Ransomware

A case study of the impact, recovery and remediation events

Peter Thermos
President & CTO
Tel: (732) 688-0413
peter.thermos@palindrometech.com

Palindrome Technologies
100 Village Court
Suite 102
Hazlet, NJ 07730
www.palindrometech.com

Palindrome Technologies

Assurance, Trust, Confidence

Agenda

- Incident Events
- Detection, analysis containment of the threat
- Threat Remediation
- About Palindrome

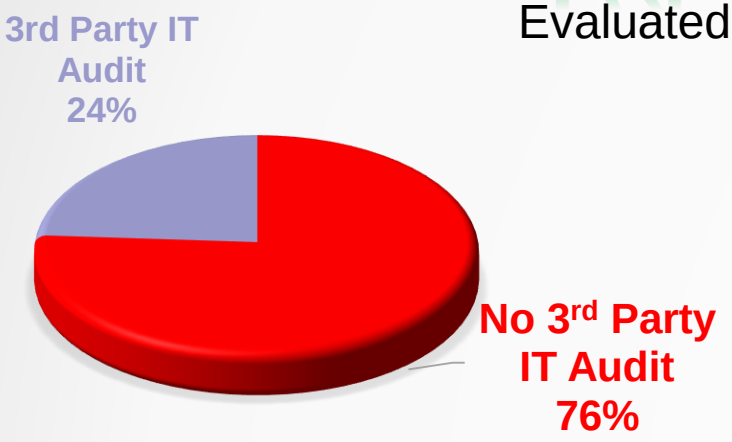
NJ Statistics on Cyber Security

"Cybersecurity is hardly the only area that governments need to consider as they try to cut down on technological risk"… Ref: M. Pheiffer, Rutgers University Nov. 2015, Study on NJ Municipalities and Cybersecurity

565
Local Governments

174
Evaluated

- 9 local governments have data breach policy
- Only 56 have performed any sort of strategic planning
- 30 local governments commissioned third-party audit and/or intrusion testing



Its 10pm, do you know where your data breach policy is?

Events

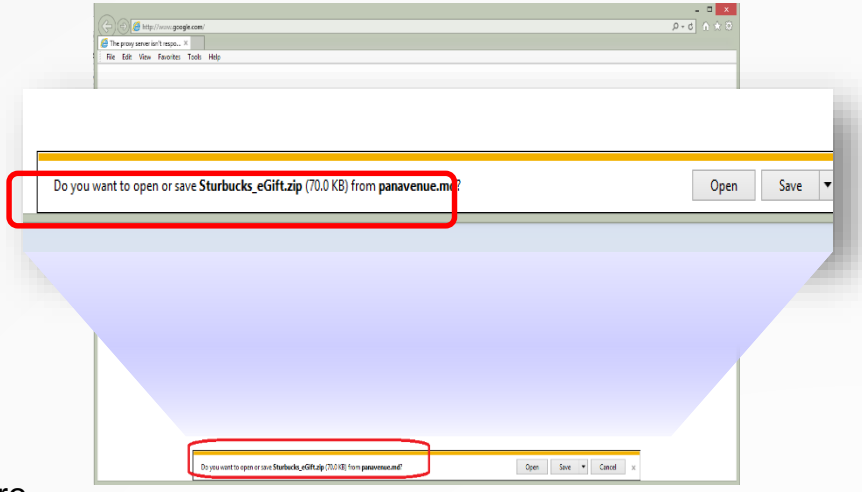
The steps to contain and recover from attack and also institute a vulnerability and threat management program.

Detection	Analysis and containment	Recovery	Remediation
a) Event detected by Municipality IT b) Impacted critical servers and workstations	a) Palindrome engaged b) Performed server and network traffic forensics c) Determined that a user's workstation was infected **d) Attack vector**: Phishing email e) Workstation Antivirus not updated	a) IT team recovered affected files from backups b) Enhanced firewall filters c) Performed Vulnerability Assessment & penetration testing d) Developed a Remediation Plan	a) Addressed vulnerabilities identified from penetration testing (patches, host/WiFi configuration, network controls) b) Deployment of SIEM • Network/Host monitoring • Vulnerability Management c) Awareness Training

Attack

User receives “promotional” email

Email contains a link to a file containing the ransomware



URL Downloads a .zip file that contains malware !!!

Once the user downloads and opens the file they get infected

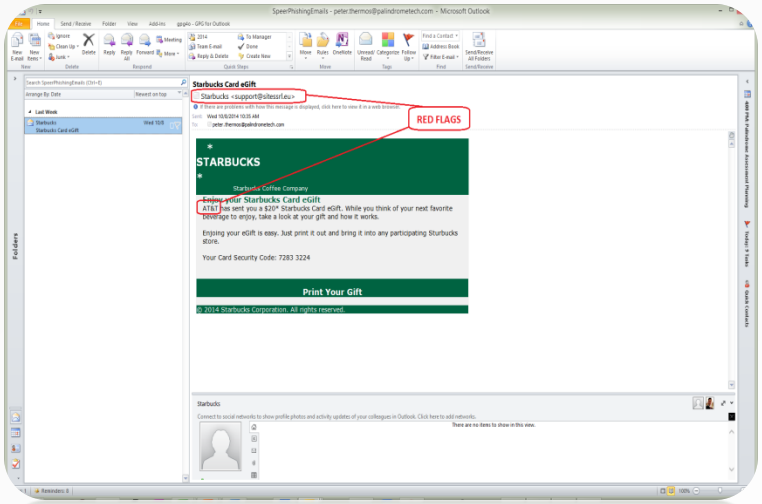
The ransomware silently propagates to local drive and network shares!

Within 1 hour of attack the infection propagated on domain servers and started encrypting files

Tuesday 9:00AM - Users cant access files on critical servers

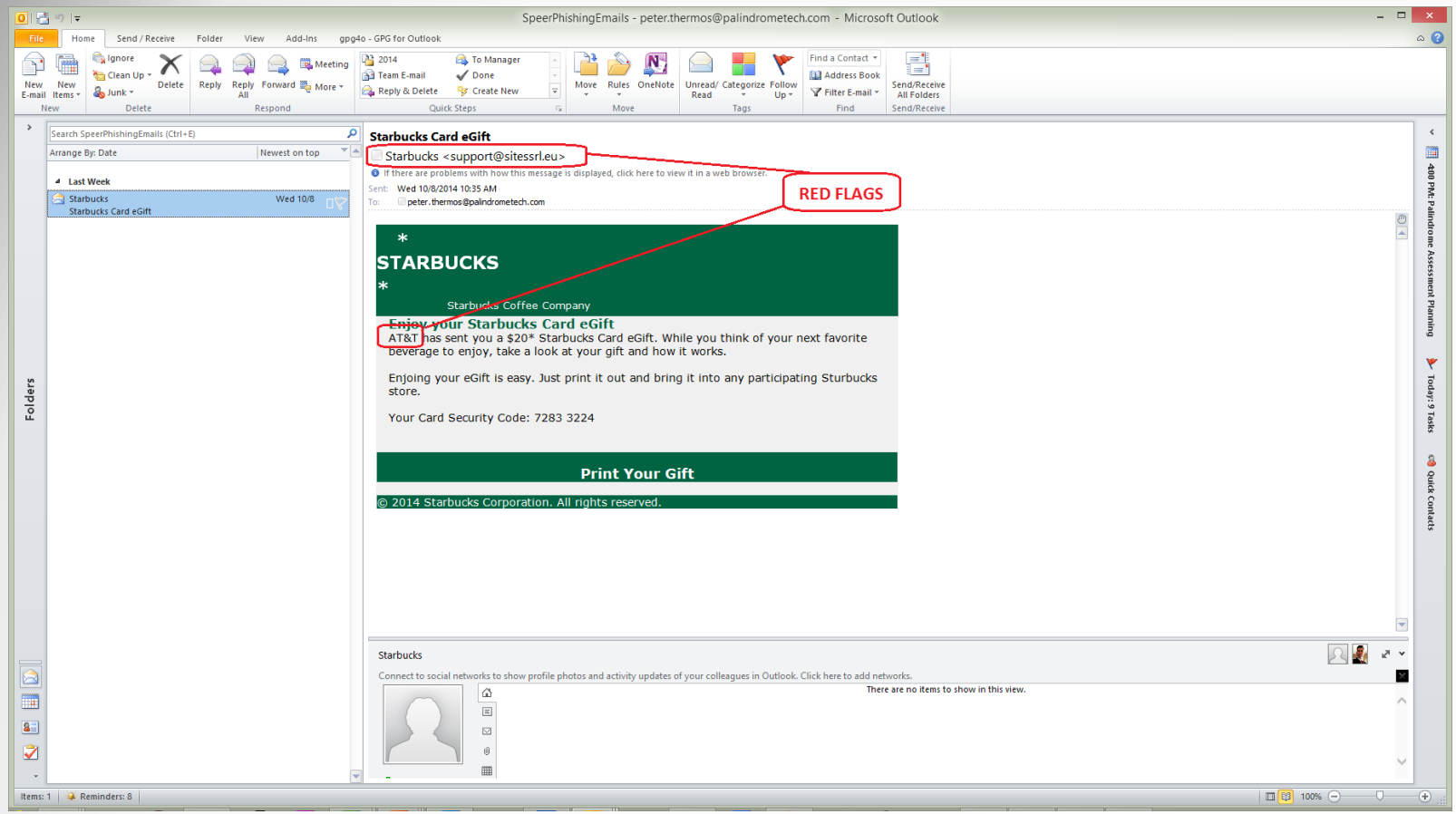
Email spear-Phishing Attack Overview

- The attacker may:
  - Address the recipient by name
  - Use lingo/jargon of the organization
  - Reference actual procedures or instructions that the user is familiar

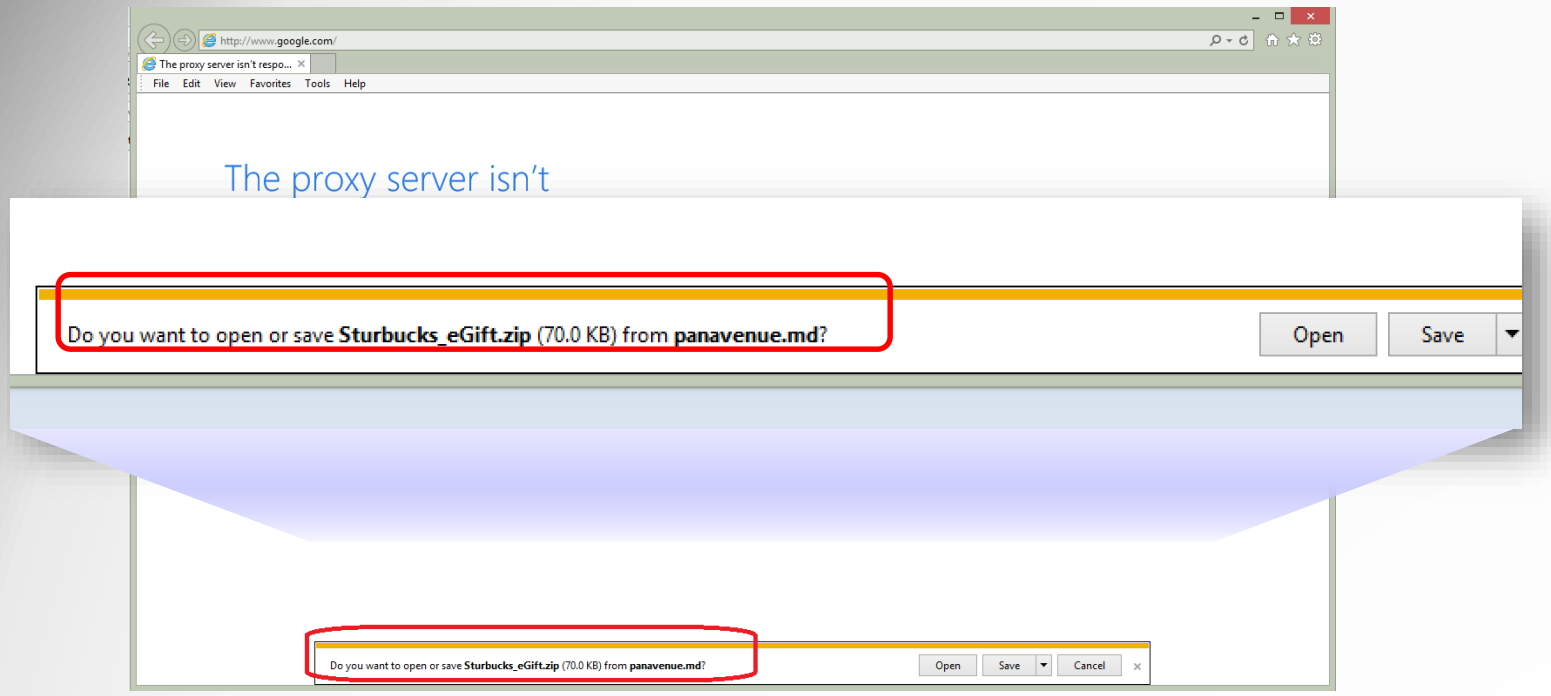


- The email appears to be genuine.
- Sometime these emails have legitimate operational and exercise nicknames, terms, and key words in the subject and body of the message.

Phishing Example

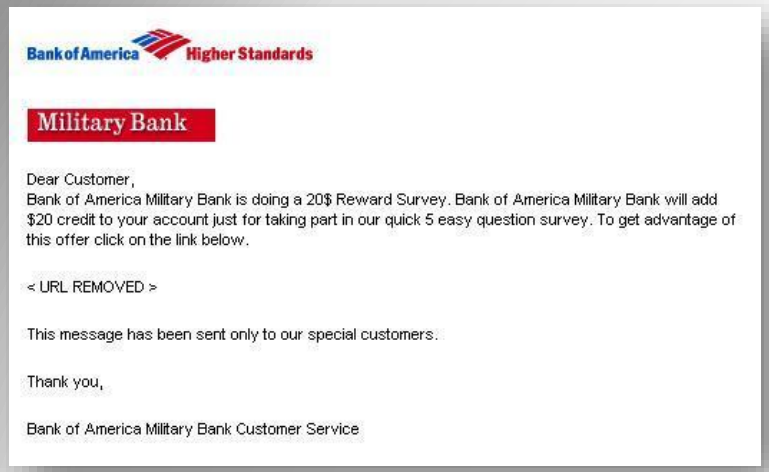


Malware/Ransomware through Phishing



URL Downloads a .zip file that contains malware !!!

Additional email Phishing Examples



Bank of America Higher Standards

Military Bank

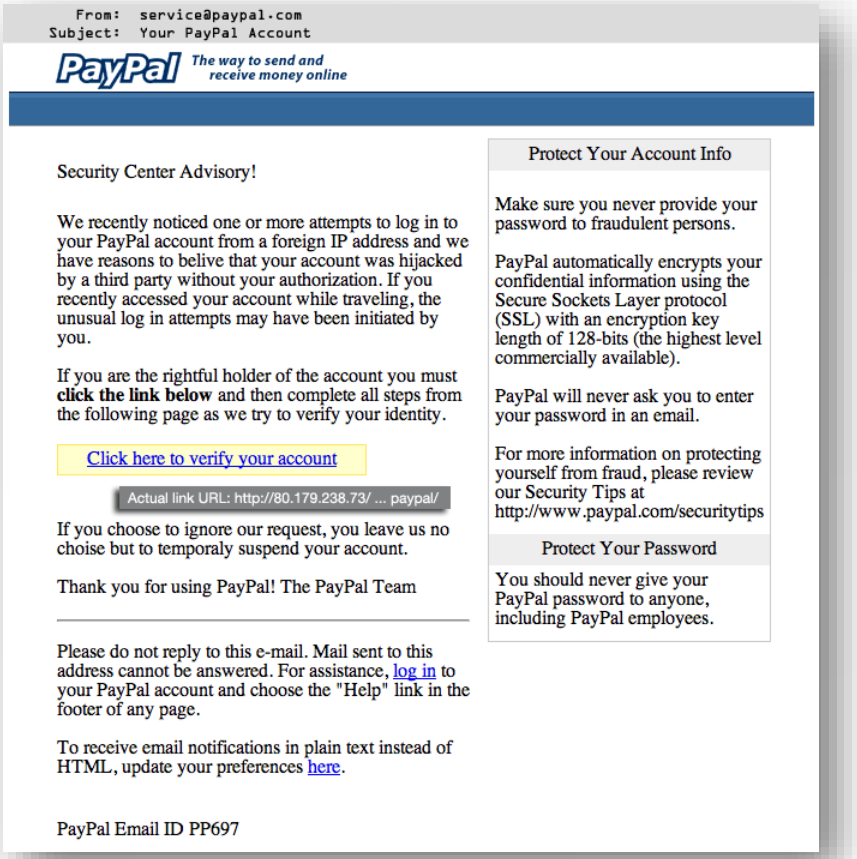
Dear Customer,
Bank of America Military Bank is doing a 20$ Reward Survey. Bank of America Military Bank will add $20 credit to your account just for taking part in our quick 5 easy question survey. To get advantage of this offer click on the link below.

< URL REMOVED >

This message has been sent only to our special customers.

Thank you,

Bank of America Military Bank Customer Service



From: service@paypal.com
Subject: Your PayPal Account

PayPal The way to send and receive money online

Security Center Advisory!

We recently noticed one or more attempts to log in to your PayPal account from a foreign IP address and we have reasons to belive that your account was hijacked by a third party without your authorization. If you recently accessed your account while traveling, the unusual log in attempts may have been initiated by you.

If you are the rightful holder of the account you must **click the link below** and then complete all steps from the following page as we try to verify your identity.

Click here to verify your account

Actual link URL: http://80.179.238.73/ ... paypal/

If you choose to ignore our request, you leave us no choise but to temporaly suspend your account.

Thank you for using PayPal! The PayPal Team

Please do not reply to this e-mail. Mail sent to this address cannot be answered. For assistance, log in to your PayPal account and choose the "Help" link in the footer of any page.

To receive email notifications in plain text instead of HTML, update your preferences here.

PayPal Email ID PP697

Protect Your Account Info

Make sure you never provide your password to fraudulent persons.

PayPal automatically encrypts your confidential information using the Secure Sockets Layer protocol (SSL) with an encryption key length of 128-bits (the highest level commercially available).

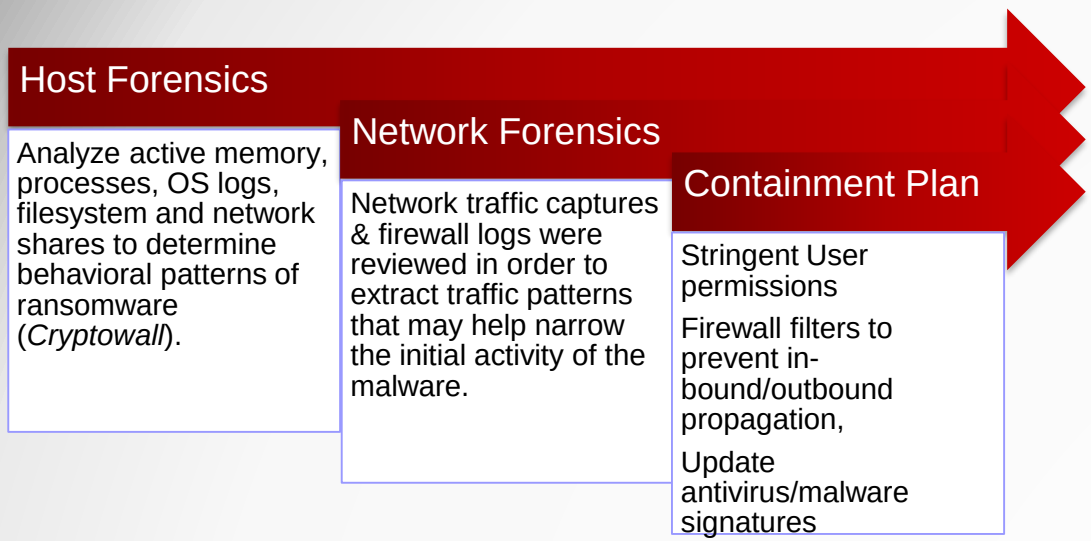
PayPal will never ask you to enter your password in an email.

For more information on protecting yourself from fraud, please review our Security Tips at http://www.paypal.com/securitytips

Protect Your Password

You should never give your PayPal password to anyone, including PayPal employees.

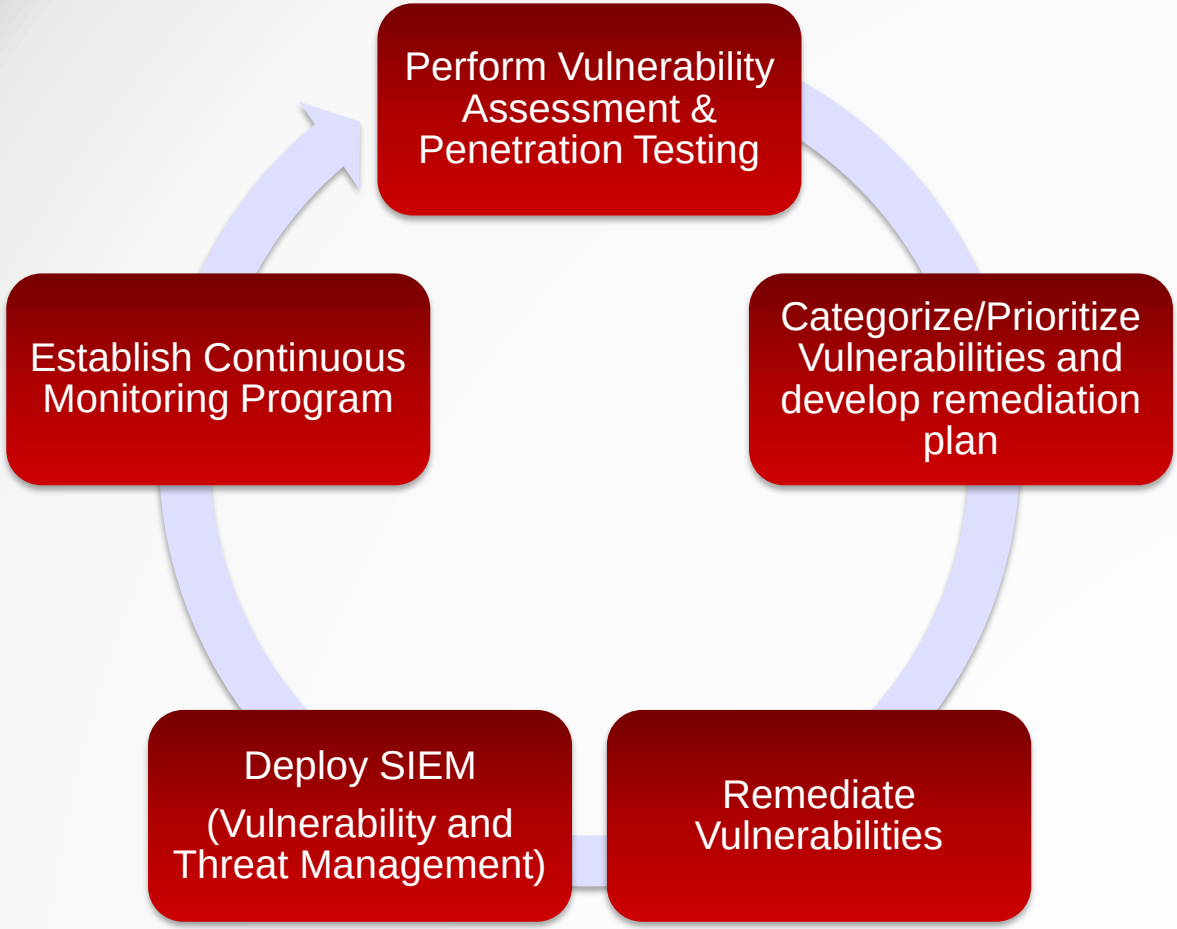
Analysis, containment, recovery



Recovery

- Examine and validate if most recent backup reference is infected
- Restore data from backup prior to infection
- Prepare remediation strategy
- Hosted awareness training

Threat Remediation



About Palindrome

Professional Services

- Information Security and Assurance
- Vulnerability Assessments
- Penetration Testing
- Risk and Threat Analysis
- Security Policy
- Architecture Review
- Forensics
- Incident Response
- Governance
- Compliance
- Disaster Recovery Planning

Managed Services

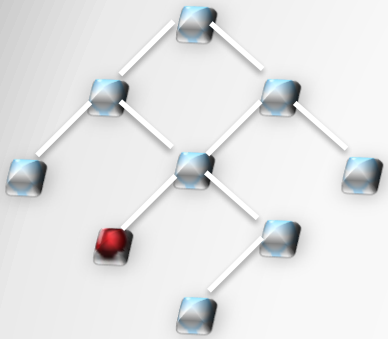
- SIEM
- Alerting
- Event Correlation
- Log Normalization
- User Monitoring
- Malware Detection

Mobile Security Solutions

- Recap Mobile Security Vulnerability and Threat Management

Managing Cyber Threats
Managed Services

- **Security Information and Event Management**
  - Log analysis
  - Linked to the intrusion detection and incident response plan



Alerting - Configure and receive automatic alerts based on customized event thresholds.

Event Correlation - Multiple forms of event correlation are available for all events including statistical anomalies, associating IDS event with vulnerabilities, and alerting on 'first time seen' events.

Log Normalization - Normalize, correlate, and analyze user and network activity from log data generated by any device or application across the enterprise in a central portal.

User Monitoring - Monitor user activity. Associate events such as a NetFlow, IDS detection, firewall log activity, file access, system error, or login failure with specific users for easy reporting and insider threat detection.

Malware Detection - monitors all processes running on Windows machines for malware processes, and can alert the security team if malware is discovered.

Q & A

Palindrome Technologies

Peter Thermos , MSc
President & CTO

Cell: +1(732) 688-0413
Peter.thermos@palindrometech.com

100 Village Court
Hazlet, NJ 07730
USA
www.palindrometech.com

Palindrome Technologies

Chris Reid
SIEM/MSS

Cell: +(732) 841-5047
Chris.reid@palindrometech.com

100 Village Court
Hazlet, NJ 07730
USA
www.palindrometech.com

Assurance, Trust, Confidence