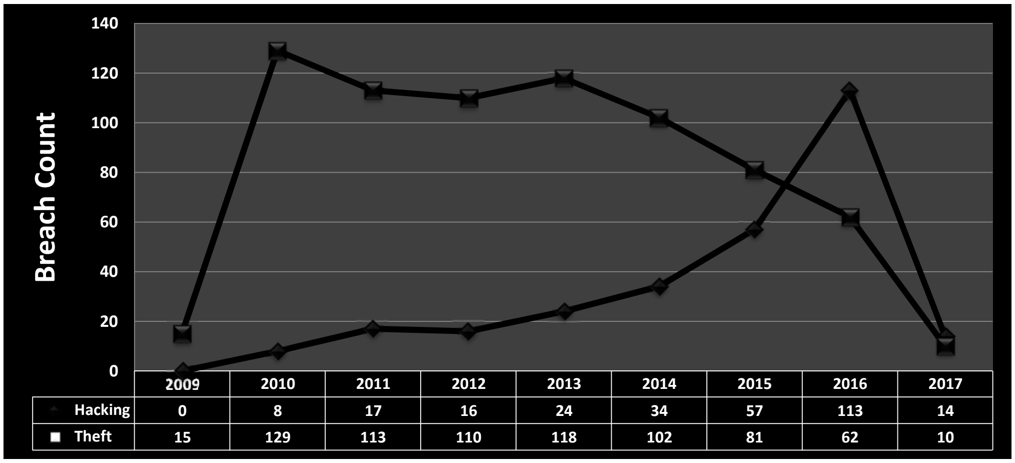
Rainbow Children's Clinic

METHODIST HOSPITAL Our mission is your health.

NJ SPINE & ORTHOPEDIC

MedStar Health

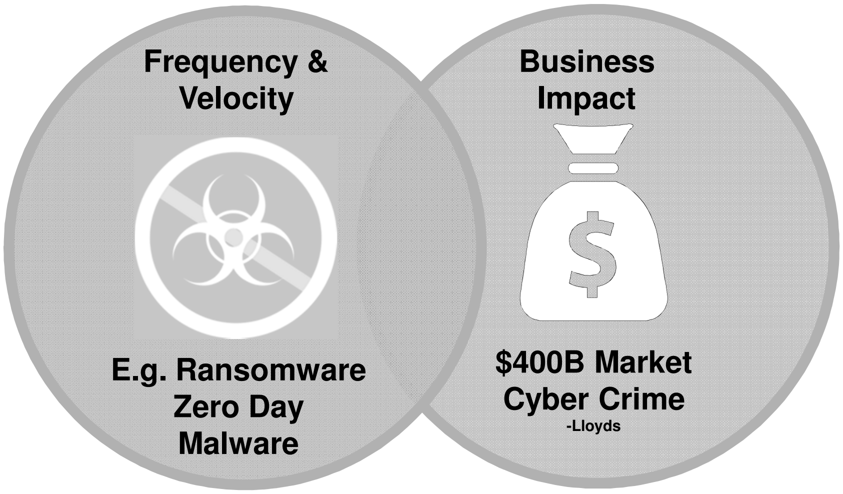
THEFT VS HACKING TREND



	2009	2010	2011	2012	2013	2014	2015	2016	2017
◆ Hacking	0	8	17	16	24	34	57	113	14
■ Theft	15	129	113	110	118	102	81	62	10

Source: U.S. Department of Health and Human Services
Office for Civil Rights Breach Portal
https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Healthcare Industry: Challenges – Cyber Threats



Frequency & Velocity

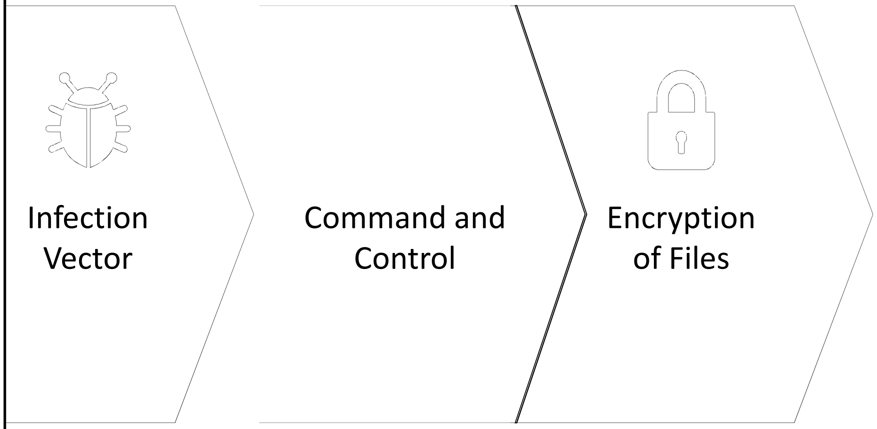
E.g. Ransomware
Zero Day
Malware

Business Impact

$400B Market
Cyber Crime
-Lloyds

Typical Ransomware Infection

Ransomware is malware for data kidnapping, an exploit in which the attacker encrypts the victim's data and demands payment for the decryption key. Ransomware spreads through e-mail attachments, infected programs and compromised websites.



Ransomware: Underground Market Place

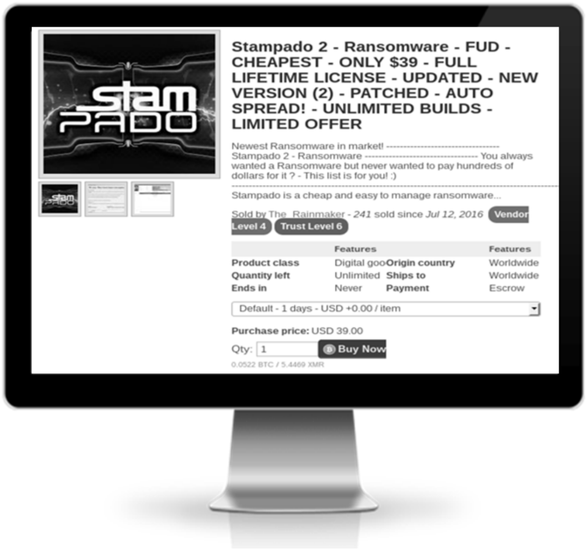
1

$39 Only

Lifetime License

2

Russian Roulette



Stampado 2 - Ransomware - FUD - CHEAPEST - ONLY $39 - FULL LIFETIME LICENSE - UPDATED - NEW VERSION (2) - PATCHED - AUTO SPREAD! - UNLIMITED BUILDS - LIMITED OFFER

Newest Ransomware in market! -------------------------------- Stampado 2 - Ransomware -------------------------------- You always wanted a Ransomware but never wanted to pay hundreds of dollars for it ? - This list is for you! :)

Stampado is a cheap and easy to manage ransomware...

Sold by The_Rainmaker - *241* sold since *Jul 12, 2016* Vendor Level 4 Trust Level 6

	Features		Features
Product class	Digital goo	**Origin country**	Worldwide
Quantity left	Unlimited	**Ships to**	Worldwide
Ends in	Never	**Payment**	Escrow

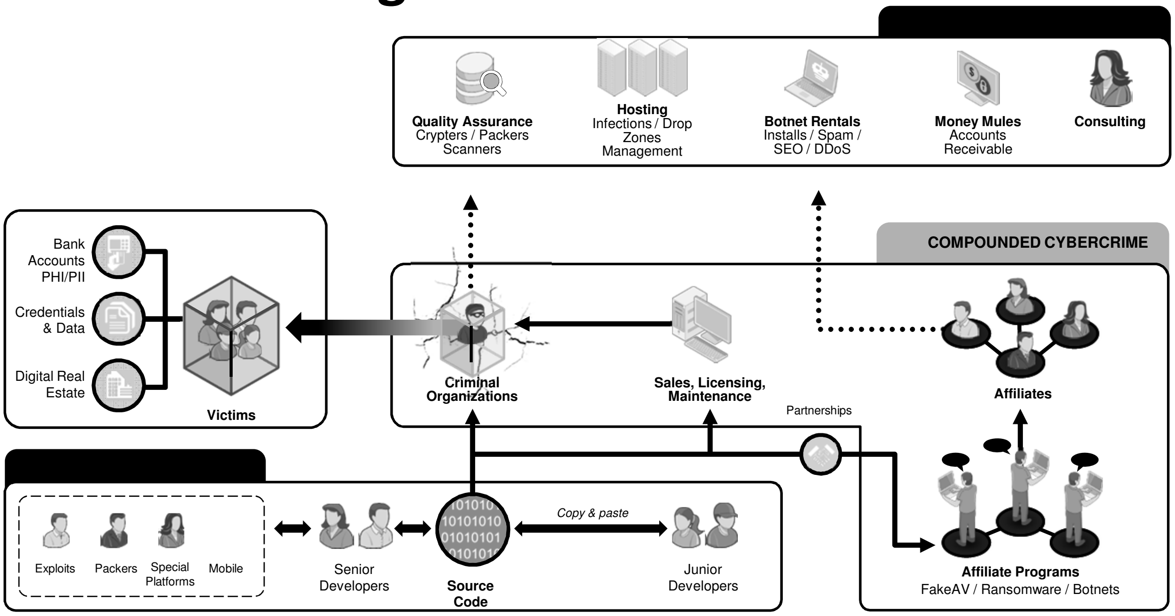
Default - 1 days - USD +0.00 / item

Purchase price: USD 39.00

Qty: 1 Buy Now

0.0522 BTC / 5.4469 XMR

Evolving Threat Market Place



Kill Chain: Attacker Defender Lifecycle

Attacker Methodology

Recon Weaponize Delivery Install Exploit Command & Controls Action

Increasing Risk and Cost to the Business

Defender Response

Preparation

- Investments
- Deployments
- Policy & Procedures
- Training & Exercises

Protection & Detection

- Network
- Hosts
- Applications

Response

- First Response
- Containment
- Mitigation
- Reporting

Recovery

- Forensics
- Clean Up
- Reporting
- Lessons Learned

“

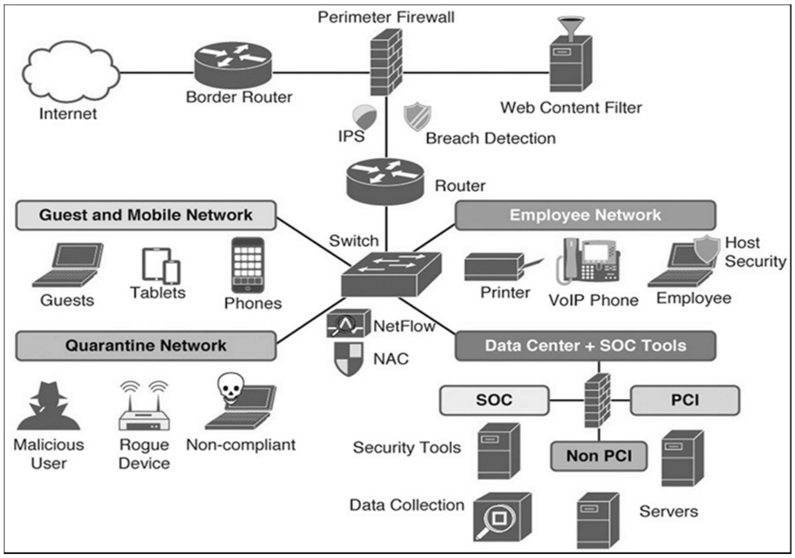
DISCUSS SOME OF THE WAYS YOU CAN **BREAK THE KILL CHAIN** AND DEFEND AGAINST MULTI-VECTOR ATTACKS.

”

Decrypting a Ransomware Strategy

SECURE NETWORK THREAT DETECTION & ANALYSIS

Sample Secure Network Topology



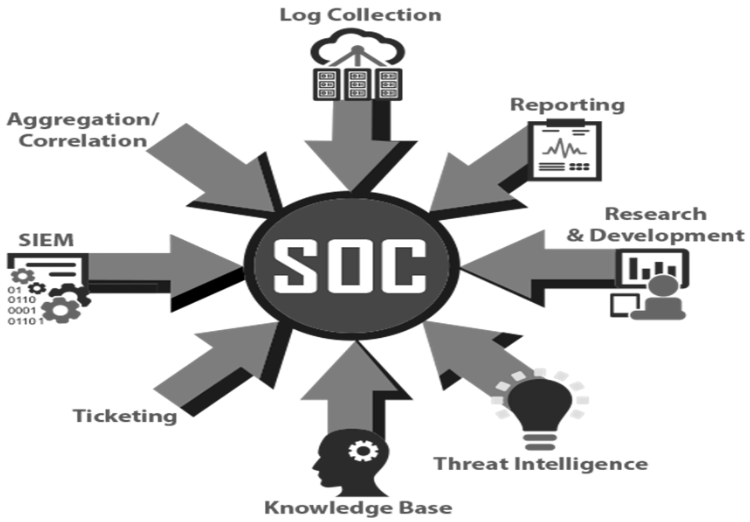
Segmentation: Not all assets are equal

LIFE CRITICAL:
No Internet -> Connection to Internal; APPS and DC only
Highly Segmented from the rest of the network
SEGMENTED NETWORK

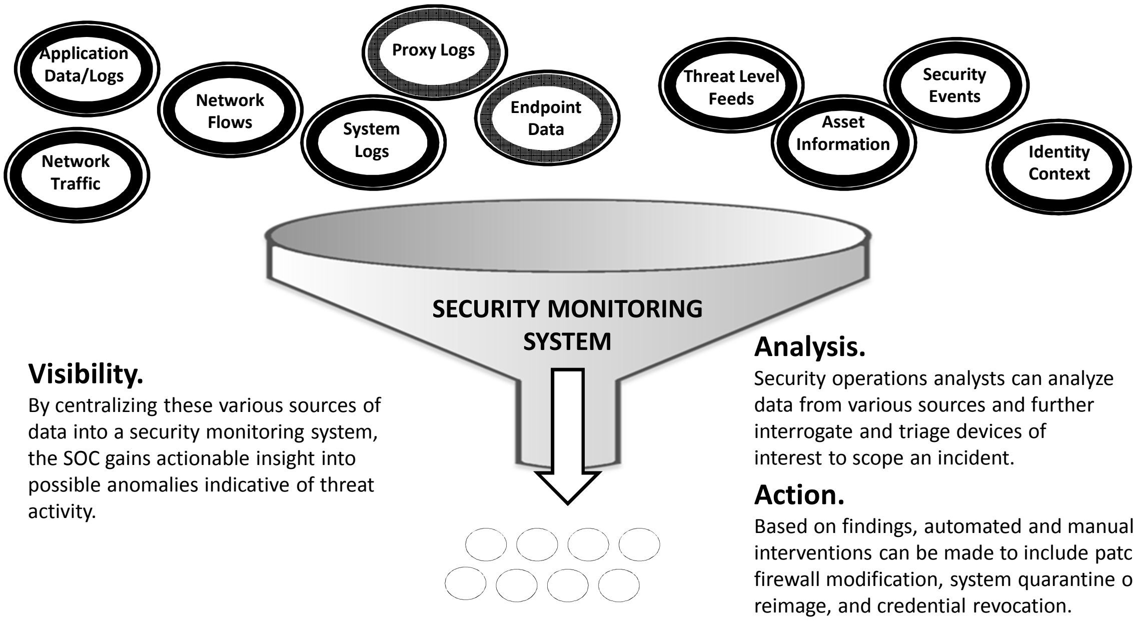
HIGH PHI/PII/PCI:
Strong Encryption, 2 Factor Authentication, Whitelist (signed) Apps, DNS Firewalling, Endpoint Protection, Server Side Protection, Proxid Interet Access, MicroSegmentation, App Sandboxing, Email Security, Content Filtetering/Inspection

Low/Medium:
DNS Firewalling, Endpoint Protection, Server side Protection, Proxied Internet Access, Content Filtering/Inspection.

Security Operations Center



SOC: Data Aggregation for Improved Incident Handling



Visibility.

By centralizing these various sources of data into a security monitoring system, the SOC gains actionable insight into possible anomalies indicative of threat activity.

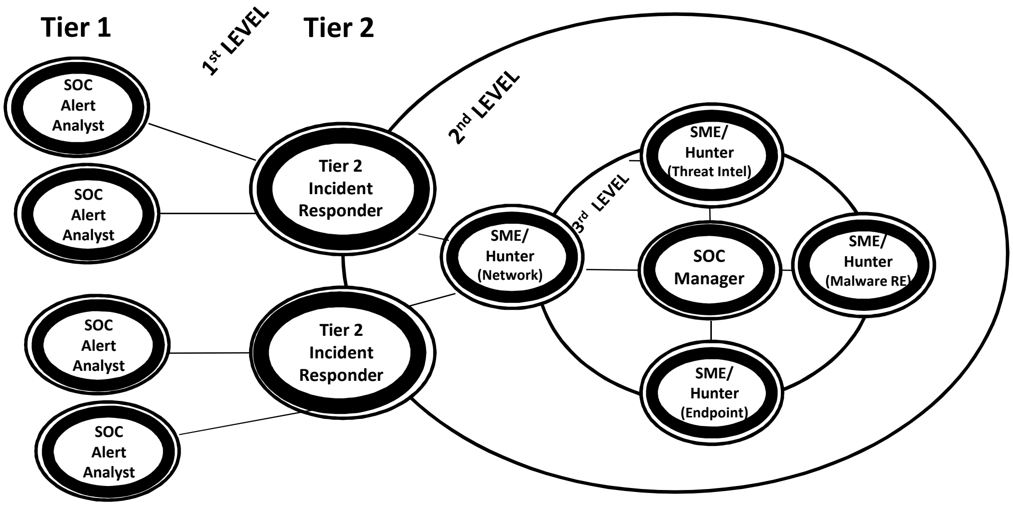
Analysis.

Security operations analysts can analyze data from various sources and further interrogate and triage devices of interest to scope an incident.

Action.

Based on findings, automated and manual interventions can be made to include patching, firewall modification, system quarantine or reimage, and credential revocation.

Tiered Security Operations



Tier 1

1st LEVEL

Tier 2

2nd LEVEL

3rd LEVEL

SOC Alert Analyst

SOC Alert Analyst

SOC Alert Analyst

SOC Alert Analyst

Tier 2 Incident Responder

Tier 2 Incident Responder

SME/ Hunter (Network)

SME/ Hunter (Threat Intel)

SOC Manager

SME/ Hunter (Malware RE)

SME/ Hunter (Endpoint)

Threat Management

- Consolidate functions of incident monitoring, detection, response, coordination, and computer network defense tool engineering, operation, and maintenance under one organization: the Cyber Security Operations Center (CSOC.)
- Achieve balance between size and visibility/agility, so that the CSOC can execute its mission effectively.
- Give the CSOC the authority to do its job through effective organizational placement and appropriate policies and procedures.
- Focus on a few activities that the CSOC practices well and avoid the ones it cannot or should not do.
- Favor staff quality over quantity, employing professionals who are passionate about their jobs, provide a balance of soft and hard skills, and pursue opportunities for growth.
- Realize the full potential of each technology through careful investment and keen awareness of—and compensation for—each tool’s limitations.

Common Vocabulary

- Attack method : The manner or technique and means an adversary may use in an assault on information or an information system.
- Exfiltration: The unauthorized transfer of information from an information system.
- Attack Vector
- Indicator of Compromise
- C2– command and control
- DPP (Deep Packet Processing) -Deep Packet Processing delivers the ability to inspect, forward, drop, clone, or even modify network traffic, at line rates. With Deep Packet Processing and combinations of policies and/or programming, the lag time from inspection to action drops from minutes or hours or worse, days, to milliseconds.
- EPP (endpoint protection): Including host-based features like firewall, anti-malware, whitelisting and disk encryption
- EVC – Endpoint Visibility and Control
- ETDR – endpoint threat detection and response
- Tactical Threat Intelligence – often referred to as tactics, techniques and procedures (TTPs) and is information about how threat actors are conducting attacks
- TTPs – Tools, Techniques and Processes

Threat Intelligence

- **Cyber Intel Collection and Analysis :** Collection, consumption, and analysis of cyber intelligence reports, cyber intrusion reports, and news related to information security, covering new threats, vulnerabilities, products, and research.
- **Cyber Intel Distribution:** Synthesis, summarization, and redistribution of cyber intelligence reports, cyber intrusion reports, and news related to information security to members of the constituency on either a routine basis (such as a weekly or monthly cyber newsletter) or a non-routine basis (such as an emergency patch notice or phishing campaign alert).
- **Cyber Intel Creation:** Primary authorship of new cyber intelligence reporting, such as threat notices or highlights, based on primary research performed by the SOC. For example, analysis of a new threat or vulnerability not previously seen elsewhere. This is usually driven by the SOC's own incidents, forensic analysis, malware analysis, and adversary engagements.
- **Cyber Intel Fusion:** Extracting data from cyber intel and synthesizing it into new signatures, content, and understanding of adversary TTPs, thereby evolving monitoring operations (e.g., new signatures or SIEM content).
- **Trending:** Long-term analysis of event feeds, collected malware, and incident data for evidence of malicious or anomalous activity or to better understand the constituency or adversary TTPs (Tools, Techniques and Processes. This may include unstructured, open-ended, deep-dive analysis on various data feeds, trending and correlation over weeks or months of log data, "low and slow" data analysis, and esoteric anomaly detection methods.
- **Threat Assessment:** Holistic estimation of threats posed by various actors against the constituency, its enclaves, or lines of business, *within the cyber realm*. This will include leveraging existing resources such as cyber intel feeds and trending, along with the enterprise's architecture and vulnerability status. Often performed in coordination with other cybersecurity stakeholders.

Security Outreach

- **Product Assessment**

Testing the security features of point products being acquired by constituency members. Analogous to miniature vulnerability assessments of one or a few hosts, this testing allows in-depth analysis of a particular product's strengths and weaknesses
from a security perspective. This may involve "in-house" testing of products rather than remote assessment of production or preproduction systems.

- **Security Consulting**

Providing cybersecurity advice to constituents outside the scope of CND; supporting new system design, business continuity, and disaster recovery planning; cybersecurity policy; secure configuration guides; and other efforts.

- **Training and Awareness Building**

Proactive outreach to constituents supporting general user training, bulletins, and other educational materials that help them understand various cybersecurity issues. The main goals are to help constituents protect themselves from common threats
such as phishing/pharming schemes, better secure end systems, raise awareness of the SOC's services, and help constituents correctly report incidents.

- **Situational Awareness**

Regular, repeatable repackaging and redistribution of the SOC's knowledge of constituency assets, networks, threats, incidents, and vulnerabilities to constituents. This capability goes beyond cyber intel distribution, enhancing constituents' understanding
of the cybersecurity posture of the constituency and portions thereof, driving effective decision making at all levels. This information can be delivered automatically through a SOC website, Web portal, or email distribution list.

- **Redistribution of TTPs (**Tools, Techniques and Processes)

Sustained sharing of SOC internal products to other consumers such as partner or subordinate SOCs, in a more formal, polished, or structured format. This can include almost anything the SOC develops on its own (e.g., tools, cyber intel, signatures, incident
reports, and other raw observables). The principle of quid pro quo often applies: information flow between SOCs is bidirectional.

- **Media Relations**

Direct communication with the news media. The SOC is responsible for disclosing
information without impacting the reputation of the constituency or ongoing response

Decrypting a Ransomware Strategy

BREACH SECURITY ASSESSMENT

Healthcare Breach Security Assessment Program

- Created by Intel and VMware
- The assessment is free of Cost
- Confidential
- Contact:

Chris Logan
Sr. Healthcare Strategist
VMware Healthcare
clogan@vmware.com

Breach Security Assessment How it Works

- One (1) hour assessment
- By conference call or in person
- Priority across 8 breach types
- Presence of 42 breach security capabilities from the maturity model
- Org type, country, size for future comparison with similar peers
- Post assessment and quarterly reports
- Maturity score, priorities and capabilities benchmarked against industry
- Spreadsheet used to gather assessment input
- No personally identifiable information or patient information collected

Breach Types Assessed

1. Cybercrime Hacking
2. Ransomware
3. Loss or Theft of Mobile Device or Media
4. Insider Accidents or Workarounds
5. Business Associates
6. Malicious Insiders or Fraud
7. Insider Snooping
8. Improper Disposal

Breach Security Capabilities Maturity Model

Baseline

+ Policy
+ Risk assessment
+ Audit and compliance
+ User training
+ Endpoint device encryption
+ Mobile device management
+ Data Loss Prevention (discovery)
+ Anti-malware
+ IAM, Single factor access control
+ Firewall
+ Email gateway
+ Web gateway
+ Vulnerability management, patching
+ Security incident response plan
+ Secure Disposal
+ Backup and Restore

Enhanced

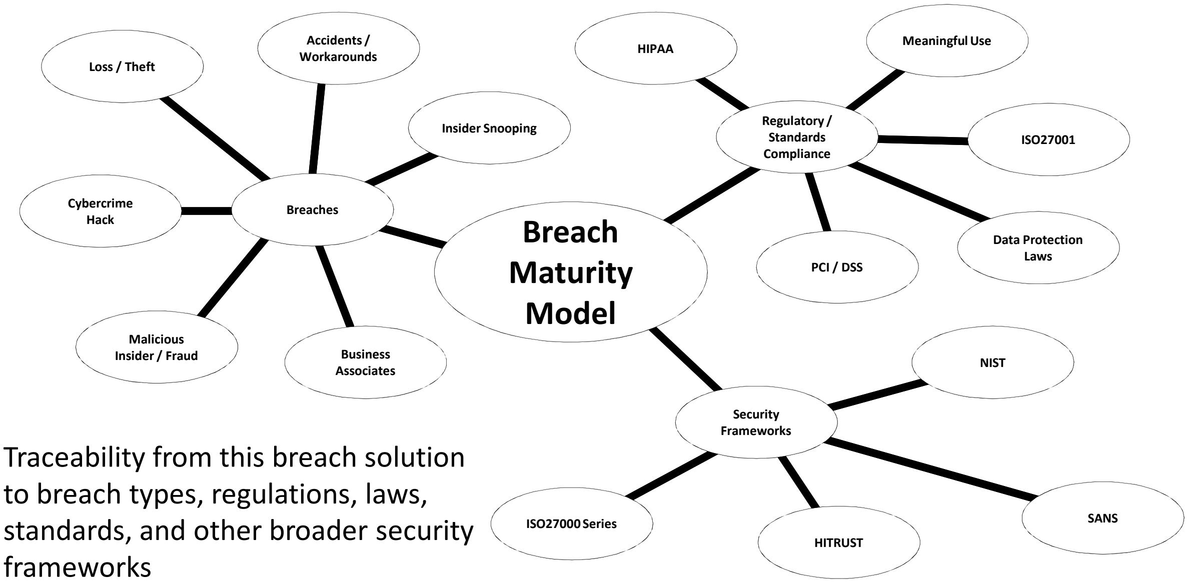
+ Device control
+ Penetration testing / vulnerability scan
+ Client Solid State Drive (encrypted)
+ Endpoint Data Loss Prevention
+ Network Data Loss Prevention (monitoring, capture)
+ Anti-theft: remote locate, lock, wipe
+ Multi-factor authentication w timeout
+ Secure remote administration
+ Policy based encryption for files and folders
+ Server / database / backup encryption
+ Network segmentation
+ Network Intrusion Prevention System
+ Business associate agreements
+ Virtualization

Advanced

+ Server Solid State Drive (encrypted)
+ Network Data Loss Prevention (prevention)
+ Database activity monitoring
+ Digital forensics
+ Security Information and Event Management
+ Threat intelligence
+ Multi-factor authentication with walk-away lock
+ Client Application Whitelisting
+ Server Application Whitelisting
+ De-identification / anonymization
+ Tokenization
+ Business Continuity and Disaster Recovery

Improved Breach Security, Usability, Cost, IT Operations

Improve Breach Security as well as Compliance



Traceability from this breach solution to breach types, regulations, laws, standards, and other broader security frameworks

Strategic Approach

ADOPT A FRAMEWORK

PERFORM FOCUSED RISK ASSESSMENTS

DEVELOP A STRATEGIC PLAN: 3 YEARS OR MORE

FOCUS ON INCIDENT RESPONSE