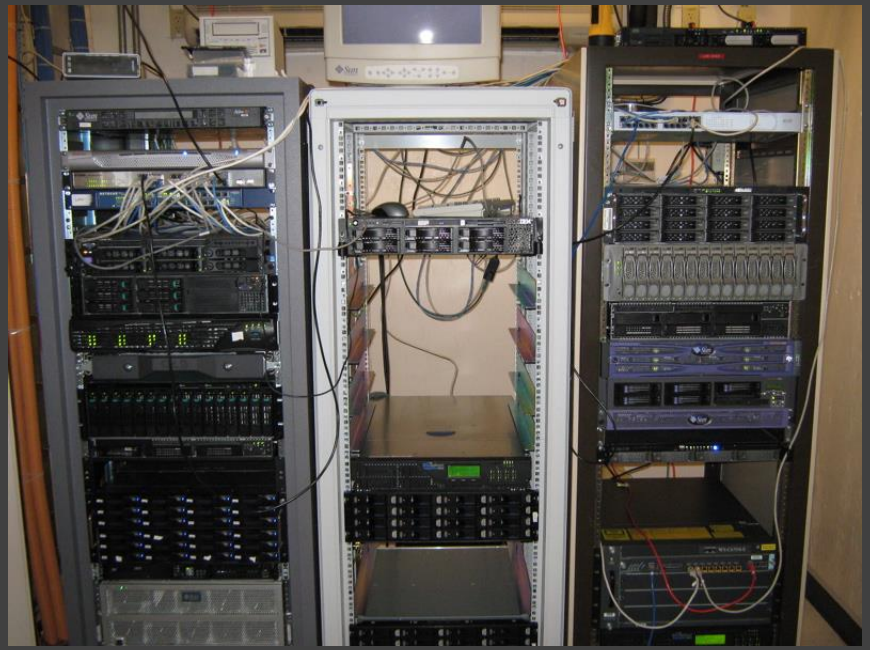
SECURITY IN MICROSOFT AZURE

Marija Strazdas – Sr. Solutions Engineer

ALERT LOGIC

Infrastructure Has Changed

Buying Hardware



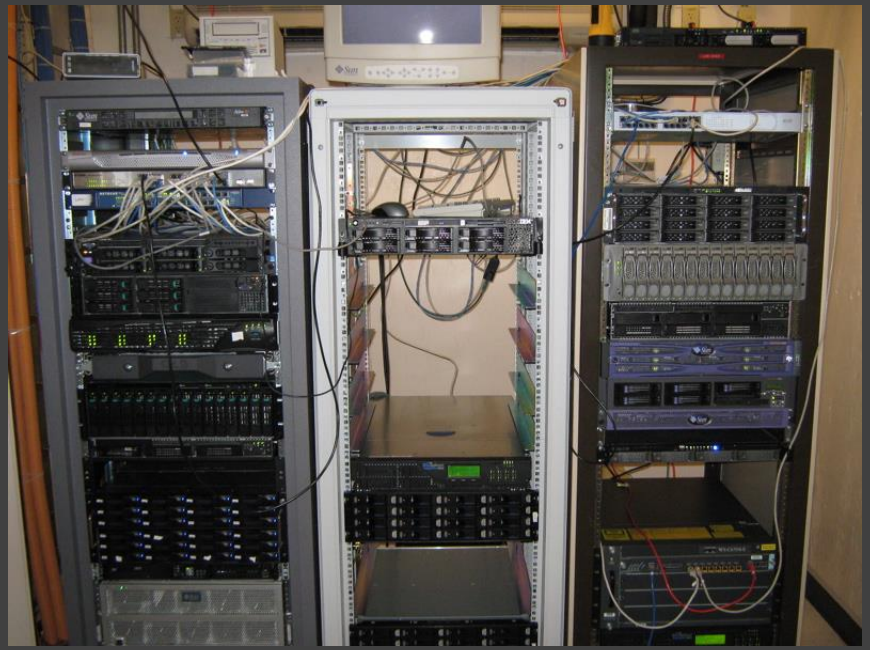
EARLY 2000's

MID 2000's

NOW

Infrastructure Has Changed

Buying Hardware



Infrastructure As Code

EARLY 2000's

MID 2000's

NOW

Cybercrime Has Also Changed

Single Actors

EARLY 2000's

MID 2000's

NOW

Cybercrime Has Also Changed

Single Actors

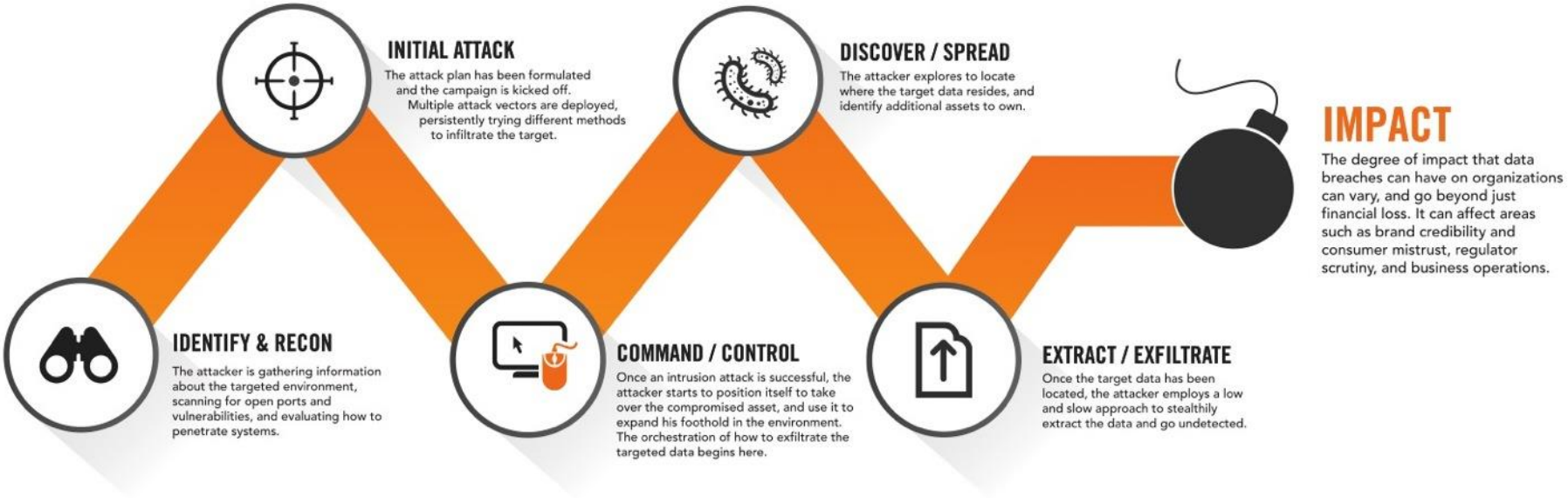
Highly Organized Groups

EARLY 2000's

MID 2000's

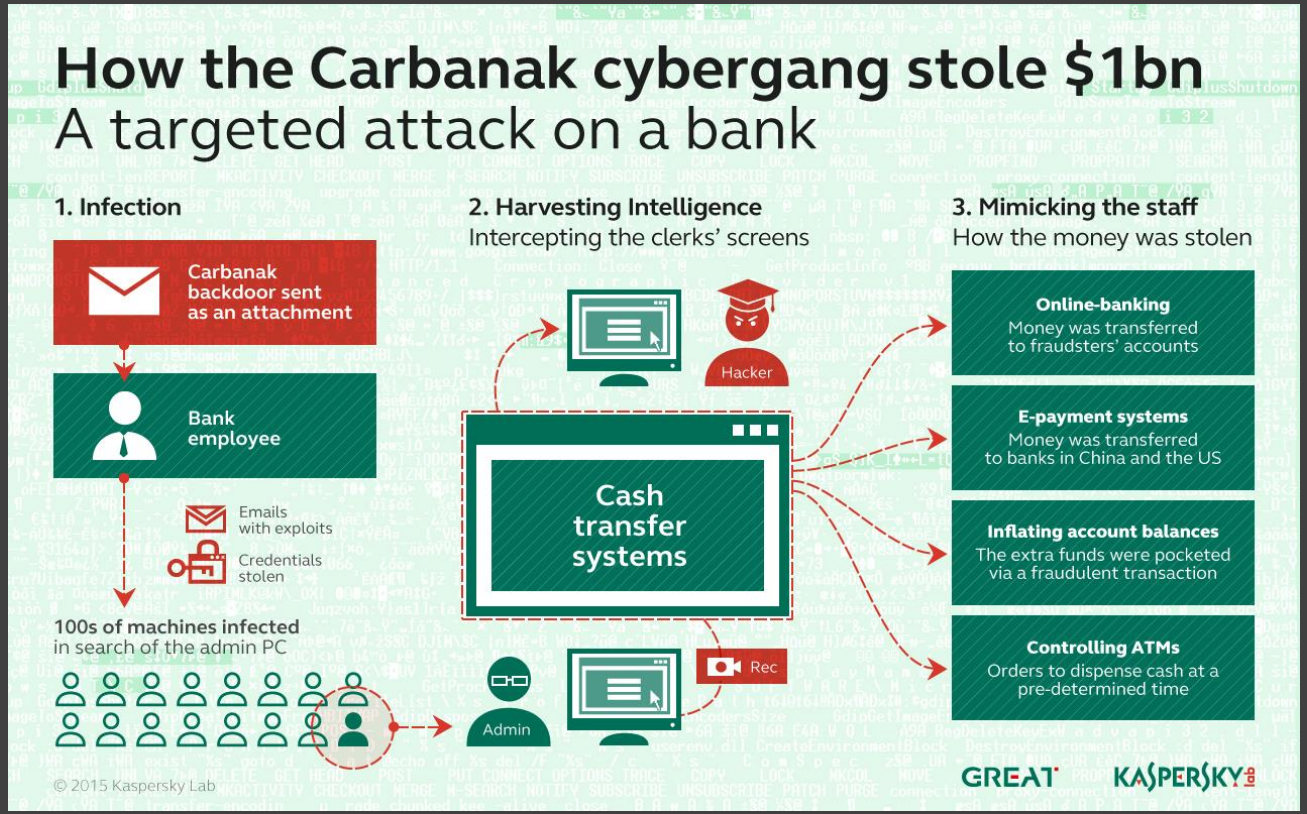
NOW

Today's Attacks Have Several Stages



Modern Bank Robbery – The Carbanak APT

- Over $1 Billion Total Stolen
- Losses per bank range from $2.5 Million - $10 Million
- Stealing money directly rather than through sale of stolen data
- Targets banks rather than endpoints
- Attacks multiple banking service channels: Databases, ATMs, E-Payment systems, etc



krebsonsecurity.com/wp-content/uploads/2015/02/Carbanak_APT_eng.pdf

Lasers!!! - Making Cars Slam on the Brakes

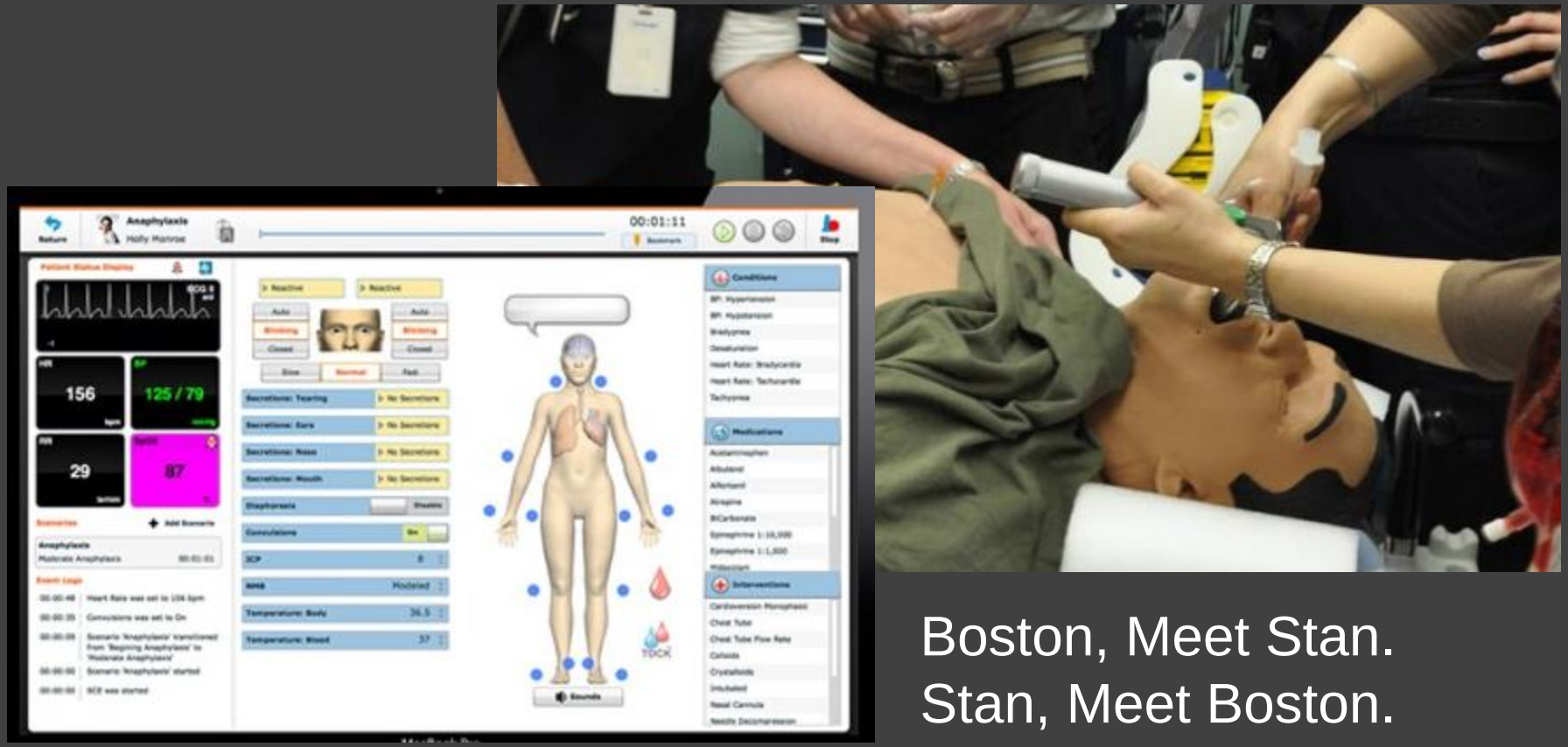
$60

amazon Prime

Internet of Things - Car Edition

A Jeep Cherokee winds up in a ditch after hackers working with "Wired" magazine successfully take control of the vehicle by hacking in through its connected-car infotainment system.
(Photo: Wired Magazine)

Internet of Things – Human Body Edition



Boston, Meet Stan.
Stan, Meet Boston.

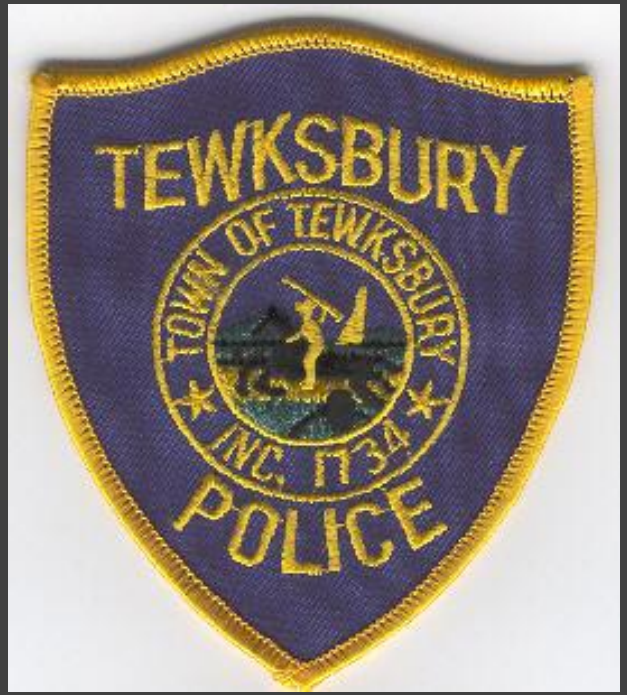
Case Study: Tewksbury Police Department

Attack

- Phishing email (package delivered – click this link for details)
- Employee clicked, malware was launched
- Attacker gained access and encrypted data on mapped servers
- Ransom demand of only $500 (if a million people give you $1, you have $1 million.)

Impact

- Total Police Operations Disruption
- Reverted to broken manual processes
- No access to arrest records/warrants
- Unable to conduct ID verification

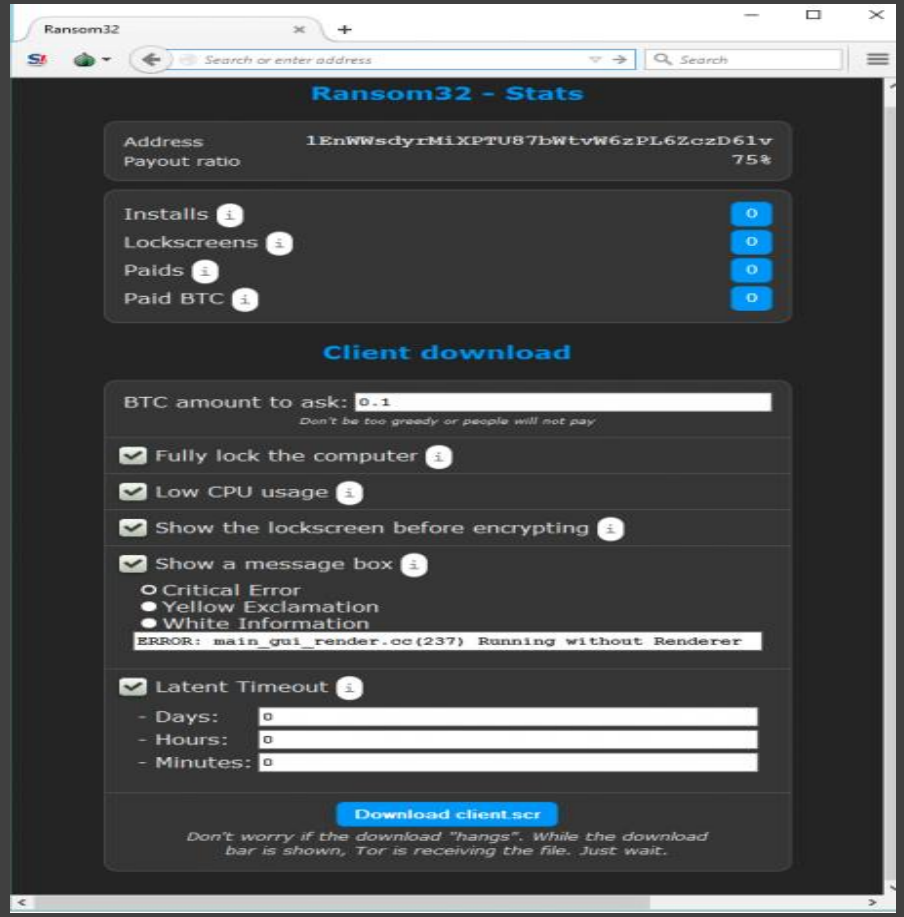


Five days with no computing. Public and private security experts unable to decrypt. No technical mitigation.

Ransomware as a Managed Service

Ransom32

- Hacking Staff Aug
- Tracking Dashboard
- BitCoin Payment Alerts
- Malware Configuration Assistance
- Zero Days Used
- You Got a Target List? – We'll give you a finder's fee
- Customize the Ransom Amount
- Customize the Ransom Message



If Ransomware Hits – Haggle!

- Act Quickly Before They Pack Up
- Most Attackers Happy
  With Much Lesser Amount
- In Larger Cases, FBI Recommends
  Professional Negotiators Be Hired

THE GOOD NEWS

ALERT LOGIC

Research Shows - You're Better Off In The Cloud

"Public cloud workloads can be at least as secure as those in your own data center, likely better."

- Neil McDonald – Gartner Security and Risk Management Summit

The security built into Azure meets the requirements of several compliance frameworks

Attestations for Microsoft Azure

Argentina PDPA
Canadian Privacy Laws
CCSL (IRAP)
CDSA
China DJCP
China GB 18030
China TRUCS
IT Grundschutz Compliance Workbook
Japan My Number Act
MARS-E
MeitY
MPAA
MTCS
NIST 800-17
CS Mark (Gold)
CSA STAR Attestation
CSA STAR Certification
CSA STAR Self-Assessment
DoD
ENISA IAF
EU Model Clauses
NZCC Framework
PCI-DSS
Section 508 VPATs
SHARED ASSESSMENTS
SOC 1
SOC 2
SOC 3
EU-U.S. Privacy Shield
FACT
FDA CFR Title 21 Part 11
FedRAMP
FERPA
FIPS 140-2
FISC
Spain ENS
UK G-Cloud
GxP
HIPAA/HITECH
IRS 1075
ISO 22301
ISO/IEC 27001
ISO/IEC 27017
ISO/IEC 27018

Cloud Security is a Shared Responsibility

APPS

- Web Application Firewall
- Application Scanning

- Secure Coding and Best Practices
- Software and Virtual Patching
- Configuration Management

- Access Management (inc. Multi-factor Authentication)
- Application level attack monitoring

VIRTUAL MACHINES

- Hypervisor Management
- System Image Library
- Root Access for Customers
- Managed Patching (PaaS, not IaaS)

- Security Monitoring
- Log Analysis
- Vulnerability Management

- Access Management
- Configuration Hardening
- Patch Management

NETWORKS

- Logical Network Segmentation
- Perimeter Security Services
- External DDOS, spoofing, and scanning monitored

- Network Packet Inspection
- Security Monitoring

- TLS/SSL Encryption
- Network Security

Configuration

INFRASTRUCTURE SERVICES

COMPUTE | STORAGE | DATABASE | NETWORK

MICROSOFT | CUSTOMER

The 5 Key Components for Cloud Security

1. Achieve Visibility
2. Keep Logs
3. Address Vulnerabilities
4. Limit Access
5. Automate

1. Achieve Visibility

2. Keep Logs

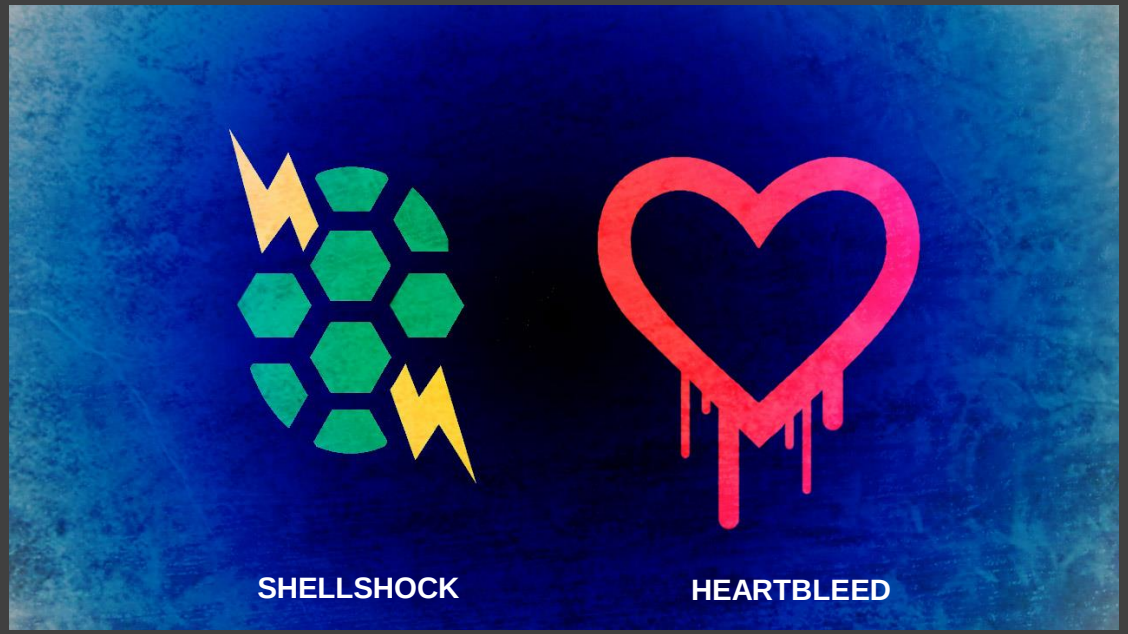
Everything you do in Azure is an API call

- New VM Created
- VM Spun Down
- Security Group Deleted / Changed
- Azure AD User Created
- Azure AD Role Modified
- Failed Console Logins
- Tag Modified

3. Address Vulnerabilities

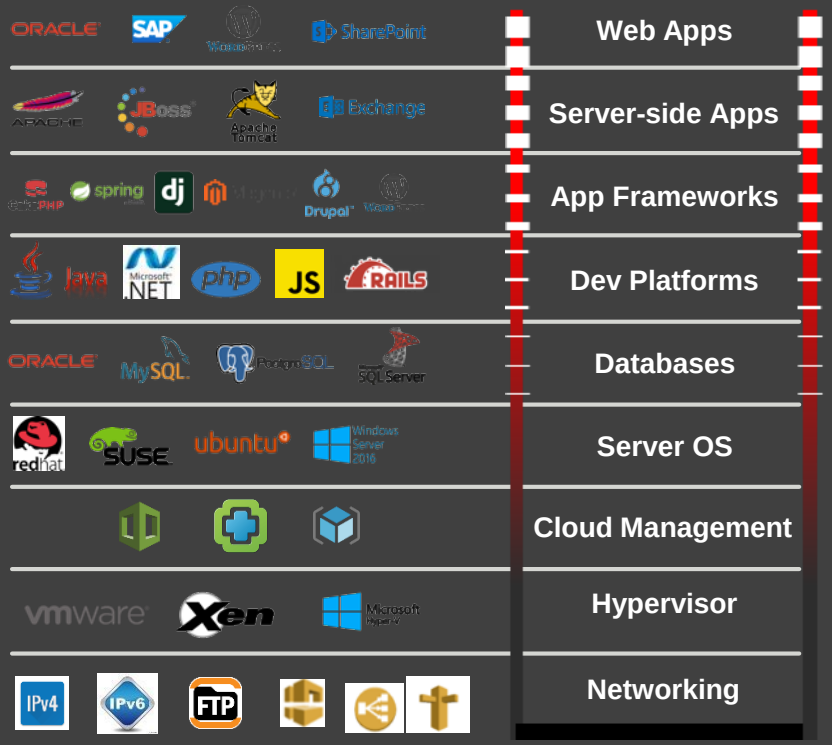
% of Global 2000 Organizations Vulnerable to Heartbleed in August 2014: ***76%***

April, 2015: ***74%***

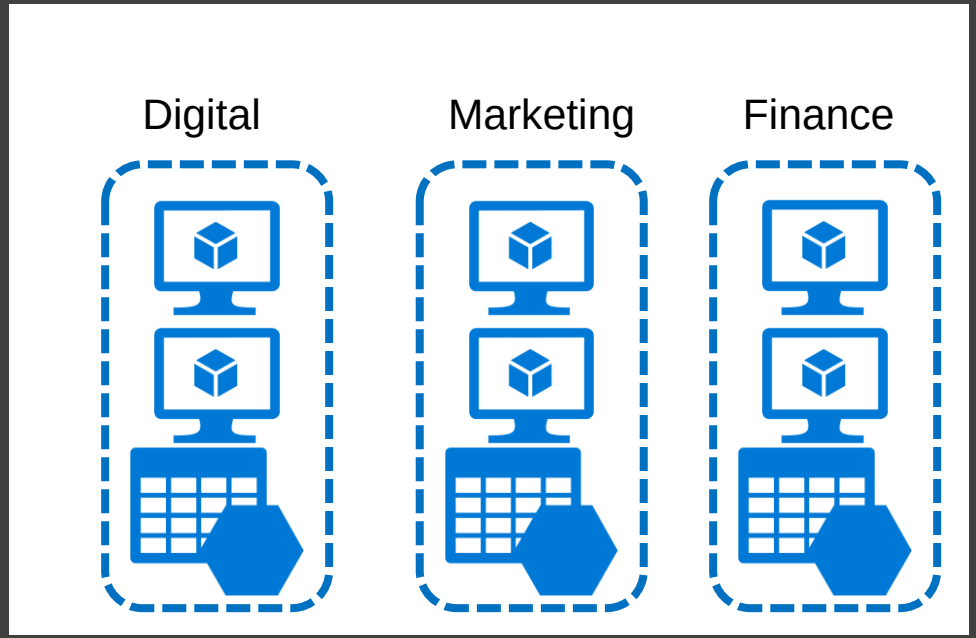


Source: SC Magazine: scmagazine.com/one-year-later-heartbleed-still-a-threat/article/407803/

Patching Involves The Whole Stack



4. Limit Access



RBAC allows for granular access control at the resource level

5. Automate

Rather than drawing a a picture each time…

..Use a printing Press.

Security can be baked into the process

Data Security and Access Management

- Lock down Admin account in Azure
- Enable MFA (Azure, hardware/software token)
- Start with a least privilege access model (e.g. Use RBAC) *avoid owner role unless absolutely necessary
- Identify data infrastructure that requires access (e.g. Lock down AzureSQL)
- Azure NSG (private vs public)
- Continually audit access (Azure Activity Logs)
- AAD Premium – (*Security analytics and alerting)
- Manage with Secure Workstations (e.g. DMZ, MGMT)
- Protect data in transit and at rest
- Encrypt Azure Virtual Machines
- Enable SQL Data Encryption

Additional Azure-Specific Security Best Practices

- Logically segment subnets
- Control routing behavior
- Enable Forced Tunneling (e.g. forcing internet through on-premise and/or DC)
- Use Virtual network appliances (e.g FW, IDS/IPS, AV, Web Filtering, Application ELB)
- Deploy DMZs for security zoning
- Optimize uptime and performance
- Use global load balancing
- Disable RDP or SSH Access to Azure Virtual Machines
- Enable Azure Security Center
- Extend your datacenter into Azure

Thank you.

ALERT LOGIC®

ALERT LOGIC SOLUTIONS

ALERT LOGIC®

What Organizations Hope To Achieve

DESIRED CAPABILITIES	REQUIRED TECHNOLOGY	REQUIRED CONTENT	REQUIRED EXPERTISE
Protect web apps	Web application firewall (WAF)	Whitelists, blacklists	WAF rules expert
Identify network threats	Intrusion detection/ protection	Signatures, rules	Network security expert
Uncover incidents of compromise in logs	Log management	Log parsers and correlation rules	Log analyst expert
Discover advanced multi-vector attacks	Threat analytics platform	Taxonomy, correlation rules	Correlation rules expert
Find vulnerabilities	Vulnerability management	CVE coverage	Scanning expert
Threat intel and security content	Databases, information management, malware	Emerging threats, zero days, malware	Expert knowledge of criminal underground
24x7 monitoring and analysis	Analysis tools	Incident information	Security analysts
Availability and performance monitoring	Middleware, APIs, and monitoring tools	Availability and performance metrics	Network ops experts, system admins

Cloud Security is a Shared Responsibility

APPS

- Web Application Firewall
- Vulnerability Scanning

- Secure Coding and Best Practices
- Software and Virtual Patching
- Configuration Management

- Access Management (inc. Multi-factor Authentication)
- Application level attack monitoring

VIRTUAL MACHINES

- Hypervisor Management
- System Image Library
- Root Access for Customers
- Managed Patching (PaaS, not IaaS)

- Security Monitoring
- Log Analysis
- Vulnerability Scanning

- Access Management
- Configuration Hardening
- Patch Management

NETWORKS

- Logical Network Segmentation
- Perimeter Security Services
- External DDOS, spoofing, and scanning monitored

- Network Threat Detection
- Security Monitoring

- TLS/SSL Encryption
- Network Security

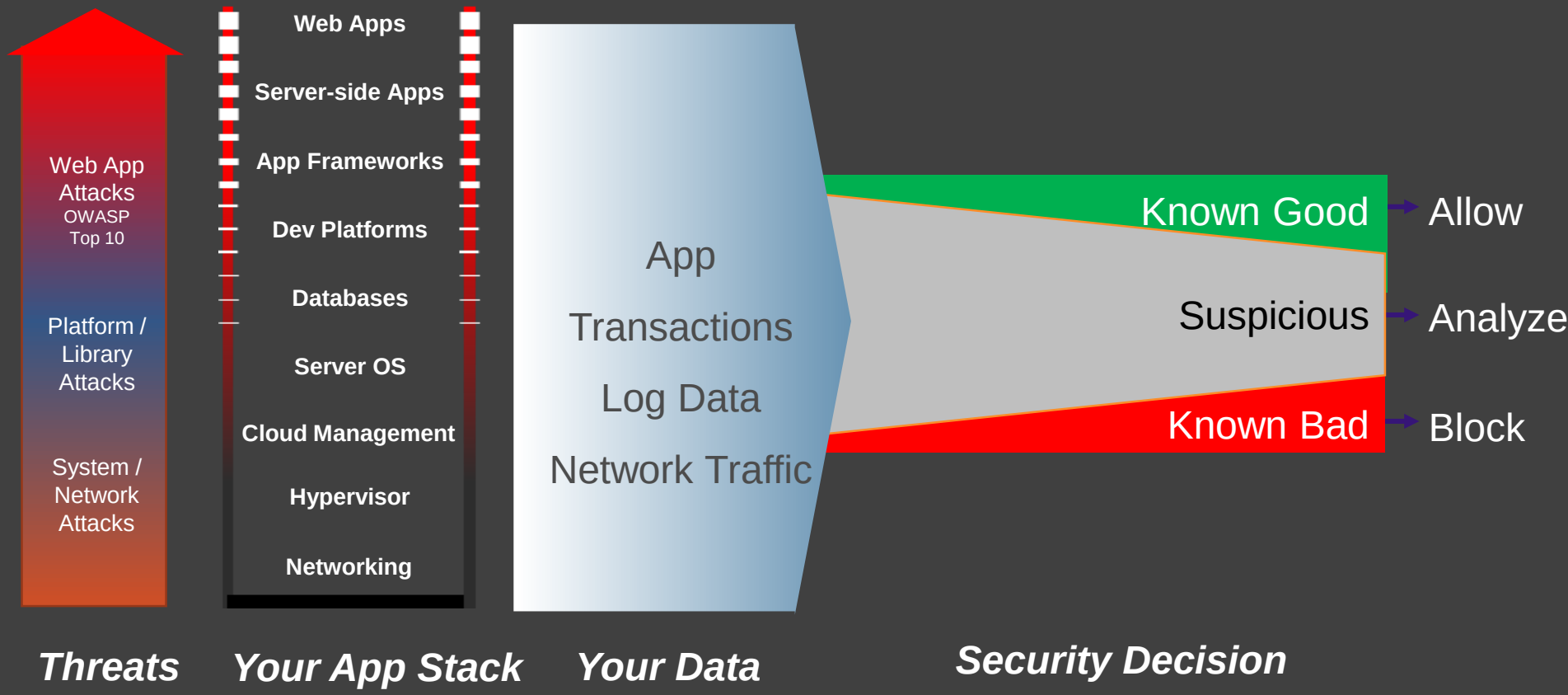
Configuration

INFRASTRUCTURE SERVICES

COMPUTE | STORAGE | DATABASE | NETWORK

MICROSOFT | ALERT LOGIC | CUSTOMER

Focus requires full stack inspection…and complex analysis



Thank you.

ALERT LOGIC®

Over 4,100 Organizations Worldwide Trust Alert Logic

AUTOMOTIVE

BMW
Hertz
SUBARU

EDUCATION

HARVARD UNIVERSITY Health Services
Rosetta Stone

ENERGY & CHEMICALS

Quantum Resources Management, LLC
WILBUR-ELLIS Ideas to Grow With
C&J Energy Services

FINANCIAL SERVICES

AMERICAN EXPRESS
Capital One
The Exeter
HSBC The world's local bank
MassMutual FINANCIAL GROUP
PayLease
PennyMac
PayPal
RBS The Royal Bank of Scotland
SCOR The Art & Science of Risk

HEALTHCARE

AstraZeneca
Johnson & Johnson
Methodist HEALTH SYSTEM
Smile Brands Group

MANUFACTURING

3M
Anheuser-Busch
FUJIFILM Value from Innovation
HERSHEY'S
Levi's
Nestlé
SIEMENS
Stanley Black&Decker

MEDIA/PUBLISHING

Disney
DreamWorks SKG
Sony/ATV MUSIC PUBLISHING
Time Inc.

TECHNOLOGY & SERVICES

Deloitte.
LOEB & LOEB LLP
Adobe
everbridge
Thru.
clickwrk
concep EMPOWERMENT MARKETING

RETAIL/E-COMMERCE

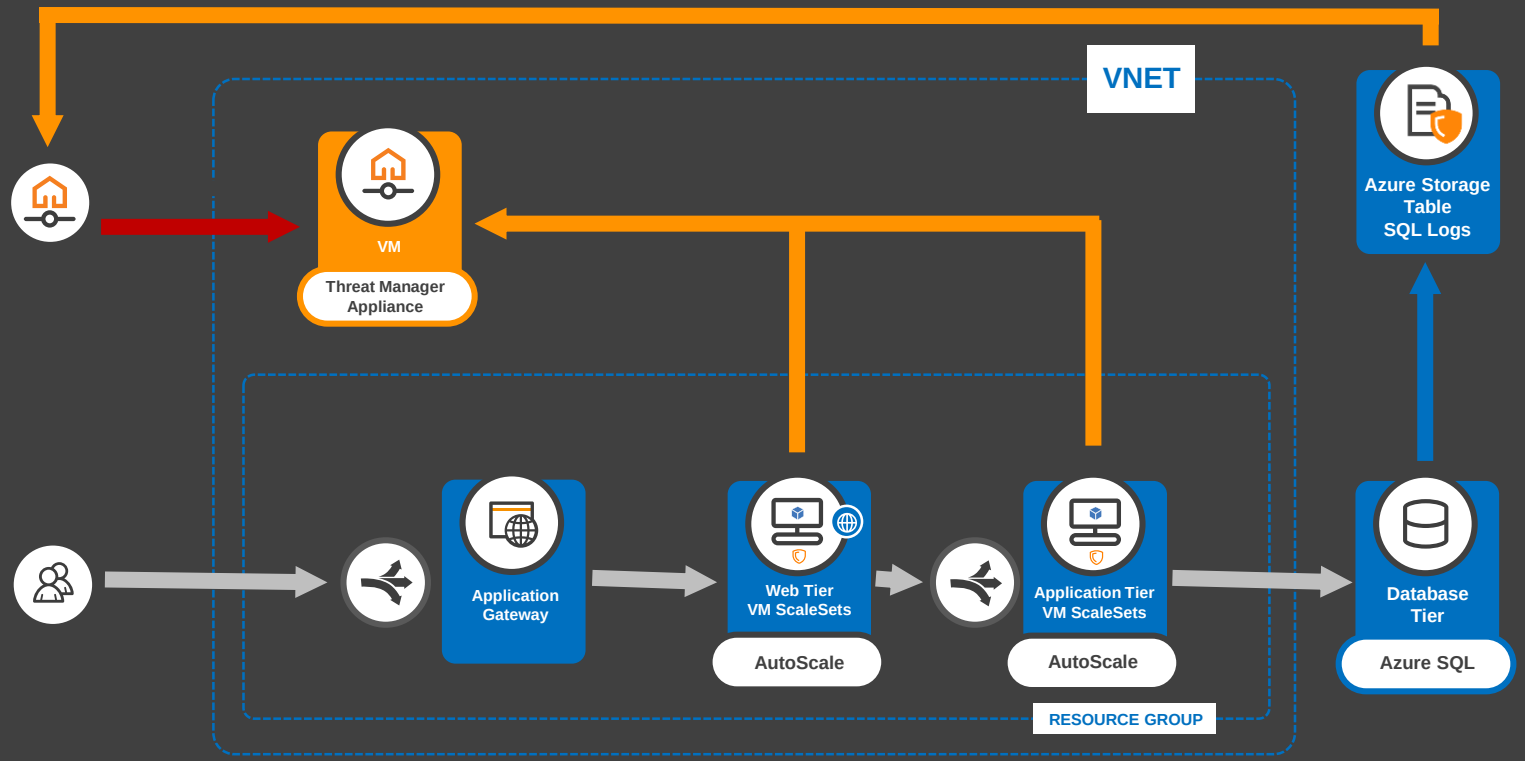
7 ELEVEN
FAZOLI'S
Rue la la
Tuesday Morning
Walmart eCommerce

NON-PROFIT

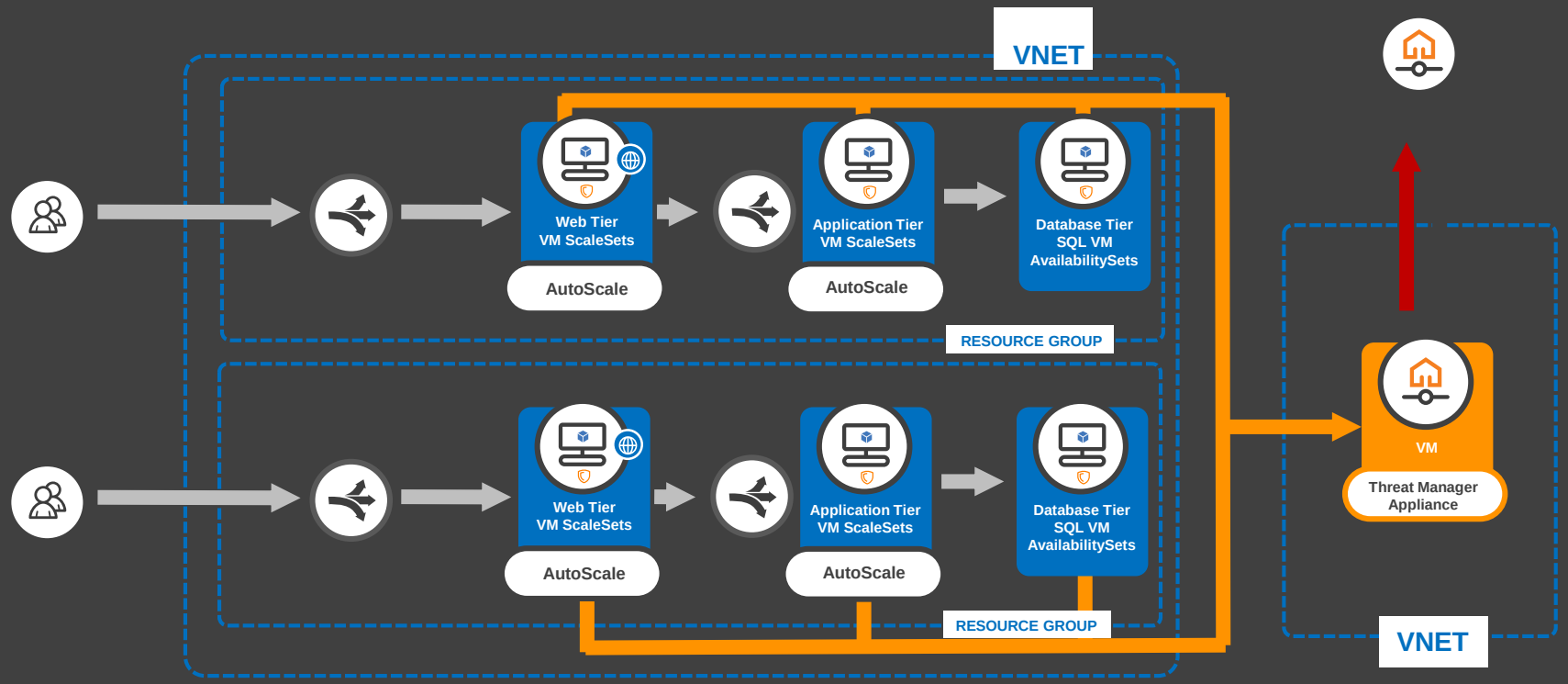
AARP Real Possibilities
LA PHIL
valldata

HOW IT WORKS:

Alert Logic Threat Manager for 3 Tier Application Stack + Azure SQL



3-Tier applications using VMs only



Agents can be baked into VM images, or automatically installed using DevOps toolsets

RSS

al_agents (19) Versions 1.3.6

Follow 2

Installs/Configures the Alert Logic Agent

Berkshelf/Librarian Policyfile Knife

```
cookbook 'al_agents', '~> 1.3.6'
```

README Dependencies Changelog Quality

build passing

Alert Logic Agent Cookbook

This cookbook is used to install and configure the Alert Logic agent.

alertlogic
Alert Logic Inc.

DETAILS

View Source View Issues

UPDATED JULY 29, 2016
Created on August 28, 2015

PLATFORMS

BADGES

LICENSE
Apache 2.0 License

https://supermarket.chef.io/cookbooks/al_agents

ARM Template automate appliance deployments

alertlogic / al-arm-templates

Watch 11 | Star 0 | Fork 2

Code | Issues 0 | Pull requests 0 | Projects 0 | Pulse | Graphs

Alert Logic Azure Resource Manager Templates

85 commits | 1 branch | 4 releases | 2 contributors

Branch: master | New pull request | Find file | Clone or download

jearly committed on GitHub Merge pull request #32 from jearly/master ... Latest commit 4290def 8 days ago

threat-manager	fixing issues #30 and #31	16 days ago
web-security-manager	fix syntax error	10 months ago
README.md	update readme	6 months ago

README.md

Alert Logic Azure Resource Manager Templates

Threat Manager(Marketplace Image): Deployment How-To

https://github.com/alertlogic/al-arm-templates

Addressing Customers with Compliance Requirements

Alert Logic Solution	PCI DSS	SOX	HIPAA & HITECH
Alert Logic Web Security Manager™	• 6.5.d Have processes in place to protect applications from common vulnerabilities such as injection flaws, buffer overflows and others • 6.6 Address new threats and vulnerabilities on an ongoing basis by installing a web application firewall in front of public-facing web applications.	• DS 5.10 Network Security • AI 3.2 Infrastructure resource protection and availability	• 164.308(a)(1) Security Management Process • 164.308(a)(6) Security Incident Procedures
Alert Logic Log Manager™	• 10.2 Automated audit trails • 10.3 Capture audit trails • 10.5 Secure logs • 10.6 Review logs at least daily • 10.7 Maintain logs online for three months • 10.7 Retain audit trail for at least one year	• DS 5.5 Security Testing, Surveillance and Monitoring	• 164.308 (a)(1)(ii)(D) Information System Activity Review • 164.308 (a)(6)(i) Login Monitoring • 164.312 (b) Audit Controls
Alert Logic Threat Manager™	• 5.1.1 Monitor zero day attacks not covered by anti-virus • 6.2 Identify newly discovered security vulnerabilities • 11.2 Perform network vulnerability scans quarterly by an ASV or after any significant network change • 11.4 Maintain IDS/IPS to monitor and alert personnel; keep engines up to date	• DS5.9 Malicious Software Prevention, Detection and Correction • DS 5.6 Security Incident Definition • DS 5.10 Network Security	• 164.308 (a)(1)(ii)(A) Risk Analysis • 164.308 (a)(1)(ii)(B) Risk Management • 164.308 (a)(5)(ii)(B) Protection from Malicious Software • 164.308 (a)(6)(iii) Response & Reporting
Alert Logic Security Operations Center providing Monitoring, Protection, and Reporting			

Stopping Imminent Data Theft

Customer Type: Retail
Threat Type: Advanced SQL Injection

COMPROMISE ACTIVITY
Discovered through inspection of 987 log messages indicative of a SQL injection attack

8 min

INCIDENT ESCALATION
Partner and customer notified with threat source information and remediation tactics

FUTHER ANALYSIS
Alert Logic Analyst confirms user IDs and password hashes leaked as part of initial attack

2 hours

6 hours

EXFILTRATION ATTEMPT PREVENTED
Partner works with customer to mitigate compromised accounts

Thank you.

ALERT LOGIC®