# CSN15: Using Whitelist Security with ArcSight ESM to Prevent Targeted Attacks and APTs

**Tracy Herriotts, Johns Hopkins University**
**Harry Sverdlove, Bit9**

JOHNS HOPKINS UNIVERSITY

Bit9

# Agenda

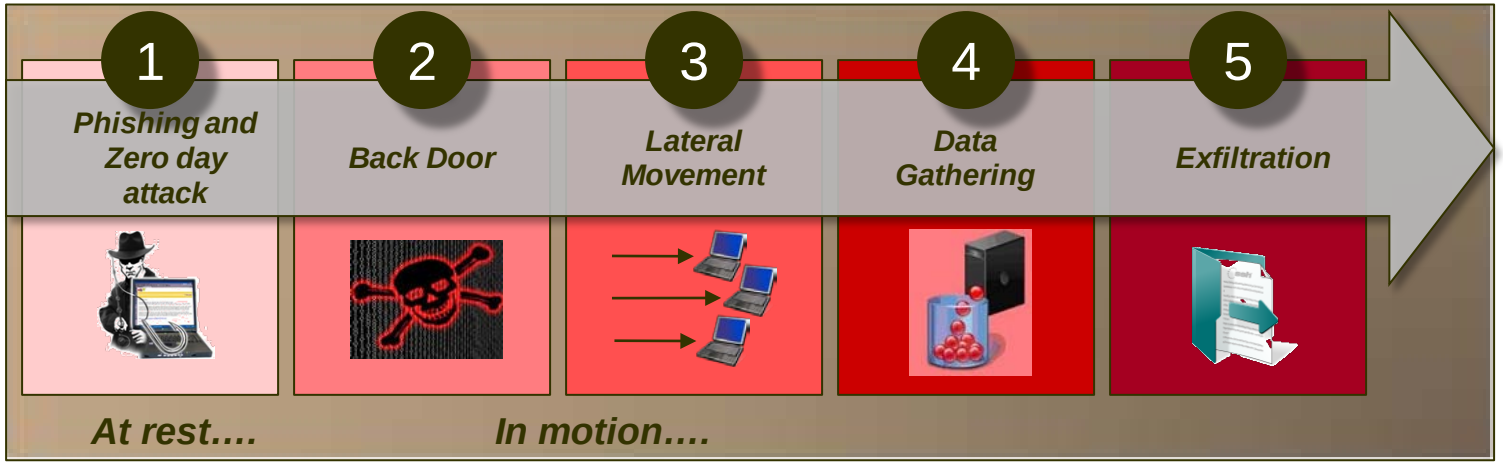
- Background
- Problem Statement
- ArcSight ESM Configuration
- Increasing Defense in Depth with Endpoint Sensor
- Use Cases and Benefits
- Reducing Time to Investigate
- Wrap up / Questions

# Background

- Bit9 was Pilot Award winner at the 2010 American Security Challenge, sponsored by ArcSight
- Identified The John Hopkins University as a key joint customer and thought leader in the cyber security arena
- Pilot launched in early 2011
- Identify integrations points between Bit9 Parity and ArcSight ESM
- Prove value of combining these technologies at the SOC
- One step in advancing cyber defense capabilities – more to come

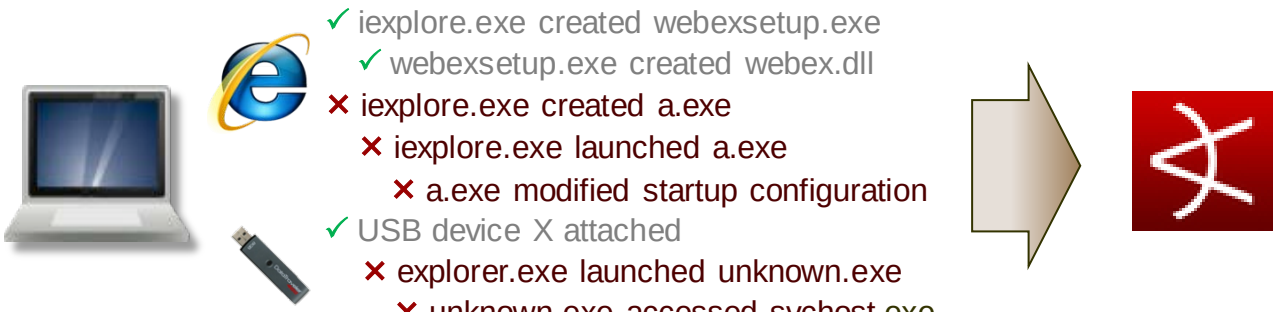
# Challenges

- ArcSight SIEM is only as good as the data being fed into it
- Most data today comes from network sensors (IDS/IPS/FW)
- Can only detect threats when they are active on the wire or “in motion”
- Most advanced attacks come through, and reside on, an endpoint
- Traditional AV can only detect known threats or malware
- The endpoint is a blind spot to the ArcSight SIEM



# Providing Better Threat Indicators

- **Whitelisting technology provides deeper near real-time visibility into endpoint activity (in addition to proactive defensive capabilities)**
- **In this context, the whitelist is a means to filter out noise**
- **Visibility into all unapproved file and process activity, and targeted configuration and memory activity**
- **Data is available even if malware removes its tracks**
- **Reputation services can augment filters with threat and trust indicators**

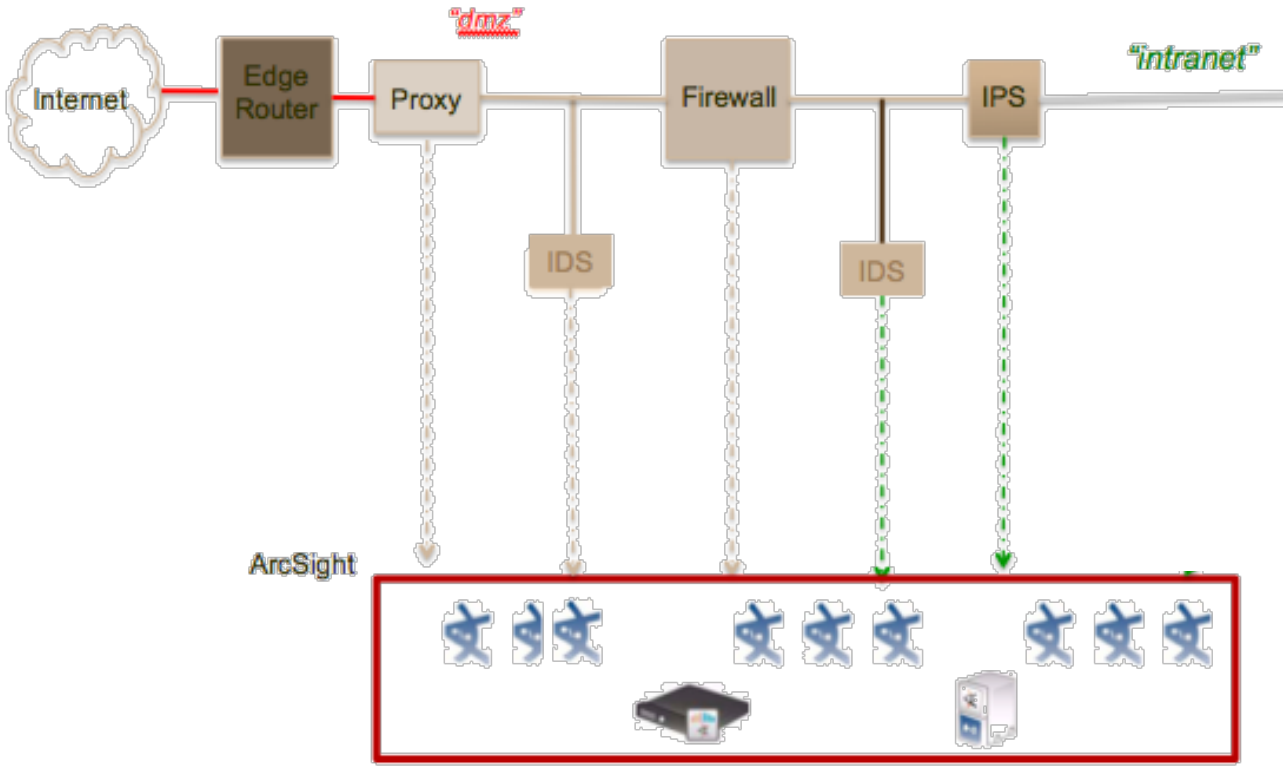


# About Johns Hopkins

- **Dynamic, open culture, environment**
  - Thousands of research and development systems
  - Critical information systems and sensitive data
- **Under constant attack by advanced and persistent threats**
- **Hundreds of millions of events enter the SOC every day**
  - After basic filtering, still managing tens of millions of events every day
- **Limited security staff to manage large set of resources**
  - Must prioritize and triage to focus on highly suspicious activity
- **In short, we are just like you**

# ArcSight Configuration

**Typically ArcSight ESM is processing events from Network: FW, IDS, IPS**



# What Bit9 Provides

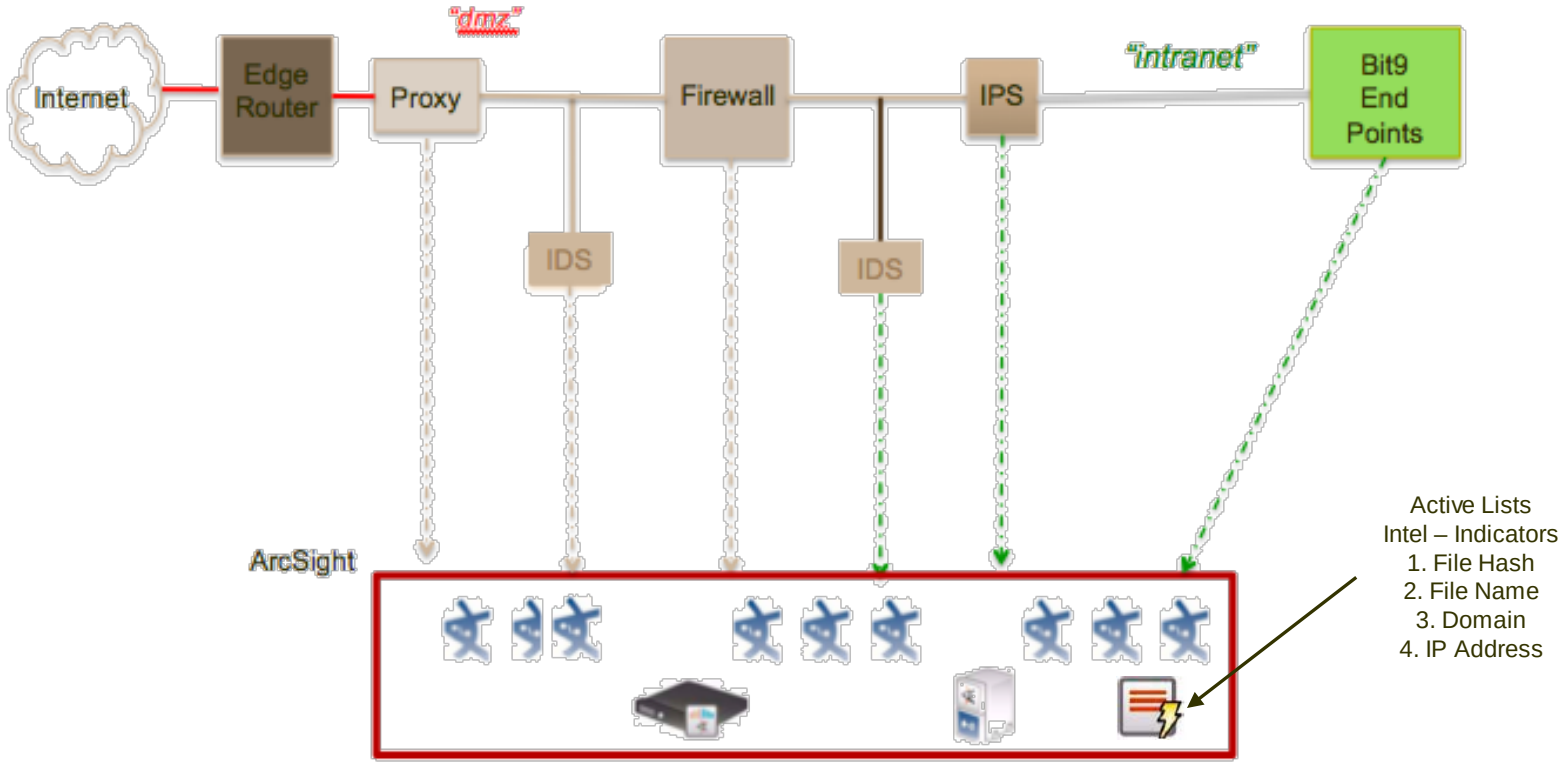
- **How many Bit9 event types are there?**
  - 240 Event Types
  - Over 300k events per day in our environment
- **Which Bit9 events can be used for InfoSec?**
  - 9 Event Types
  - 35 events per day in our environment
- **Which events are significant / stand on their own?**
- **Which events can be correlated with other Bit9 events?**
- **Which events can be correlated with other security devices?**

# Insight Gained from Endpoint Events

- **New File Detection**
  - First on network, endpoint, method of delivery
- **File Categorization**
  - New/pending, potential risk, malicious
- **Endpoint Actions**
- **Correlate Endpoint Activity**
  - Intelligence Indicators and blocked outbound activity
- **Detect Parity Tampering by Potential Risks**

# Increasing Defense in Depth

**Endpoint activity can be correlated by ArcSight ESM with FW, IDS, IPS, and Intelligence Indicators**



# Bit9 InfoSec Events

| Event ID | Message | Description | Significance |
|---|---|---|---|
| 1201 | Malicious file detected | File with high threat has been detected based on Bit9 software reputation service | Standalone |
| 1200 | Potential risk file detected | Potentially unwanted file has been detected based on Bit9 software reputation service | Standalone |
| 1004 | Banned file written to computer | Explicitly blocked file (name and/or hash) detected. [active process, installer, …] | Standalone |
| 802 | Execution block (banned file) | Explicitly blocked file attempted execution. | Standalone |
| 1009 | Device attached | USB with file system attached. [vendor, device] | Correlate |
| 1003 | New pending file to computer | Unapproved file detected. [file, hash, installer, …] | Correlate |
| 1007 | First execution on network | Never before seen file executed. [file, hash, installer, …] | Correlate |
| 800 | Tamper protection blocked | Attempt to stop security service, or modify/delete files or configuration. [user, process, …] | Correlate |
| 305 | Multiple failed logins | Three consecutive login failures | Standalone |
| *[Future]* | Registry / memory / file traps | Specific traps can be defined on any file, registry or cross process memory activity | Standalone |

# Bit9 Event Fields

- **Time**
- **Event ID / Class / Name**
- **Message**
- **Target Hostname, IP Address**
- **Target Security Policy**
- **User Name**
- **Process Name**
- ***File related events:***
  **File Path, Filename, Hash, Installer Filename / Hash**
- ***USB Device events:***
  **Vendor, Device Name**

| ArcSight Field | Bit9 |
|---|---|
| time | - |
| Device Event Class ID | 1004 |
| Name | Banned file written to computer |
| Message | Computer A7 wrote new banned file 'c:\documents and settings\a7\desktop\test.bat' |
| Device Custom String3 | Global_BlockAndAsk_3030 |
| File Name | test.bat |
| File Hash | [49bfe618a1c7e…] |
| Target Process Name | c:\windows\explorer.exe |
| Device Custom String2 | winword.exe |
| File Path | c:\documents and settings\a7\desktop\test.bat |
| Target Host Name | a7 |
| Target User Name | tracy |
| Target Address | 192.168.67.7 |
| Device Event Category | Discovery |
| Device Vendor | Bit9 |
| Device Product | Parity |
| destination host/domain | n/a |
| destination address | n/a |

# Bit9 Correlation with Other Devices

| Description | ids1 | fw | ips | ids2 | dns | av | intel | Bit9 |
|---|---|---|---|---|---|---|---|---|
| time | • | • | • | • | • | • | | • |
| Event ID | • | • | • | • | • | • | | • |
| Name | | | | | | | | • |
| Message | | | | | | | | • |
| End Point Mode | | | | | | | | • |
| File Name | | | | • | | • | • | • |
| File Hash | | | | • | | • | • | • |
| Process Name | | | | | | • | | • |
| Device Custom String2 | | | | | | | | • |
| File Path | | | | | | | | • |
| Local Host | | • | | | • | • | | • |
| User Name | | | | | | | | • |
| Local IP | • | • | • | • | • | • | | • |
| Function | | | | | | | | • |
| Remote Host/Domain | | | | • | • | | • | |
| Remote IP | • | • | • | • | • | | • | |

# Assessing Risk Against Attack Patterns

- **Track entry vectors of attacks**
  - USB devices (Bit9)
  - EXE download over the wire (IDS)
- **Track arrival of unapproved executables**
  - New pending files (Bit9)
- **Look for suspicious indicators, e.g.**
  - Is parent process unlikely install vector (Bit9) (e.g. MS office, Adobe, browser,…)
  - Is file trying to hide itself (e.g. ADS) (Bit9)
  - Does file match known intelligence indicators (Intel)
- **Track new file executions** (Bit9)
- **Correlate with suspicious outbound traffic** (FW)

# Detection and Correlation Use Cases

**Standalone Events**

- UC 1: Bit9 Actionable Events
- UC 2: ADS Executable Hidden Files
- UC 3: New EXE created by a Suspicious Process

**Correlated Events**

- Tracking New Endpoint Files
- Tracking New External Drives
- Tracking New Internet Downloads
- UC 4: Bit9 Actionable Event Correlated with Origin
- UC 5: Bit9 Actionable Event Correlated with Intelligence Indicators
- UC 6: Outbound Activity Blocked after New File Dropped

# Use Case 1: Bit9 Actionable Events

Bit9

Sends Actionable Event E1 to ArcSight ESM

ArcSight ESM

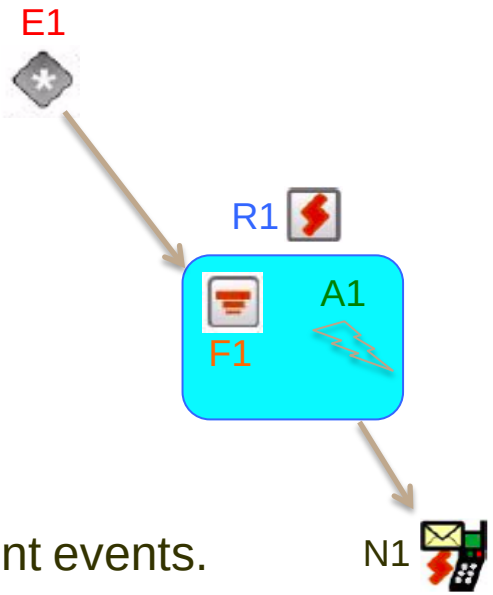
F1 : Filter passes Bit9 Actionable events

R1 : Rule triggers Action A1 sends Notification N1

N1 : Notification “Actionable Event” sent

Benefit

Analysts are notified of potentially harmful Endpoint events.



# Use Case 2: Alternate Data Streams - ADS

- **Windows Hidden file Attached to normal File**
- **Originally created for NTFS compatibility with Macintosh OS Resource Fork.**
- **Some malware hides executables in ADS files**
- **ADS Filename resembles – good.exe:bad.exe**
  - Where good.exe is known but the related good.exe:bad.exe is HIDDEN.
  - Utilities are generally needed to list ADS files in directories
  - To execute the ADS, the call must be: “start {fullpath}\goodfile.exe:bad.exe”

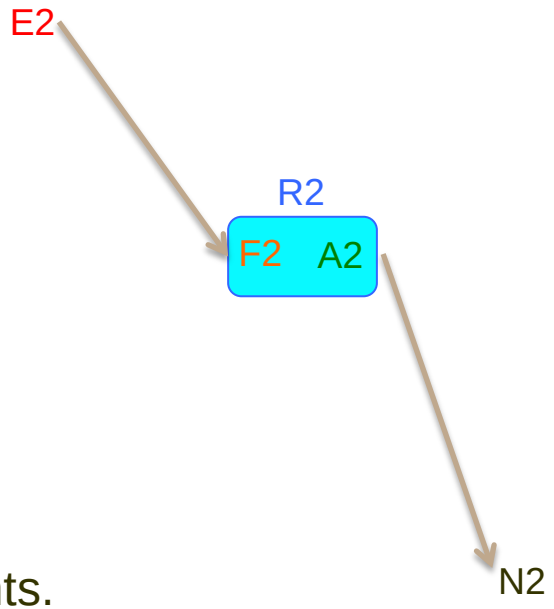
# Use Case 2: Bit9 New Executable is an ADS

Bit9

Sends New File Event E2 to ArcSight ESM

ArcSight ESM

F2 : Filter passes Bit9 New File events
R2 : Rule triggers if filename contains ":"
and does not start with "<fileid:"
A2 : Action sends Notification
N2 : "ADS File"




Benefit

Analysts notified of New ADS Files on Endpoints.

# Use Case 3: Bit9 New EXE File written by atypical Process.

Bit9

Sends New File Event E2 to ArcSight ESM

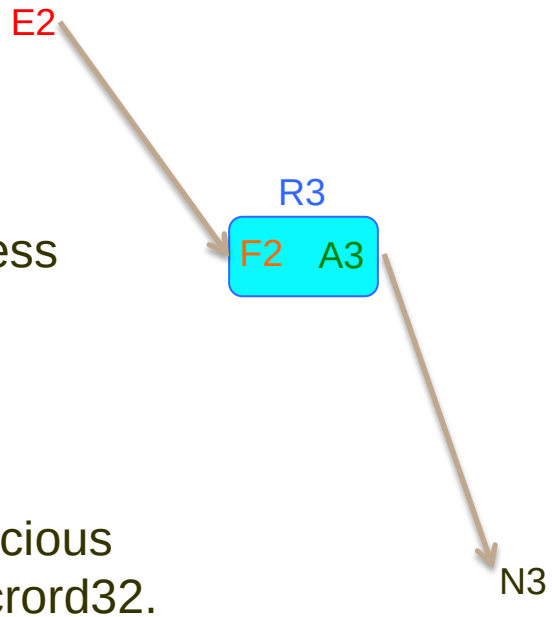
ArcSight ESM

F2 : Filter passes Bit9 New File events

R3 : Rule triggers if New File is an EXE
and the Creation Process is not a typical Process

A3 : Action sends Notification

N3: “New EXE written by abnormal Process”




Benefit

Analysts notified of New EXE Files written by suspicious processes, e.g. winword, powerpoint, excel, and acrord32.

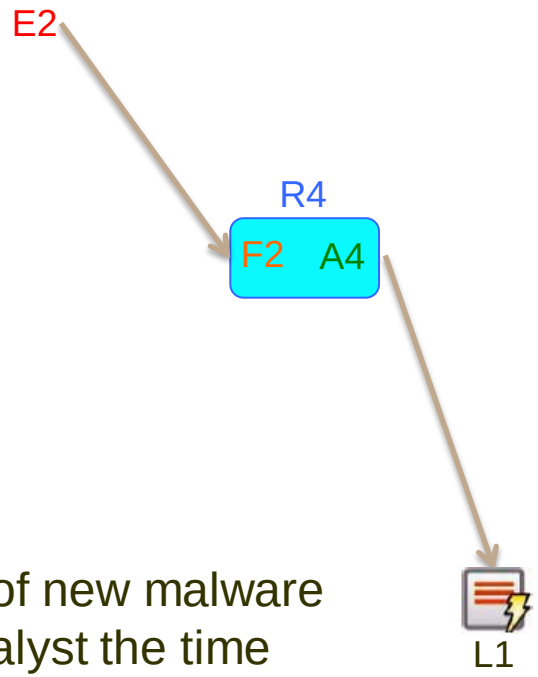
# Tracking New Endpoint Files

Bit9

User writes new file to Endpoint
Bit9 sends New File event E2 to ArcSight ESM

ArcSight ESM

F2 : Filter passes event
R4 : Rule triggers and its…
A4 : Action writes record to Active List L1
L1 : Active List record = PC IP address




Benefit

ArcSight ESM potentially correlates the origin of new malware introduced on an Endpoint. This saves the analyst the time required to backtrack through events during an incident response.

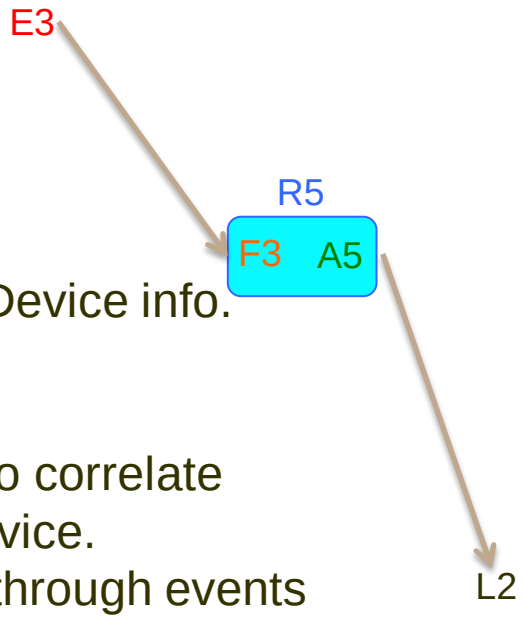
# Tracking New Endpoint External Drives

Bit9 Endpoint

User attaches new device to PC
Bit9 sends Device Attached E3 Event ID 1009 to ArcSight ESM

ArcSight ESM

F3 : Filter passes event 1009
R5 : Rule triggers and its…
A5 : Action writes record to Active List 4
L2 : Active List record = PC IP address and attached Device info.



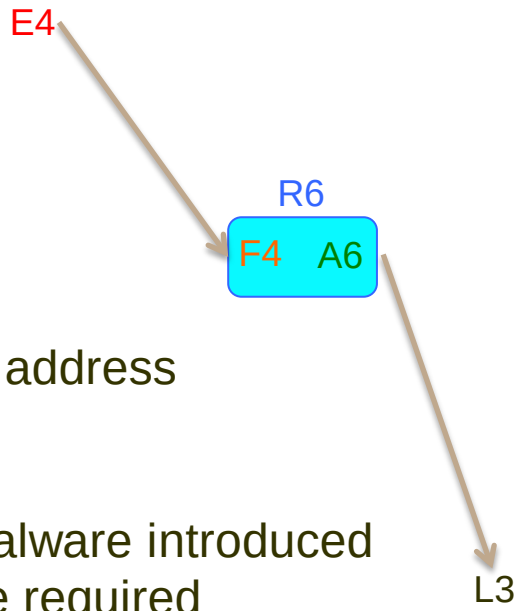

Benefit

This ArcSight Active List will potentially be used later to correlate the origin of new malware introduced by a physical device.
This saves the analyst the time required to backtrack through events during an incident response.

# Tracking New Internet Downloads

IDS

User downloads EXE to PC
IDS sends EXE Download E4 to ArcSight ESM




ArcSight ESM

F4 : Filter passes event
R6 : Rule triggers and its…
A6 : Action writes record to Active List 5
L3 : Active List record = PC IP address, Remote Site IP address

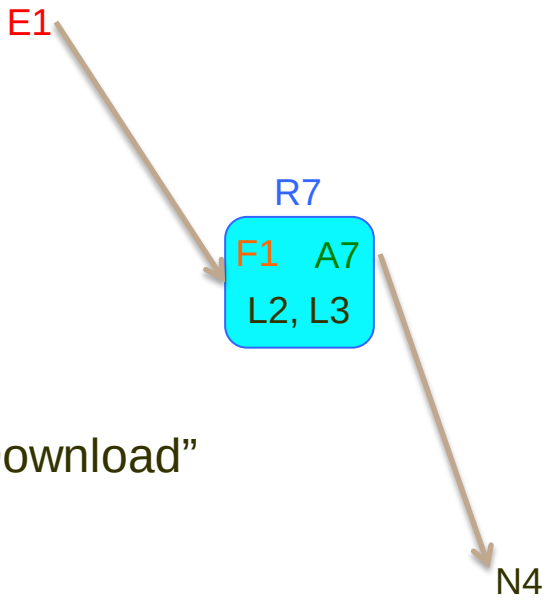
Benefit

ArcSight ESM potentially correlates the origin of new malware introduced by a network download. This saves the analyst the time required to backtrack through events during an incident response.

# Use Case 4: Bit9 Actionable Events with Drop Vector

Bit9

Sends Actionable Event E1 to ArcSight ESM




ArcSight ESM

F1 : Filter passes Bit9 Actionable events

R7 : Rule compares User/Endpoint IP address to records in L2 “Device Attached” and L3 “IDS EXE Download”

A7 : If Rule R7 triggers Action A7 sends Notification

N7 : “Actionable Event with Device Attached or EXE Download”

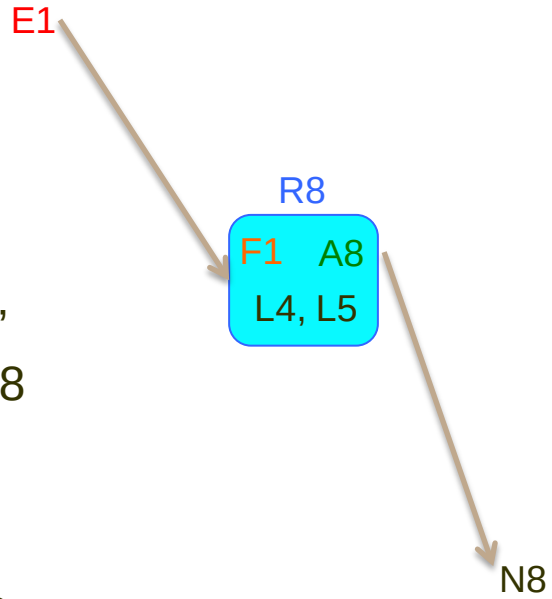
Benefit

ArcSight ESM potentially correlates, in real-time, the origin of new malware introduced into the environment by a new Drive or Internet download. This saves an Analyst the time typically spent researching the malware’s origin during incident response.

# Use Case 5: Bit9 Actionable Events with Intelligence Indicators

Bit9

Sends Actionable Event E1 to ArcSight ESM




ArcSight ESM

F1 : Filter passes Bit9 Actionable events

R8 : Rule compares User/Endpoint Filename
or File hash records to same in
Active Lists L4 “Filenames” and L5 “File hash”
If Rule triggers Action A8 sends Notification N8

N8: “Actionable Event with Intelligence Indicator”

Benefit

ArcSight ESM potentially correlates Actionable Bit9 events to suspect Filenames or File hashes from known malware. Analysts are notified of suspect malware in the environment.

# Use Case 6: Bit9 Actionable Events with Blocked Outbound Activity

FW/DNS

Sends Deny event E5 to ArcSight ESM

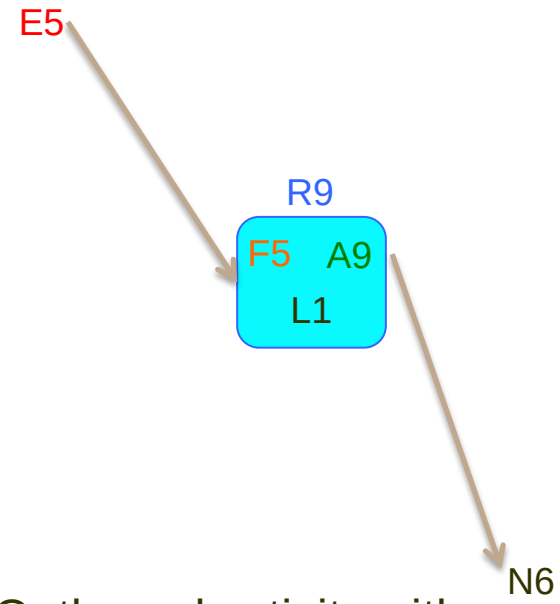
ArcSight ESM

F5 : Filter passes Outbound Deny events

R9 : Rule compares Intranet Source IP with Active List L1 records of Endpoints with New Files.

A9 : If Rule triggers Action 8 sends Notification 8

N6: “Outbound Traffic Blocked with New File”




Benefit

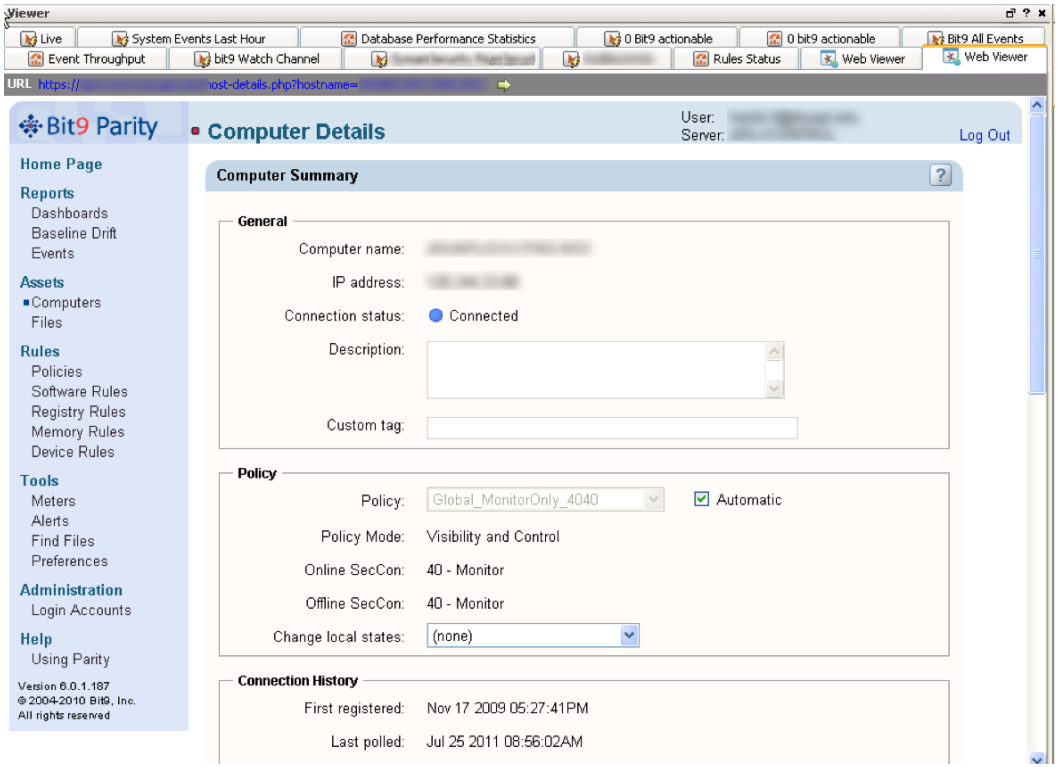
ArcSight ESM potentially correlates New Blocked Outbound activity with New Files on the Endpoint. Analysts are notified of suspect malware in the environment.

# Reducing Time to Investigate

- **Analysts cannot investigate every event that arrives**
  - Need to determine if system is protected as expected or action is required
- **Bit9 events provide immediate assessment of:**
  - Is target machine in a lockdown state?
  - Did suspicious file actually arrive on target? If yes, was it blocked?
- **When further investigation is required…**
  - Single click access to:
  - All recent activity on target machine
  - Detailed information about suspect file (where is it, who created it, what other files did it drop, trust level of file, …)
- **Remediation and response is accelerated**
  - Ban the file, lockdown the target machine, …

# Console Integration with ArcSight Viewer

- **Using Navigator Pane – Resources - Integration to provide click through integration from ArcSight events directly to Bit9 console**



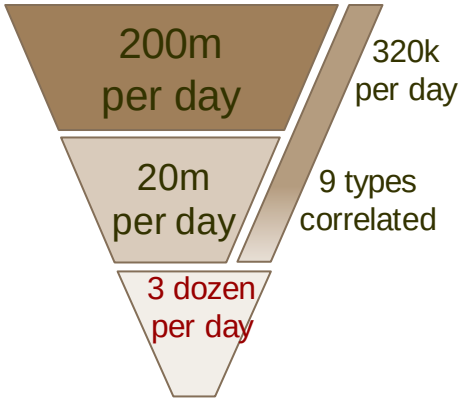
# What Integration Provides

**Bit9 Endpoint Insight Saves Analyst Incident Response Time by:**

- Identifying creation of EXE's by suspicious processes
- Identifying suspicious ADS hidden files
- Identifying potential origin / method of malware drop
- Identify user mode and their actions
- Identify new files / hashes for correlation with Intelligence Indicators
- Potential post correlation with FW/DNS callouts
- ArcSight Viewer integration to Bit9 console

# Summary of Benefits

- **Extended detection of new threats and attacks**
  - Detection based on new indicators
  - Detection of malware “at rest” versus “in motion”
- **Reduce signal-to-noise ratio: Better filtering**
  - Escalate severity of suspicious network activity based on actual endpoint activity
  - Correlation to identify suspicious attack vectors using complete picture




- **Reduce time to investigate**
  - Use endpoint events to gain more insight into suspicious activity
  - Console integration for investigation and analysis from single pane

**Impact mean time to threat conclusion by removing endpoint blind spot**

# Next Steps

- **Bit9 Data Connector for ArcSight**
  - Deeper and more secure data integration
  - Single pane of glass: provide Bit9 views directly in ArcSight console
- **Additional correlation rules**
  - Additional active lists and correlation with IDS/IPS/FW
  - Unauthorized lateral movement detection
- **Advanced traps to extend endpoint threat indicators**
  - Monitoring (or blocking) of suspicious registry activity
  - Monitoring (or blocking) of suspicious memory activity (e.g. cross process injection, dynamic code execution, system process tampering)

# Questions?

**Tracy Herriotts**
**Senior Staff Engineer**
**Johns Hopkins University**
**tracy.herriotts@gmail.com**

**Harry Sverdlove**
**Chief Technology Officer**
**Bit9, Inc.**
**hsverdlove@bit9.com**