Optimizing Security for Situational Awareness

BRIAN KENYON
McAfee

Session ID: SPO1-106
Session Classification: Intermediate


ble=network_objects, Operation=Update,Administrator=fwadmin, Machine=cp-mgmt-
ClientType=Policy Editor SessionId=Modification Info: ipaddr: changed from
on,ClientType=Policy Editor SessionId=Modification Info: ipaddr: changed from '10.10.5.3' to '10.10.5.7'
.3' to '10.10.5.7'
Machine=cp-mgmt-station, ClientType=
Viewer, Info=connected with user pas
%PIX-4-106023: Deny protocol src [in
interface]:[src_address/src_port] ds
outbound-interface: dst_address/dst_
[type {type}, code {code}] by access_group
list-name
:54 gw.foobar.com %PIX-4-400027: IDS:3041 TCP
s from 10.121.146.23 to 356.512.10.2 on
tside
356.884.146.12 rule 1514:55:20 accept
gw.foobar.com >eth1 product VPN-1 &
Firewall-1
Oct 17 10:00:27,
Application=smtp,
Event='Email Status',
From=billf1223@gmail.com,
size=25140,
source=(66.55.23.4),
reputation=49, tls=1
"Block Windows File Sharing""
blocked (192.168.1.54,netbios-
ssn(139)). Inbound TCP connection
16 drop gw.foobar.com
product VPN-1 &
ll-1
KENT,userk,,,,,,,16777216,
re
10/17/2011 10:00:27,
TRAFFIC, end, 66.55.23.4,
192.168.46.15, Monitor
SPAN Port, Tap Zone,
ethernet1/12, 83752, 1,
59404, 25, tcp, allow, any
356.884.146.12 rule
1514:55:20 accept
gw.foobar.com >eth1
product VPN-1 & Firew
SAVPROD,{
926-356005616892 },End
926-356005616892 },End
src 10.5.5.1 s_port 4523 dst
789.105.10.2 service http proto tcp
xlatesrc
0.0.0.0:0.0.0.0,0.0.0.338
0.0.0.0:0.0.0.0,0.0.0.338
OperationTime=Thu Dec 13 15:00:48 2002,
ObjectName=Sanitized-Router,ObjectType=host_plain,
ObjectTable=network_objects,
Operation=Update,Administrator=fwadmin,
Machine=cp-mgmt-station,ClientType=Policy Editor
SessionId=Modification Info: ipaddr: changed from
'10.10.5.3' to '10.10.5.7'
10/17/2011 10:02:52 PM,
Deleted (detection isn't
cleanable), W7MANG\host35
C:\Program
Files\VMware\Infrastructure
\Virtual Infrastructure
Client\4.1\vmware-vmrc.exe,
C:\Users\brogers\Desktop\45
5_23_setup.exe
Generic.dx!bbfq
Oct 17 10:00:26, Src
66.55.23.4, s_port 4523,
dst 192.168.46.15, service
smtp, proto tcp, xlatesrc
ObjectName=Sanitized-
Router,ObjectType=host_plain,
ObjectTable=network_objects,
lassification: Attempted
formation Leak] [Priority: 2]
/06-8:14:09.082119
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
gw.foobar.com >eth1
product VPN-1 & Firewall-1
product VPN-1 & Firewall-1
14:53:16 drop gw.foobar.com >eth0
product VPN-1 & Firewall-1
14:53:16 drop gw.foobar.com
>eth0 product VPN-1 &
Firewall-1
3/6/2011 8:14:0
(192.168.1.54,r
(192.168.1.54,r
is(KENT(172.30.
is(192.168.1.54
Dec 19 04:40:54 gw.foobar.com %PIX-4-400027: IDS:3041 TCP
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
2.54.10.2:/aharrison@awod.com?on_url=http://785.131.1
2/scripts/..%%35c../winnt/system32/cmd.exe?/c+
%%35c../winnt/system32/cmd.e
e?/c+
%PIX-4-106023: Deny protocol src [inbound-
interface]:[src_address/src_port] dst
outbound-interface: dst_address/dst_port
[type {type}, code {code}] by access_group
access-list-name
[**] [1:1407:9] SNMP trap ud
[**] [Classification:
Attempted Information Leak]
[Priority: 2] 03/06-
8:14:09.082119
192.168.1.167:1052 ->
172.30.128.27:162 UDP TTL:11
TOS:0x0 ID:29101 IpLen:20
DgmLen:8
[Classification: Attempted
Information Leak]
[Priority: 2]
589.432.146.12 s_port
235.001.10.2 service ms-
src 10.5.5.1 s_port 4523 dst 789.105.10.2 service http proto
tcp xlatesrc

What is SIEM?

SIEM-the Evolution & Integration 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

1. Real-Time Threat Visibility
2. Security Operational Efficiency
3. Compliance and/or Log Management Requirements

The SIEM "Catch 22"

80% of threats come from insiders

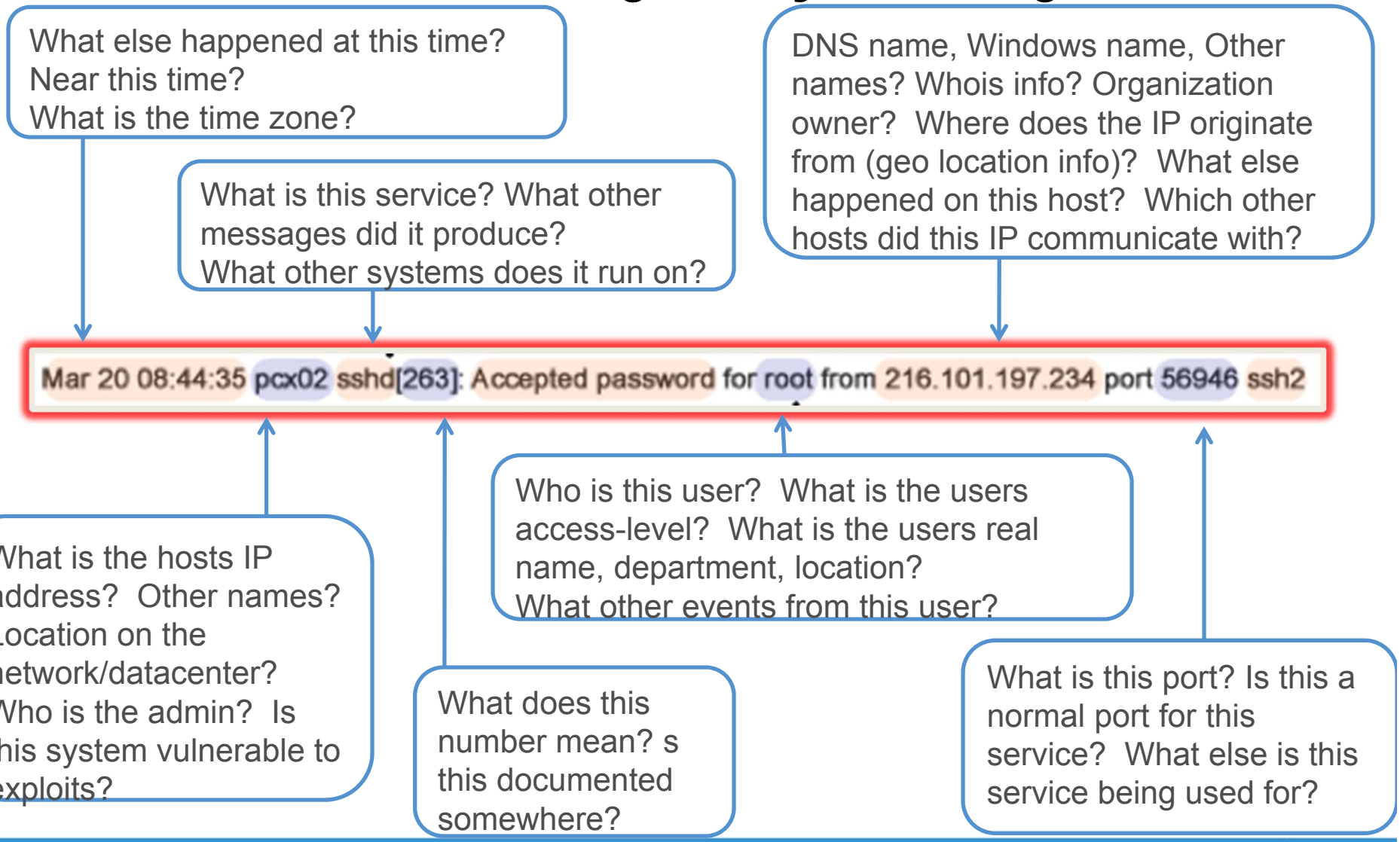
39% of threats target software, applications, and services

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

Source: Forrester, Verizon

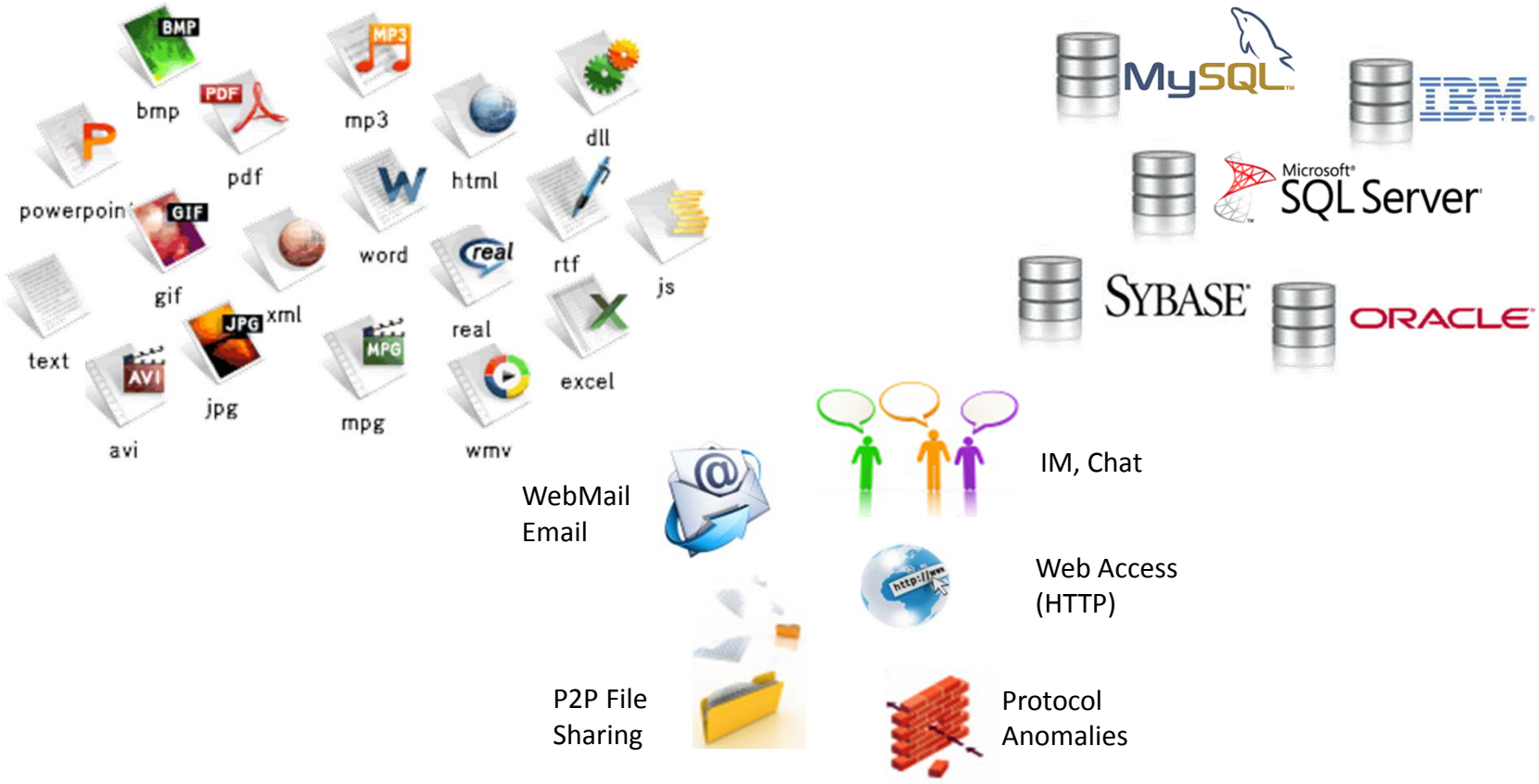
- To address these concerns, there is a need to monitor and analyze **more data**
- However, there is already **too much data** for other SIEMs

SIEM is Still Evolving ...Beyond Logs

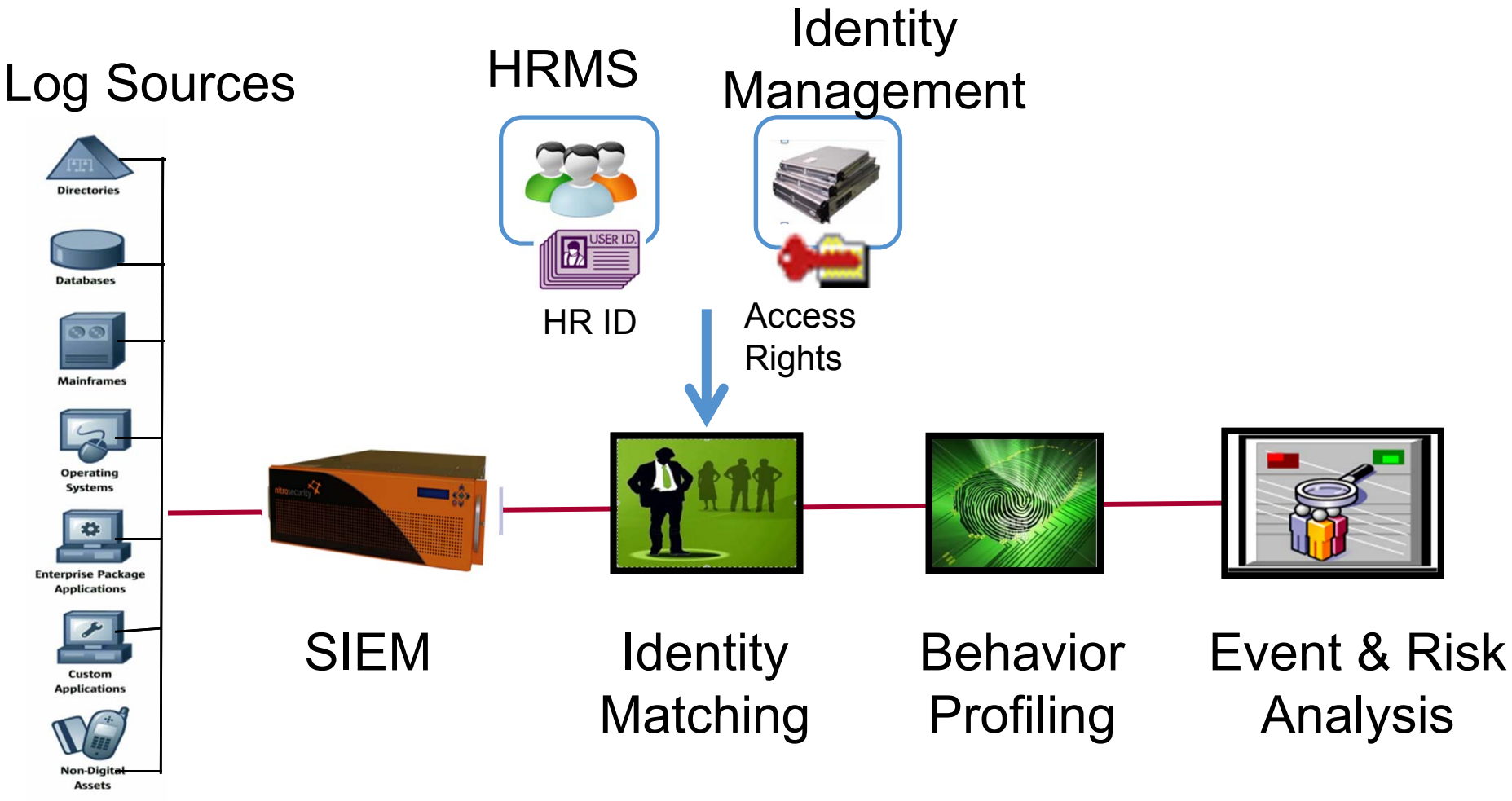


SIEM is Still Evolving…To

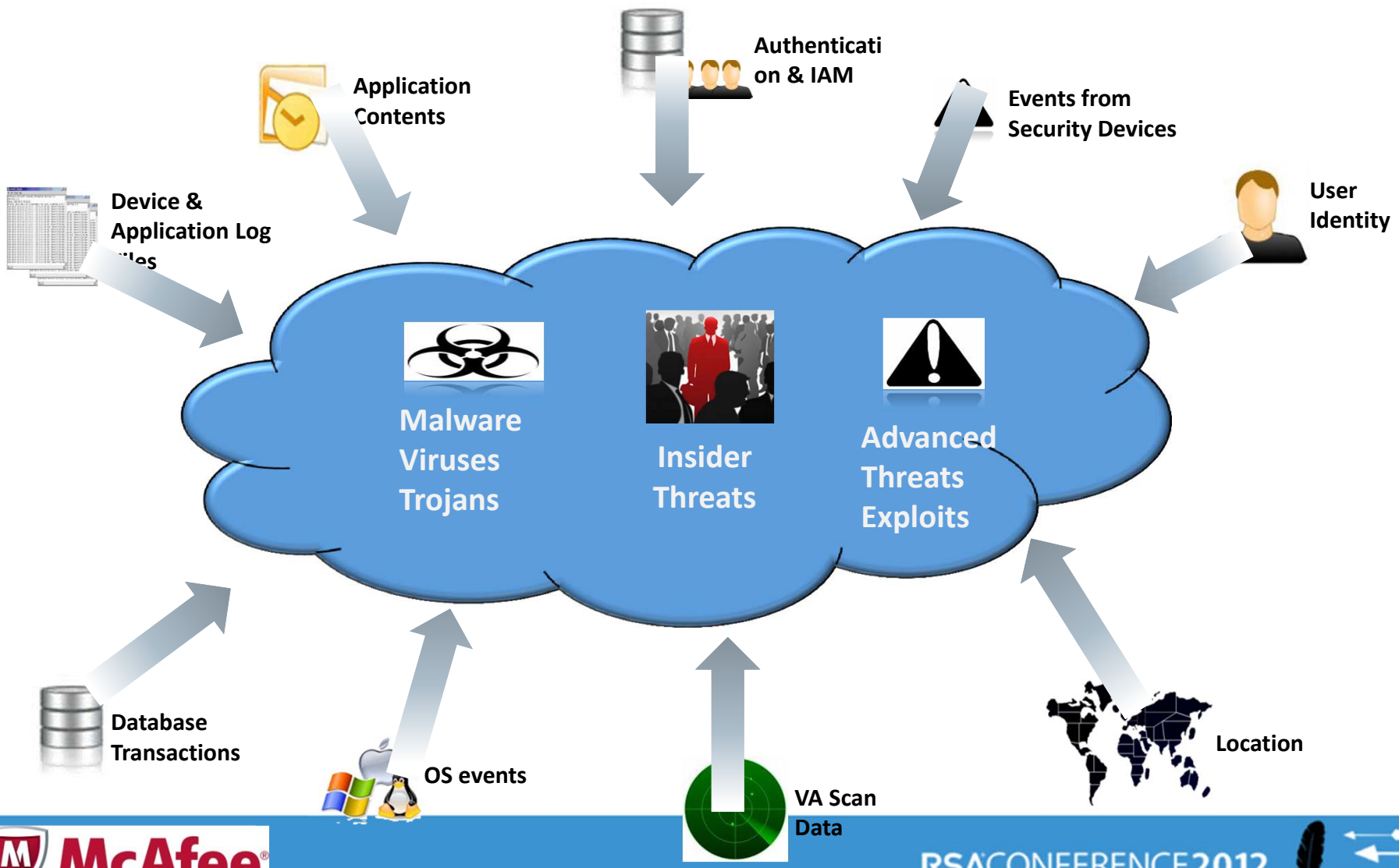
- SIEM Content Awareness (Next Generation SIEM)
  - Content Awareness is Understanding the Payload at the Application Layer



SIEM is Still Evolving...To



Broad Content and Context Correlation



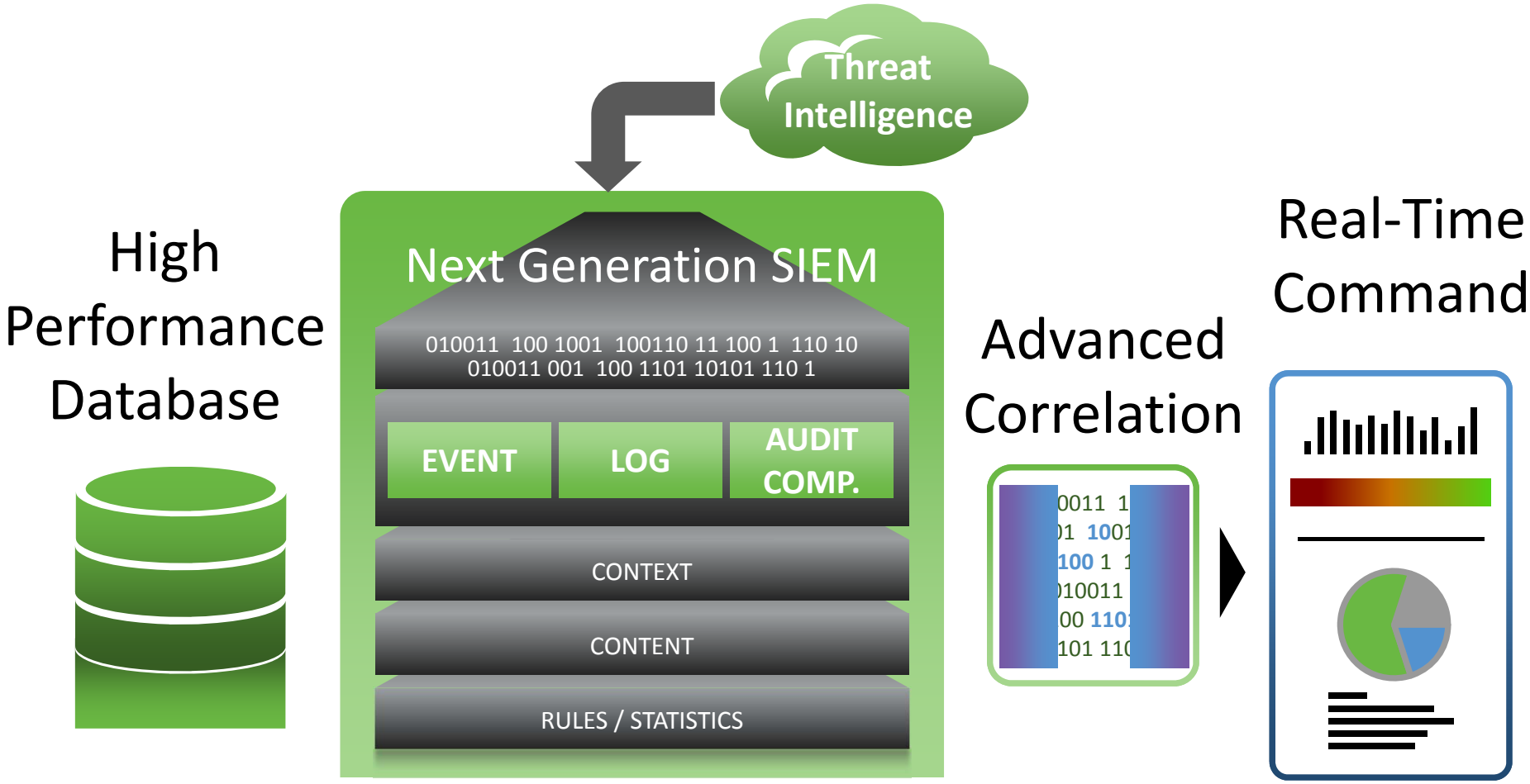
Benefits of Content Awareness

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

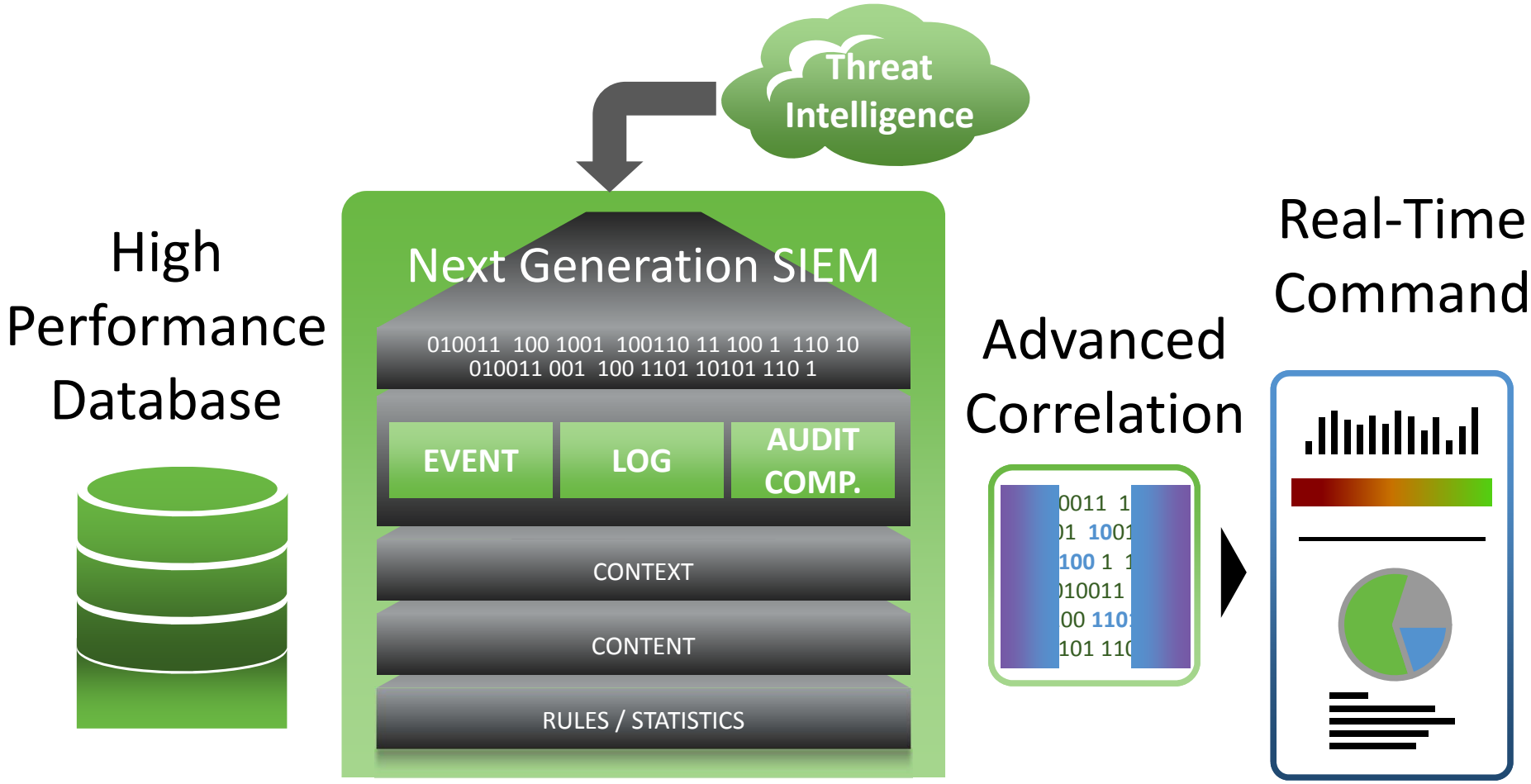
Technology Highlights

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

The Requirements…



The Requirements…

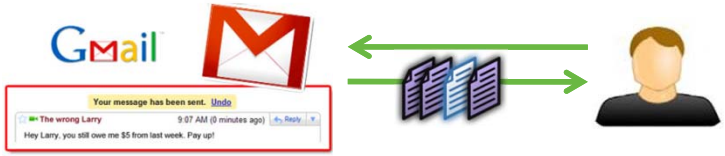


1 SEEK 2 ANALYZE 3 PREVENT 4 ERADICATE


ble=network_objects, Operation=Update,Administrator=fwadmin, Machine=cp-mgmt-
ClientType=Policy Editor SessionId=Modification Info: ipaddr: changed from
on,ClientType=Policy Editor SessionId=Modification Info: ipaddr: changed from '10.10.5.3' to '10.10.5.7'
.3' to '10.10.5.7'
Machine=cp-mgmt-station, ClientType=
Viewer, Info=connected with user pas
%PIX-4-106023: Deny protocol src [in
interface]:[src_address/src_port] ds
outbound-interface: dst_address/dst_
[type {type}, code {code}] by access_group
list-name
:54 gw.foobar.com %PIX-4-400027: IDS:3041 TCP
s from 10.121.146.23 to 356.512.10.2 on
tside
356.884.146.12 rule 1514:55:20 accept
gw.foobar.com >eth1 product VPN-1 &
Firewall-1
Oct 17 10:00:27,
Application=smtp,
Event='Email Status',
From=billf1223@gmail.com,
size=25140,
source=(66.55.23.4),
reputation=49, tls=1
"Block Windows File Sharing""
blocked (192.168.1.54,netbios-
ssn(139)). Inbound TCP connection
16 drop gw.foobar.com
product VPN-1 &
ll-1
KENT,userk,,,,,,,16777216,
re
10/17/2011 10:00:27,
TRAFFIC, end, 66.55.23.4,
192.168.46.15, Monitor
SPAN Port, Tap Zone,
ethernet1/12, 83752, 1,
59404, 25, tcp, allow, any
356.884.146.12 rule
1514:55:20 accept
gw.foobar.com >eth1
product VPN-1 & Firew
SAVPROD,{
926-356005616892 },End
926-356005616892 },End
src 10.5.5.1 s_port 4523 dst
789.105.10.2 service http proto tcp
xlatesrc
0.0.0.0:0.0.0.0,0.0.0.338
0.0.0.0:0.0.0.0,0.0.0.338
OperationTime=Thu Dec 13 15:00:48 2002,
ObjectName=Sanitized-Router,ObjectType=host_plain,
ObjectTable=network_objects,
Operation=Update,Administrator=fwadmin,
Machine=cp-mgmt-station,ClientType=Policy Editor
SessionId=Modification Info: ipaddr: changed from
'10.10.5.3' to '10.10.5.7'
10/17/2011 10:02:52 PM,
Deleted (detection isn't
cleanable), W7MANG\host35
C:\Program
Files\VMware\Infrastructure
\Virtual Infrastructure
Client\4.1\vmware-vmrc.exe,
C:\Users\brogers\Desktop\45
5_23_setup.exe
Generic.dx!bbfq
Oct 17 10:00:26, Src
66.55.23.4, s_port 4523,
dst 192.168.46.15, service
smtp, proto tcp, xlatesrc
ObjectName=Sanitized-
Router,ObjectType=host_plain,
ObjectTable=network_objects,
lassification: Attempted
formation Leak] [Priority: 2]
/06-8:14:09.082119
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
gw.foobar.com >eth1
product VPN-1 & Firewall-1
product VPN-1 & Firewall-1
14:53:16 drop gw.foobar.com >eth0
product VPN-1 & Firewall-1
14:53:16 drop gw.foobar.com
>eth0 product VPN-1 &
Firewall-1
3/6/2011 8:14:0
(192.168.1.54,r
(192.168.1.54,r
is(KENT(172.30.
is(192.168.1.54
Dec 19 04:40:54 gw.foobar.com %PIX-4-400027: IDS:3041 TCP
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
2.54.10.2:/aharrison@awod.com?on_url=http://785.131.1
2/scripts/..%%35c../winnt/system32/cmd.exe?/c+
%%35c../winnt/system32/cmd.e
e?/c+
%PIX-4-106023: Deny protocol src [inbound-
interface]:[src_address/src_port] dst
outbound-interface: dst_address/dst_port
[type {type}, code {code}] by access_group
access-list-name
[**] [1:1407:9] SNMP trap ud
[**] [Classification:
Attempted Information Leak]
[Priority: 2] 03/06-
8:14:09.082119
192.168.1.167:1052 ->
172.30.128.27:162 UDP TTL:11
TOS:0x0 ID:29101 IpLen:20
DgmLen:8
[Classification: Attempted
Information Leak]
[Priority: 2]
589.432.146.12 s_port
235.001.10.2 service ms-
src 10.5.5.1 s_port 4523 dst 789.105.10.2 service http proto
tcp xlatesrc


Oct 17 10:00:27, Application=smtp, Event='Email Status', From=billf1223@gmail.com, size=251440, source=(66.55.23.4), reputation=49, tls=1
10/17/2011 10:00:27, TRAFFIC_end, 66.55.23.4, 192.168.46.15, Monitor SPAN Port, Tap Zone, ethernet1/12, 83752, 1, 59404, 25, tcp, allow, any
Oct 17 10:00:26, src 66.55.23.4, sport 4523, dst 192.168.46.15, service smtp, proto tcp, xlatesrc
10/17/2011 10:02:52 PM, Deleted (detection isn't cleanable), W7MANG\host35 C:\Program Files\VMware\Infrastructure\Virtual Infrastructure Client\4.1\vmware-vmrc.exe, C:\Users\brogers\Desktop\55_23_setup.exe Generic.dx!bbfq
RESPOND

Content-Aware Forensics & Correlated Breach Discovery

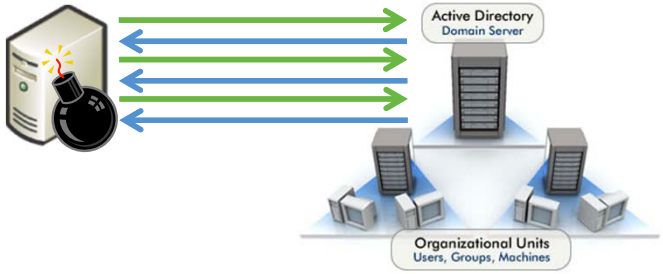


A user receives an ***email*** with an ***attachment*** from an external source identified in the ***GTI blacklist*** as a malicious host.

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.

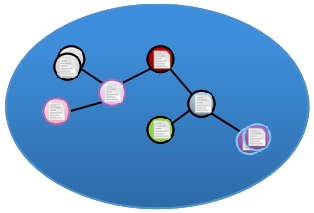
Potential Compromised Endpoint



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