CYBER-RESILIENT APPLICATIONS

Andy Waterhouse
EMEA Presales Director

Twitter : @Andy_J_W
AGENDA

- What is Cyber Resilience?
- What applications and application infrastructure can we protect
- How do we create Cyber Recovery Solutions
- What about emerging / cloud applications
- How do we protect by detecting earlier?
What is a Cyber Resilient Application?

Should we ask application developers to be aware of cyber threats
- If so, which threats? Just attacks on data?
- How do we tell applications about infrastructure-level attacks

How do we make existing applications more resilient
- Huge amounts of money invested in traditional applications
- Too risky and too costly to re-write / re-architect
- What about old / static platforms like OT?

How do we handle embedded applications
- IoT, sensors, …, etc.

The reality is that there is no single approach that we can take
- We need to understand how to manage our digital risk
- Then we can understand our approach to cyber resilience
Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don’t waste your time. Nobody can recover your files without our decryption service.

We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:
   
   1Mz7153HuXTuRaR21t74mGSdzaAtNbBWX

2. Send your Bitcoin wallet ID and personal installation key to e-mail wowsmith123456@posteo.net. Your personal installation key:

   74f296-2Nx1Gm-yHQRWr-S8gAN6-8Bsltd-U2DKui-2ZpKJE-kE6sNM-o8tizU-gUeUMa

If you already purchased your key, please enter it below.

Key: _
## Current State: Risk Profile Summary

<table>
<thead>
<tr>
<th>Technical</th>
<th>People &amp; Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>✷ All data is currently susceptible to a cyber attack</td>
<td>✷ IT Engineering and Ops have access to most if not all Backup Assets</td>
</tr>
<tr>
<td>✷ Primary storage replication can replicate corruption</td>
<td>✷ Security teams not assigned to assets. Bad actors inside the firewall can create havoc.</td>
</tr>
<tr>
<td>✷ Backup catalog not replicated</td>
<td>✷ Franchise critical and non-critical data are not segregated</td>
</tr>
<tr>
<td>✷ Recovery of backup catalog from tape is slow and failure prone</td>
<td>✷ Backup images can be expired without authorization</td>
</tr>
<tr>
<td>✷ Backup copies not isolated from network</td>
<td></td>
</tr>
</tbody>
</table>

- These risks are consistent with traditional Prod/DR models.
- This is a **different challenge** and requires a different architecture.
Traditional Strategies Are Not Enough

**Data Encryption**
Not preventative against attacks
Hacktivists can encrypt your encrypted data
For data protection, not recovery
Potential negative impacts on cost to store, replicate and protect

**Tape Backups**
Too long to recover
Difficult to validate data
Requires backup infrastructure to recover
May not protect:
Backup Catalog
PB Backup Appliances
Tape Library Meta Data DB

**Cyber Insurance**
All breaches may not be covered
Policies have baseline security requirements
Monetary limits may not cover all damages
Does not protect:
Patient needs
Brand
Lost trust
## Disaster Recovery ≠ Cyber Recovery

<table>
<thead>
<tr>
<th>Category</th>
<th>DR</th>
<th>CR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recovery Time</td>
<td>Close to Instant</td>
<td>Reliable &amp; Fast</td>
</tr>
<tr>
<td>Recovery Point</td>
<td>Ideally Continuous</td>
<td>1 Day Average</td>
</tr>
<tr>
<td>Nature of Disaster</td>
<td>Flood, Power Outage, Weather</td>
<td>Cyber Attack, Targeted</td>
</tr>
<tr>
<td>Impact of Disaster</td>
<td>Regional; typically contained</td>
<td>Global; spreads quickly</td>
</tr>
<tr>
<td>Topology</td>
<td>Connected, multiple targets</td>
<td>Isolated, in addition to DR</td>
</tr>
<tr>
<td>Data Volume</td>
<td>Comprehensive, All Data</td>
<td>Selective, Includes Foundation SVCs</td>
</tr>
<tr>
<td>Recovery</td>
<td>Standard DR (e.g. failback)</td>
<td>Iterative, selective recovery; part of IR</td>
</tr>
</tbody>
</table>
The Most Critical Data First

- Protect the “heartbeat” of the business first
- Prioritize top applications or data sets to protect
- Usually less than 10% of data
- Start with a core set and build from there
Cyber Recovery Solutions

- Create backup of data
- No management connectivity to IR Vault
- Enable data link and replicate to isolated system
- Complete replication and disable data link
- Maintain WORM locked restore points
- Optional security analytics on data at rest
- Professional Services
Separate Copy Streams For Better Recovery

- Distribution Mgmt.
  - Clean Room: Vendor Distros, Material For IR Vault
  - Change Control Process
  - Backup Process

- Data Domain
  - Change Control Copy
  - Daily Backup
  - DD MTTree Replication

- Cyber Recovery Vault
  - OS
  - DD MTTree Replication
ICS THREATS

- Northeast Blackout 20023
- Worcester ATC Attack
- Zotob
- CSX Train Signaling System
- Stuxnet
- Shamoon
- Maroochy Shire Sewage Spill
- Kemuri Water Company
ICS / OT

- **Challenges**
  - Large numbers of unpatched / un-patchable systems
  - Many systems running unsupported software versions
  - Inability to make any system changes
  - Huge risk to operational capabilities

- **Approach**
  - Deploy detect & respond technology onto endpoints
  - Detail the risk associated with each primary component and create a mitigation plan
  - Use evolved SIEM to protect network access
A Different Strategy for the Endpoint

Detect by threat behavior rather than by signature

Intelligent Scoring System for Risk

A Force Multiplier for Security Analysts & IR

More rapidly expose new, unknown, targeted and non-malware threats on endpoints

Eliminate white noise; prioritize threats more efficiently & accurately

Quickly understand and confirm the full scope of an attack to accelerate response actions
New Architecture For IoT Digital Transformation
Making things smarter across the IoT ecosystem

Edge
- Edge Analytics
  - Push Insights from the Edge

Core
- Machine Learning
  - Pull Insights from the Cloud

Cloud
- Deep Learning
**Problem Statement:** Rapid increase in IoT endpoints significantly increases the enterprise threat surface

**Hypothesis:** Securing only the “thing” will not scale in long-term
- Massive scale: complex and inefficient
- Embedded: hard to secure
- Brownfield: limited flexibility
- Constrained devices: limited power/compute

**Strategy:** Start with IoT gateways and expand from there
- Use gateway as a foundation for monitoring connected devices
- Leverage analytics & machine learning
  - Profile/Classify devices
  - Monitor devices for anomalous behavior
  - Detect threats/attacks
**IRIS 3 MAIN COMPONENTS:**

<table>
<thead>
<tr>
<th>Iris Container</th>
<th>Iris Cloud</th>
<th>Logstash</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Simple information gathering container</td>
<td>1. Azure hosted free SaaS service</td>
<td>1. Logstash integration to NetWitness Logs</td>
</tr>
<tr>
<td>2. Leverages Docker host to gather information about other containers in the same environment</td>
<td>2. Provides Registration and enablement</td>
<td>2. Enables integration across other platforms</td>
</tr>
<tr>
<td>3. Packages up and securely transmits to Iris Cloud.</td>
<td>3. Advanced Behavioral Analytics and AI techniques for threat detection</td>
<td>3. Conveys alerts and associated meta data</td>
</tr>
<tr>
<td>4. Works with EdgeX and Azure IoT Edge today…</td>
<td>4. Alerts Dashboard for easy threat inspection</td>
<td></td>
</tr>
</tbody>
</table>
Platform Architecture

“NORTHBOUND” INFRASTRUCTURE AND APPLICATIONS

EXCHANGE SERVICES

CLIENT REGISTRATION
DISTRIBUTION
ADDITIONAL SERVICES

SUPPORTING SERVICES

RULES ENGINE
SCHEDULING
ALERTS & NOTIFICATIONS
LOGGING
ADDITIONAL SERVICES

CORE SERVICES

CORE DATA
COMMAND
METADATA
REGISTRY & CONFIG

DEVICE SERVICES (ANY COMBINATION OF STANDARD OR PROPRIETARY PROTOCOLS VIA SDK)

REST
OPC-UA
MODBUS
BACNET
ZIGBEE
BLE
MQTT
SNMP
VIRTUAL
ADD'L DEVICE SERVICES

“SOUTHBOUND” DEVICES, SENSORS AND ACTUATORS

“ADDITIONAL SERVICES

CONTAINER DEPLOYMENT

LOCAL MGMT CONSOLE

ADDITIONAL SERVICES

IRIS Agent
WHAT IS COLLECTED?

- Service metadata
  - e.g. id, name, status, open ports, volumes
- Network flow (Netflow) data:
  - Source & Destination IP/port/protocol
  - Byte & packet counts
- Process data
  - Process attributes (e.g. process ids, effective user, group, %cpu, %mem)
  - Real-time process creation and termination events
- Service resource consumption
  - Network I/O, CPU usage, Memory usage
- Service events
  - e.g. Stop, start, die, kill, exec_create
WHAT IS DETECTED?

− Current: Focused on the gateway
  • Initial infection
  • Command & control
  • Lateral movement
  • Data exfiltration
  • Denial of service

− Planned: Expand to cover compromised devices
  • Anomalies in device sensor data
  • Anomalies in device network behavior
DETECTING COMPROMISED DEVICES

• Assume the data is generated by some natural distribution such as Uniform, Gaussian, Exponential, Beta, Gamma, etc., or a mixture of distributions such as GMM.

• Fit the data onto the distribution and determine the parameters of the model.

• Given a new reading find how probable it is to belong to the distribution.

• Report on anomalous events.

PROJECT IRIS

{DeviceID A on a TimeStamp:T had an anomalous ReadingValue: R}
USER AND ENTITY BEHAVIOUR ANALYSIS
WHAT IS UEBA?

- **Data Ingest**
- **Unified Metadata Taxonomy**
- **Native Data Collection**
- **Unified Behavioral Baseline**
- **Analytics**
- **Anomaly Detection**
- **Behavioral Modeling**
- **Alert Correlation**
- **Risk Score & Priority**
- **Enriched User Context**
- **Unsupervised Machine Learning**
- **Anomalies Investigation**
- **Use Case Focused**
WHY USE UEBA?

- DETECT ANOMALIES

- MULTI-TIERED UNSUPERVISED MACHINE LEARNING
- AUTONOMOUS TUNING
- RECURSIVE PATTERN RECOGNITION
- STANDARD DEVIATIONS
- NEW OCCURRENCES
- BEHAVIORAL OUTLIERS
- DATA AGGREGATION FRAMEWORK
- MULTIVARIATE ANALYSIS
- ROBUST AND COMPREHENSIVE
- ADAPTIVE ALERT PRIOTIZATION
- STREAMLINED INVESTIGATION

- ADVANCED CORRELATION
- ADVANCED CORRELATION

- SEAMLESS ANOMALY EXPLORATION
WHY USE UEBA?

- USER ANALYSIS

**TIME BASED MODEL**

- Unix timestamp = 1491988104
- ISO 8601 = 2017-04-12T09:08:24+00:00
- RFC 2822 = Wednesday, 12-Apr-17 09:08:24 UTC

**CONTINUOUS MODEL**

- Computers accessed = 23
- Failed logons = 144
- Files copied = 6544

**CATEGORICAL MODEL**

- Application = outlook.exe
- Computer name = pc1
- Country = nz

**GLOBAL MODEL**

- Computer name = pc1
- Failed logons = 144
- Files copied = 6544

**AUTHENTICATION TIME ANOMALY**

**FILE ACCESS TIME ANOMALY**

**AD CHANGE TIME ANOMALY**

**HIGH NUMBER OF FILES ACCESSED**

**HIGH NUMBER OF AD CHANGES**

**HIGH NUMBER OF FAILED LOGONS**

**SOURCE COMPUTER ANOMALY**

**FOLDER ACCESS ANOMALY**

**SERVER ACCESS ANOMALY**

**NOISY FEATURE REDUCTION**

**RARITY REDUCTION**

**CERTAINTY REDUCERS**
ANOMALY DETECTION (CONT.)

- CONNECTING THE DOTS. LITERALLY.

User: Martin Brenner

- Raw events
- Threat indicators
- Correlated SMART alert

Correlated SMART alert score = 15
## EVOLVED SIEM PLATFORMS

<table>
<thead>
<tr>
<th>SIEM 1.0</th>
<th>SIEM 2.0</th>
<th>Evolved SIEM (3.0)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log-centric SIEM</td>
<td>Log-centric SIEM</td>
<td>Log-centric SIEM</td>
</tr>
<tr>
<td>Compliance Focused</td>
<td>Security Focused; Bolted On</td>
<td>Endpoint Detection &amp; Response</td>
</tr>
<tr>
<td></td>
<td>Network Forensics</td>
<td>Network Forensics</td>
</tr>
<tr>
<td></td>
<td>UEBA</td>
<td>UEBA</td>
</tr>
<tr>
<td></td>
<td>Workflow &amp; Case Management</td>
<td>Threat Intelligence</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Orchestration &amp; Automation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Security Focused; Modular and Integrated</td>
</tr>
</tbody>
</table>
AUTHENTICATION

A technical control
A single data point
Ineffective without context

IDENTITY ASSURANCE

Who is the user?
How confident are you?
How much assurance is required?
ANY USER, ANYWHERE, ANY DEVICE

Who can access?
What can they access?
Where can they access?

Secure Access Control
Convenient Single Sign-On

SAML / WS-FED
Password Vaulting
Reverse Proxy
IWA

HUNDREDS OF APPLICATIONS ON-PREM AND IN THE CLOUD
IDENTITY ACCESS CAPABILITIES

Pervasive MFA
Connect to anything

Modern MFA Methods
Easy & convenient

Risk-based Authentication
Access in context

Assurance Levels
Challenge according to the level of risk

Risk-based Authentication
Role
Threats
Device
Location
Behavior
App

Security
Risk
Low
Medium
High

Pervasive MFA
Connect to anything

Modern MFA Methods
Easy & convenient

Risk-based Authentication
Access in context

Assurance Levels
Challenge according to the level of risk

Risk-based Authentication
Role
Threats
Device
Location
Behavior
App

Security
Risk
Low
Medium
High

Pervasive MFA
Connect to anything

Modern MFA Methods
Easy & convenient

Risk-based Authentication
Access in context

Assurance Levels
Challenge according to the level of risk

Risk-based Authentication
Role
Threats
Device
Location
Behavior
App

Security
Risk
Low
Medium
High

Pervasive MFA
Connect to anything

Modern MFA Methods
Easy & convenient

Risk-based Authentication
Access in context

Assurance Levels
Challenge according to the level of risk

Risk-based Authentication
Role
Threats
Device
Location
Behavior
App

Security
Risk
Low
Medium
High

Pervasive MFA
Connect to anything

Modern MFA Methods
Easy & convenient

Risk-based Authentication
Access in context

Assurance Levels
Challenge according to the level of risk

Risk-based Authentication
Role
Threats
Device
Location
Behavior
App

Security
Risk
Low
Medium
High

Pervasive MFA
Connect to anything

Modern MFA Methods
Easy & convenient

Risk-based Authentication
Access in context

Assurance Levels
Challenge according to the level of risk

Risk-based Authentication
Role
Threats
Device
Location
Behavior
App

Security
Risk
Low
Medium
High
SUMMARY

- Traditional apps cannot be easily redesigned for resilience
  - Need to use effective cyber recovery solutions
- ICS /OT environments need risk mapping and a secure solution
- IoT needs scalable and embedded security
- UEBA and machine learning will help us spot the needle in the haystack
- Use an Identity management platform with a risk engine
  - People are the weakest link in applications
- Our approach to cyber resilience is about managing digital risk
QUESTIONS?
THANK YOU!

Andy Waterhouse
EMEA Presales Director

Twitter : @Andy_J_W