

Optimizing Security for Situational Awareness

BRIAN KENYON McAfee

Session ID: SPO1-106

Session Classification: Intermediate

RS/CONFERENCE**2012**

```
istrator=fwadmin, Machine=cp-mgmt-
                                                                                                                                                                            Machine=cp-mqmt-station, ClientType=
ClientType=Policy Editor SessionId=Modification Info: ipaddr: changed from

Viewer, Info=connected with user pas

Light to 10.10.5.3' to '10.10.5.7'

REIX=4e1166023d Deny pretopelsswrd[in
                                                                                                                                                                            %aterface@013rcDaddressterclpert | ds
                                                                     1 TCP
                                                                                                                                                                            outbound-interface: dst address/dst
                                                                                              356.884.146.12 rule 1514:55:20 accept
                                                                                                                                                                            interinged acceptation in the state of the s
                                                                                             gw.foobar.com >eth1 product VPN-1 &
                                                                                                                                                                            list-name
                                                                                             Firewall-1
                                                            0:00:27,
                                                                                                   "Block Windows File Sharing""
                                                        ation=smtp.
                                                                                                   blocked (192.168.1.54, netbios-
                                                   at='Email Status',
                                                                                                   ssn(139)). Inbound TCP connection
                                                rom=billf1223@qmail.com,
                                                                                                                                                                                                      356.884.146.12 rule
                                              size=25140.
                                                                                                                                      10/17/2011 10:00:27,
                                                                                                                                                                                                      1514:55:20 accept
                                              source=(66.55.23.4),
                                                                                                                                      TRAFFIC, end, 66.55.23.4,
                             ,16777216, reputation=49, tls=1
                                                                                                                                                                                                      qw.foobar.com >eth1
                                                                                                                                      192.168.46.15, Monitor
                                                                                                                                                                                                      product VPN-1 & Firew
                                                                                                                                      SPAN Port, Tap Zone,
                                                             src 10.5.5.1 s_port 4523 dst
       SAVPROD,
                                                                                                                                      ethernet1/12, 83752, 1,
                                                             789.105.10.2 service http proto tcp
926-356005616892 };End
                                                                                                                                       59404, 25, tcp, allow, any
                                                             xlatesrc
. 6 : 6 : 6 : 6 : 6 : 6 : 6 : 6 : 3 3 8
                                                                         OperationTime=Thu Dec 13 15:00:48 2002,
                                                                                                                                                                                    10/17/2011 10:02:52 PM,
                                                                         ObjectName=Sanitized-Router,ObjectType=host_plain,
               Oct 17 10:00:26, Src
                                                                                                                                                                                     Deleted: (detection isn't
                                                                         ObjectTable = network objects,
               66.55.23.4, s_port 4523,
                                                                                                                                                                                     cleanable), W7MANG\host35
                                                                         Operation-Update Administrator=fwadmin,
               dst 192.168.46.15, service
                                                                                                                                                                                     C:\Brogram
                                                                         Machine=cp-mgmt-station,ClientType=Policy Editor
                                                                                                                                                                                     Files\\\Mware\\Infrastructure
               smtp, proto tcp, xlatesrc
                                                                         SessionId=Modification Info: ipaddr: changed from
                                                                                                                                                                                     \Wirtual Infrastructure
                                                                         '10.10.5.3' to '10.10.5.7'
                                                                                                                                                                                     Client\4.1\vmware-vmrc.exe,
lassification: Attempted
                                                                                                                                                                                    C:\Users\brogers\Desktop\45
formation Leak] [Priority: 2]
                                                                                                                                                                                    5_23_setup.exe
/06-8:14:09.082119
                                                                                                                                                                                    Generic.dx!bbfq
2.168.1.167:1052 ->
                                                                                     14:53:16 drop gw.foobar.com >eth0 product VPN-1 &
                                                                                     Firewall-1
        356.884.146.12 rule
        1514:55:20 accept
                                                            14:53:16 dropw gwo gloobaconcome bletho
                                                                                                                                                       14:53:16 drop gw.foobar.com
                                                                                                                                                                                                                 3/6/2011 8:14:0
        gw.foobar.com >eth1
                                                            product VPN-1 & Firewall-1
                                                                                                                                                       >eth0 product VPN-1 &
                                                                                                                                                                                                                 (192.168.1.54,r
        Broduct ₩BN=1 & Firewall=1
                                                                                                                                                       Firewall-1
                                                                                                                                                                                                                 (192.168.1.54,r
                                                                                                                                                                                                                 is(KENT(172.30)
                                                                                                       Dec 19 04:40:54 qw.foobar.com %PIX-4-400027: IDS:3041 TCP
                                                                                                                                                                                                                 is(192.168.1.54
                                                                                                       SYN+FIN flags from 10.121.146.23 to 356.512.10.2 on
                                                                                                       interface outside
r 5 07:12:50 10.87.62.40 %PIX-5-304001: 10.5.5.1
cessed URL
                                                                                                      %PIX-4-106023: Deny protocol src [inbound-
                                                                                                                                                                                          [**] [1:1407:9] SNMP trap ud
2.54.10.2:/aharrison@awod.com?on_url=http://785.131.1
                                                                                                      interface]:[grc_address/src_port] dst
                                                                                                                                                                                          [**] [Classification:
2/$c716ts/winnt55system32/cmd.exe?/c+
                                                                                                     outbound-interface: dst_address/dst_port
                                                                                                                                                                                          Attempted Information Leak
                                                                                                      [type {type}, code {code}] by access_group
e?/c+
                                                                                                                                                                                          [Brigrity: 2] 03/06-
                                                                                                      access-list-name
                                                                                                                                                                                          8:14:09.082119
89.432.146.12 s port
                                                                                                                                                                                          192.168.1.167:1052 ->
35.001.10.2 service ms-
                                                        src 10.5.5.1 s port 4523 dst 789.105.10.2 service http proto
                                                                                                                                                                                          172.30.128.27:162 UDP TTL:11
                                                        tcp xlatesrc
                                                                                                                                                                                         TOS:0x0 ID:29101 IpLen:20
```

DamLen:8

What is SIEM?

of Two Distinct Technologies

- Security Event Management (SEM)
 - Primarily focused on Collecting and Aggregating Security Events
- Security Information Management(SIM)
 - Primarily focused on the Enrichment,
 Normalization, and Correlation of
 Security Events

Security Information &

Event Management is a Set of Technologies for:

- Log Data Collection
- Correlation
- Aggregation
- Normalization
- Retention
- Analysis and Workflow

Three Major Factors Driving the Majority of SIEM Implementations



Real-Time Threat Visibility



Security
Operational
Efficiency



Compliance and/or Log Management Requirements





The SIEM "Catch 22"



80% of threats come from insiders



39% of threats target software, applications, and services



66% of those involved did not know the data was on the system

Source: Forrester, Verizon

- To address these concerns, there is a need to monitor and analyze more data
- However, there is already too much data for other SIEMs



SIEM is Still Evolving ... Beyond Logs

What else happened at this time? Near this time? What is the time zone?

What is this service? What other messages did it produce? What other systems does it run on?

DNS name, Windows name, Other names? Whois info? Organization owner? Where does the IP originate from (geo location info)? What else happened on this host? Which other hosts did this IP communicate with?

Mar 20 08:44:35 pcx02 sshd[263]: Accepted password for root from 216.101.197.234 port 56946 ssh2

What is the hosts IP address? Other names? Location on the network/datacenter? Who is the admin? Is this system vulnerable to exploits?

Who is this user? What is the users access-level? What is the users real name, department, location? What other events from this user?

What does this number mean? s this documented somewhere?

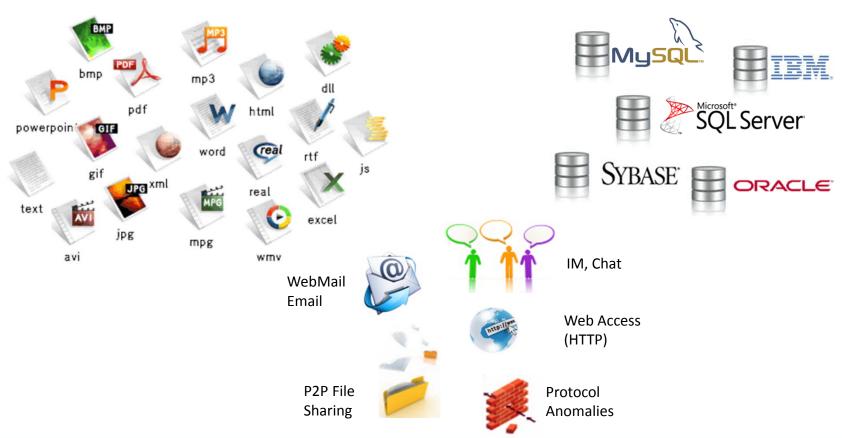
What is this port? Is this a normal port for this service? What else is this service being used for?





SIEM is Still Evolving...To

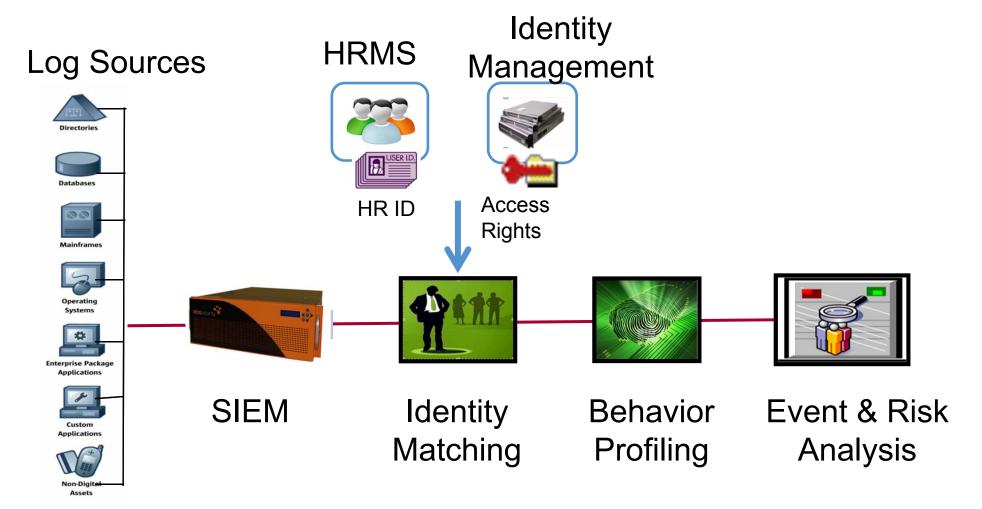
- SIEM Content Awareness (Next Generation SIEM)
 - Content Awareness is Understanding the Payload at the Application Layer







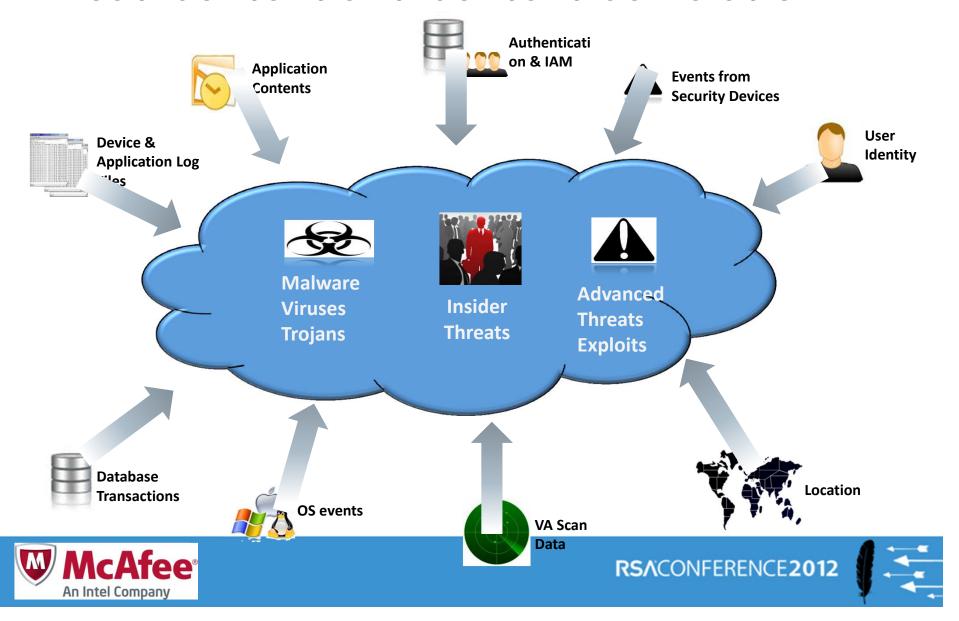
SIEM is Still Evolving...To







Broad Content and Context Correlation



Benefits of Content Awareness

- Visibility into the network
- Complement logs
- Data leak monitoring
- Advanced threat detection
 - Malware, bots, client-side attacks, APTs
- Network Forensics
- Security Policy Violations

Technology Highlights

- Protocol Classification
- Deep Packet Inspection
- Application Discovery
- Document Discovery
- Document Reconstruction
- Session Replay







The Requirements...

Threat Intelligence Real-Time High **Next Generation SIEM** Command Performance Advanced 010011 100 1001 100110 11 100 1 110 10 010011 001 100 1101 10101 110 1 Database Correlation Johnson **AUDIT** LOG **EVENT** COMP. 0011 1)1 **10**01 100 1 CONTEXT 10011 00 110 CONTENT 101 110 **RULES / STATISTICS**





The Requirements...

Threat Intelligence Real-Time High **Next Generation SIEM** Command Performance Advanced 010011 100 1001 100110 11 100 1 110 10 010011 001 100 1101 10101 110 1 Database Correlation **AUDIT** LOG **EVENT** COMP. 0011 1)1 **10**01 100 1 **CONTEXT** 10011 00 110 CONTENT 101 110 **RULES / STATISTICS**

1 SEEK

2 ANALYZE

3 PREVENT

4 ERADICATE





```
istrator=fwadmin, Machine=cp-mgmt-
                                                                                                                                                                            Machine=cp-mqmt-station, ClientType=
ClientType=Policy Editor SessionId=Modification Info: ipaddr: changed from

Viewer, Info=connected with user pas

Light to 10.10.5.3' to '10.10.5.7'

REIX=4e1166023d Deny pretopelsswrd[in
                                                                                                                                                                            %aterface@013rcDaddressterclpert | ds
                                                                     1 TCP
                                                                                                                                                                            outbound-interface: dst address/dst
                                                                                              356.884.146.12 rule 1514:55:20 accept
                                                                                                                                                                            interinged acceptation in the state of the s
                                                                                             gw.foobar.com >eth1 product VPN-1 &
                                                                                                                                                                            list-name
                                                                                             Firewall-1
                                                            0:00:27,
                                                                                                   "Block Windows File Sharing""
                                                        ation=smtp.
                                                                                                   blocked (192.168.1.54, netbios-
                                                   at='Email Status',
                                                                                                   ssn(139)). Inbound TCP connection
                                                rom=billf1223@qmail.com,
                                                                                                                                                                                                      356.884.146.12 rule
                                              size=25140.
                                                                                                                                      10/17/2011 10:00:27,
                                                                                                                                                                                                      1514:55:20 accept
                                              source=(66.55.23.4),
                                                                                                                                      TRAFFIC, end, 66.55.23.4,
                             ,16777216, reputation=49, tls=1
                                                                                                                                                                                                      qw.foobar.com >eth1
                                                                                                                                      192.168.46.15, Monitor
                                                                                                                                                                                                      product VPN-1 & Firew
                                                                                                                                      SPAN Port, Tap Zone,
                                                             src 10.5.5.1 s_port 4523 dst
       SAVPROD,
                                                                                                                                      ethernet1/12, 83752, 1,
                                                             789.105.10.2 service http proto tcp
926-356005616892 };End
                                                                                                                                       59404, 25, tcp, allow, any
                                                             xlatesrc
. 6 : 6 : 6 : 6 : 6 : 6 : 6 : 6 : 3 3 8
                                                                         OperationTime=Thu Dec 13 15:00:48 2002,
                                                                                                                                                                                    10/17/2011 10:02:52 PM,
                                                                         ObjectName=Sanitized-Router,ObjectType=host_plain,
               Oct 17 10:00:26, Src
                                                                                                                                                                                     Deleted: (detection isn't
                                                                         ObjectTable = network objects,
               66.55.23.4, s_port 4523,
                                                                                                                                                                                     cleanable), W7MANG\host35
                                                                         Operation-Update Administrator=fwadmin,
               dst 192.168.46.15, service
                                                                                                                                                                                     C:\Brogram
                                                                         Machine=cp-mgmt-station,ClientType=Policy Editor
                                                                                                                                                                                     Files\\\Mware\\Infrastructure
               smtp, proto tcp, xlatesrc
                                                                         SessionId=Modification Info: ipaddr: changed from
                                                                                                                                                                                     \Wirtual Infrastructure
                                                                         '10.10.5.3' to '10.10.5.7'
                                                                                                                                                                                     Client\4.1\vmware-vmrc.exe,
lassification: Attempted
                                                                                                                                                                                    C:\Users\brogers\Desktop\45
formation Leak] [Priority: 2]
                                                                                                                                                                                    5_23_setup.exe
/06-8:14:09.082119
                                                                                                                                                                                    Generic.dx!bbfq
2.168.1.167:1052 ->
                                                                                     14:53:16 drop gw.foobar.com >eth0 product VPN-1 &
                                                                                     Firewall-1
        356.884.146.12 rule
        1514:55:20 accept
                                                            14:53:16 dropw gwo gloobaconcome bletho
                                                                                                                                                       14:53:16 drop gw.foobar.com
                                                                                                                                                                                                                 3/6/2011 8:14:0
        gw.foobar.com >eth1
                                                            product VPN-1 & Firewall-1
                                                                                                                                                       >eth0 product VPN-1 &
                                                                                                                                                                                                                 (192.168.1.54,r
        Broduct ₩BN=1 & Firewall=1
                                                                                                                                                       Firewall-1
                                                                                                                                                                                                                 (192.168.1.54,r
                                                                                                                                                                                                                 is(KENT(172.30)
                                                                                                       Dec 19 04:40:54 qw.foobar.com %PIX-4-400027: IDS:3041 TCP
                                                                                                                                                                                                                 is(192.168.1.54
                                                                                                       SYN+FIN flags from 10.121.146.23 to 356.512.10.2 on
                                                                                                       interface outside
r 5 07:12:50 10.87.62.40 %PIX-5-304001: 10.5.5.1
cessed URL
                                                                                                      %PIX-4-106023: Deny protocol src [inbound-
                                                                                                                                                                                          [**] [1:1407:9] SNMP trap ud
2.54.10.2:/aharrison@awod.com?on_url=http://785.131.1
                                                                                                      interface]:[src_address/src_port] dst
                                                                                                                                                                                          [**] [Classification:
2/$c716ts/winnt55system32/cmd.exe?/c+
                                                                                                     outbound-interface: dst_address/dst_port
                                                                                                                                                                                          Attempted Information Leak
                                                                                                      [type {type}, code {code}] by access_group
e?/c+
                                                                                                                                                                                          [Brigrity: 2] 03/06-
                                                                                                      access-list-name
                                                                                                                                                                                          8:14:09.082119
89.432.146.12 s port
                                                                                                                                                                                          192.168.1.167:1052 ->
35.001.10.2 service ms-
                                                        src 10.5.5.1 s port 4523 dst 789.105.10.2 service http proto
                                                                                                                                                                                          172.30.128.27:162 UDP TTL:11
                                                        tcp xlatesrc
                                                                                                                                                                                         TOS:0x0 ID:29101 IpLen:20
```

DamLen:8

Oct 17 10:00:27,

App bication samtp,

Evente Email Status',
From billilization sample om,
size 25190,
source (66.55:2344),
reputation 49, tis=1
reputation 49, tis=1

10/17/2011 10:00:27, TRAFFIC₁₇ end, 16:60 55, 23.4, 192.168.46.15, Monfet&r⁴, SPAN Port, Tap Zone, ethernatine12/1283752, 11, 594045,9425, 25cpp, allow, arany

Oct₀47₁710:00:226 srsrc 66.5552334, spotrt524523, dst^{dst}9¹⁹²168:46¹⁵75 service smtp, proto tcp, xlatesrc smtp, proto tcp, xlatesrc

cleanabled, W7MANG\host35
C: TPlesbyMagre\Infrastructure
Filvirtual Marre\Infrastructure
Filvirtual briggrastructure
e\Vivtual briggrastructure
Client\4.1\vmwarewmrc.exe,
client\4.1\vmwarevmrc.exe,

10/1/4/2011 1002052:512, PM,

Deleted detection isn't detection isn't

55_23_setup.exe
Generic.dx!bbfq

RESPOND

Content-Aware Forensics & Correlated Breach Discovery



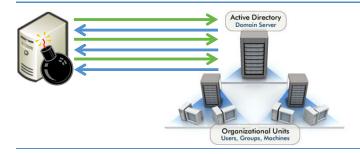
A user receives an *email* with an *attachment* from an external source identified in the *GTI blacklist* as a malicious host.

Suspected Malware Infection

The *HIPS* agent running on the local host generates an alert claiming to have identified an *unwanted application* however due to UAC, the threat *failed* to be *quarantined* or deleted.



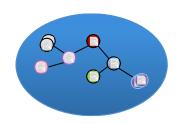
Potential Compromised Endpoint



The compromised system is next seen having failed *multiple authentication attempts* to a trusted enterprise host.

Attack Proliferation

Further investigation reveals that over the past 6 *months*, several other endpoints have exhibited a *similar behavior*; Communicating with a known malicious host via email, failing a remediation attempt and launching a subsequent brute force attack against neighboring enterprise systems.



Long-Term Situational Awareness





Real Time Security Intelligence



- Enrich from Enterprise Sources
- Enrich from Threat Feeds (GTI, SANS, etc.)
- User/Identity Normalization
- Advanced Vulnerability Feeds
- Data Source Reputation
- Accurate Risk Scores

- Accurate Threat Correlation
- Risk Correlation
- Historical Correlation





Apply These Key Takeaways

- SIEM functionality can now deliver true situational awareness
 - Assess your specific needs (security, compliance, or both)
 - Centralized or distributed needs
 - Network, endpoints, and cloud feeds benefitting all points of risk with intelligent information
 - Identify critical assets and prioritize
 - Start with a small or incremental project
 - Look for compliance budget to fund your security needs





Thank You For Your Time

Questions



