WHAT IS

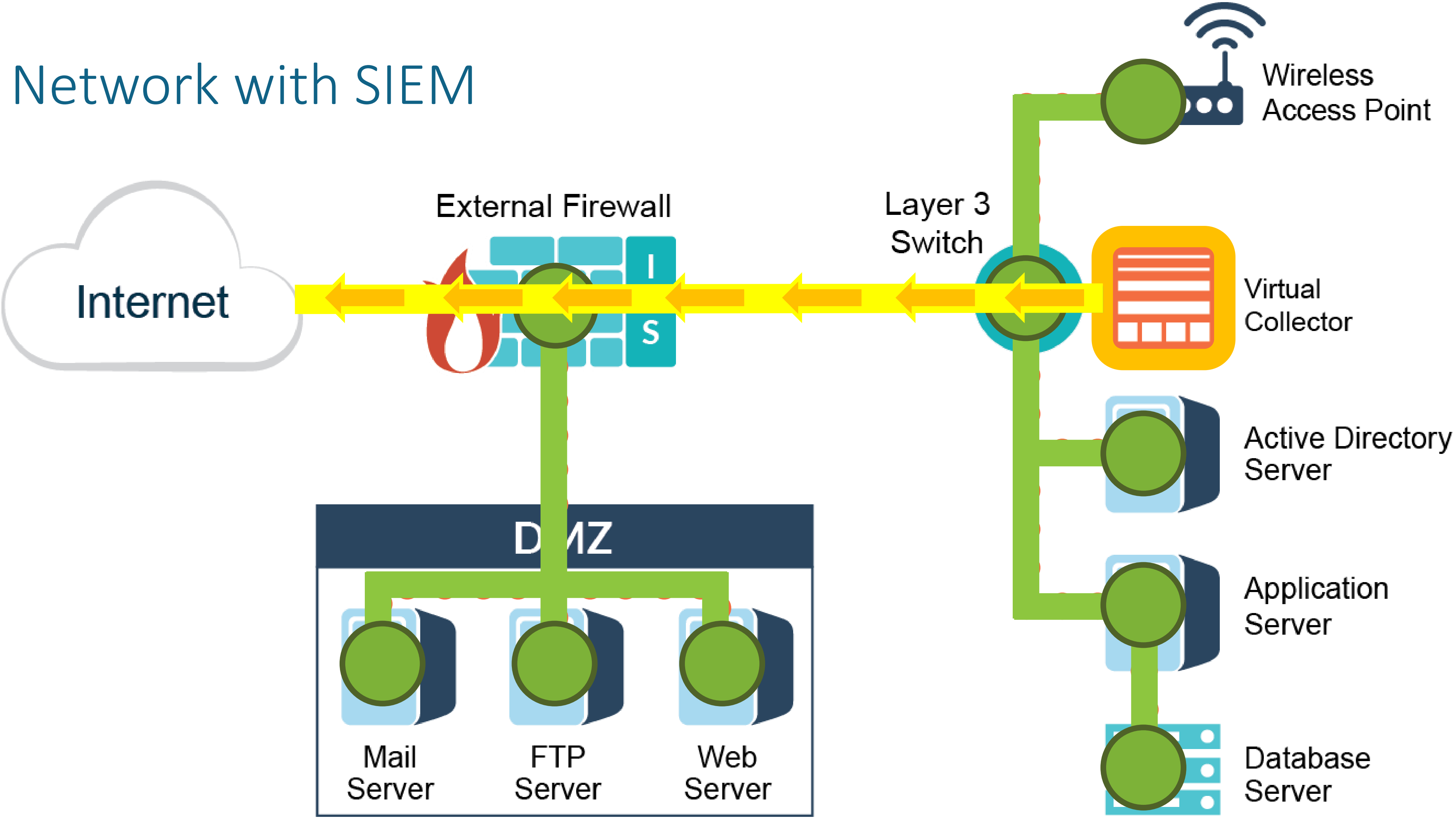
SIEM?

SIEM

Security Information Event Management

Aggregates valuable data across business units/solutions in order to identify and correlate these feeds into helpful and holistic intelligence.

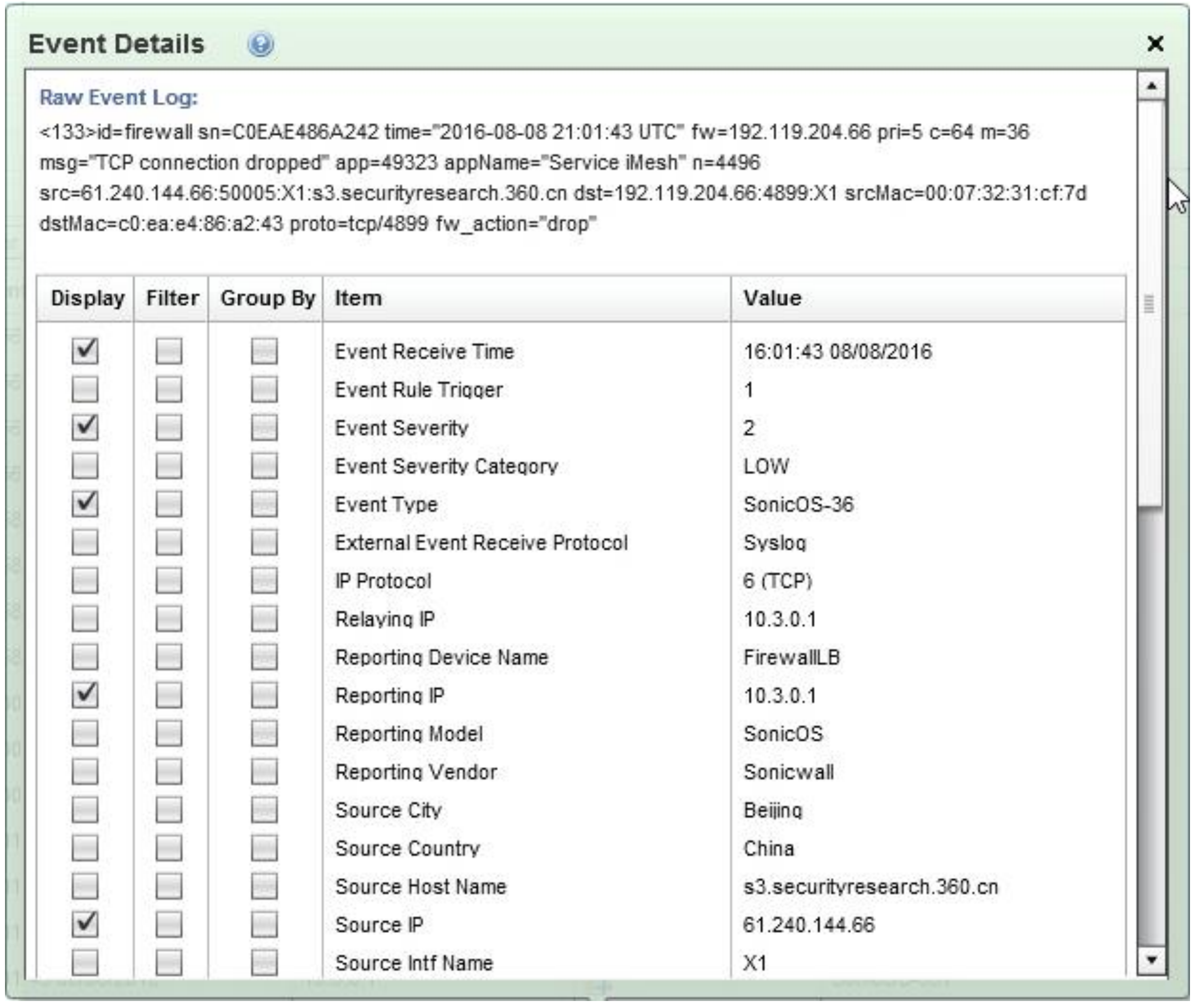
Network with SIEM



Pratum

What is an event log?

An event log is typically a string of information. The SIEM interprets this data and generally extracts key attributes to use for correlation.



Raw Event Log:

```
<133>id=firewall sn=C0EAE486A242 time="2016-08-08 21:01:43 UTC" fw=192.119.204.66 pri=5 c=64 m=36
msg="TCP connection dropped" app=49323 appName="Service iMesh" n=4496
src=61.240.144.66:50005:X1:s3.securityresearch.360.cn dst=192.119.204.66:4899:X1 srcMac=00:07:32:31:cf:7d
dstMac=c0:ea:e4:86:a2:43 proto=tcp/4899 fw_action="drop"
```

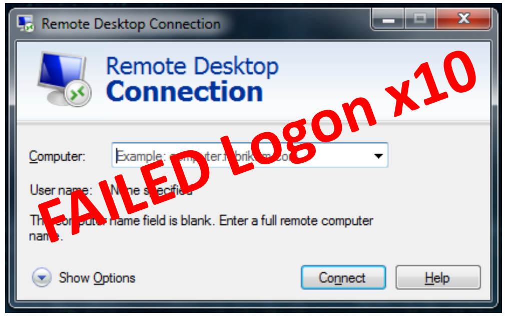
Display	Filter	Group By	Item	Value
☑	□	□	Event Receive Time	16:01:43 08/08/2016
□	□	□	Event Rule Trigger	1
☑	□	□	Event Severity	2
□	□	□	Event Severity Category	LOW
☑	□	□	Event Type	SonicOS-36
□	□	□	External Event Receive Protocol	Syslog
□	□	□	IP Protocol	6 (TCP)
□	□	□	Relaying IP	10.3.0.1
□	□	□	Reporting Device Name	FirewallLB
☑	□	□	Reporting IP	10.3.0.1
□	□	□	Reporting Model	SonicOS
□	□	□	Reporting Vendor	Sonicwall
□	□	□	Source City	Beijing
□	□	□	Source Country	China
□	□	□	Source Host Name	s3.securityresearch.360.cn
☑	□	□	Source IP	61.240.144.66
□	□	□	Source Intf Name	X1

Correlation

Public IP 139.130.4.5

Public IP 8.8.8.8

Public IP 8.8.4.4



Remote Desktop Connection

Remote Desktop Connection

Computer: Example: computer.fabrikam.com

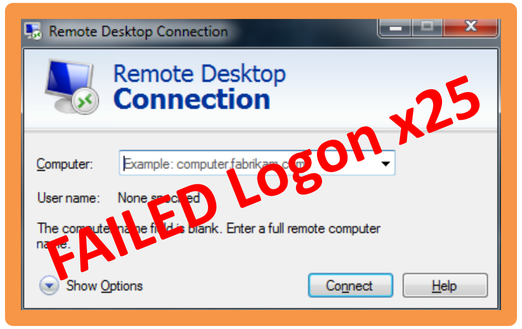
User name: None specified

The computer name field is blank. Enter a full remote computer name.

SIEM

Private IP 192.168.1.5

Public IP 139.130.4.5



Remote Desktop Connection

Remote Desktop Connection

Computer: Example: computer.fabrikam.com

User name: None specified

The computer name field is blank. Enter a full remote computer name.

It starts with… INFORMATION

- Log data from the correct devices.
  - Logging simply from your firewalls is not sufficient.

- Ensure the correct information from those devices is being audited.

SIEM’s intelligence will be limited by the data transmitted to it.

One of the

Best Defenses

Layered Defense

Identify Risk:

Business Data – PII/PCI/PHI/IP

Risk assessment / Gap analysis / Vulnerable / Existing controls

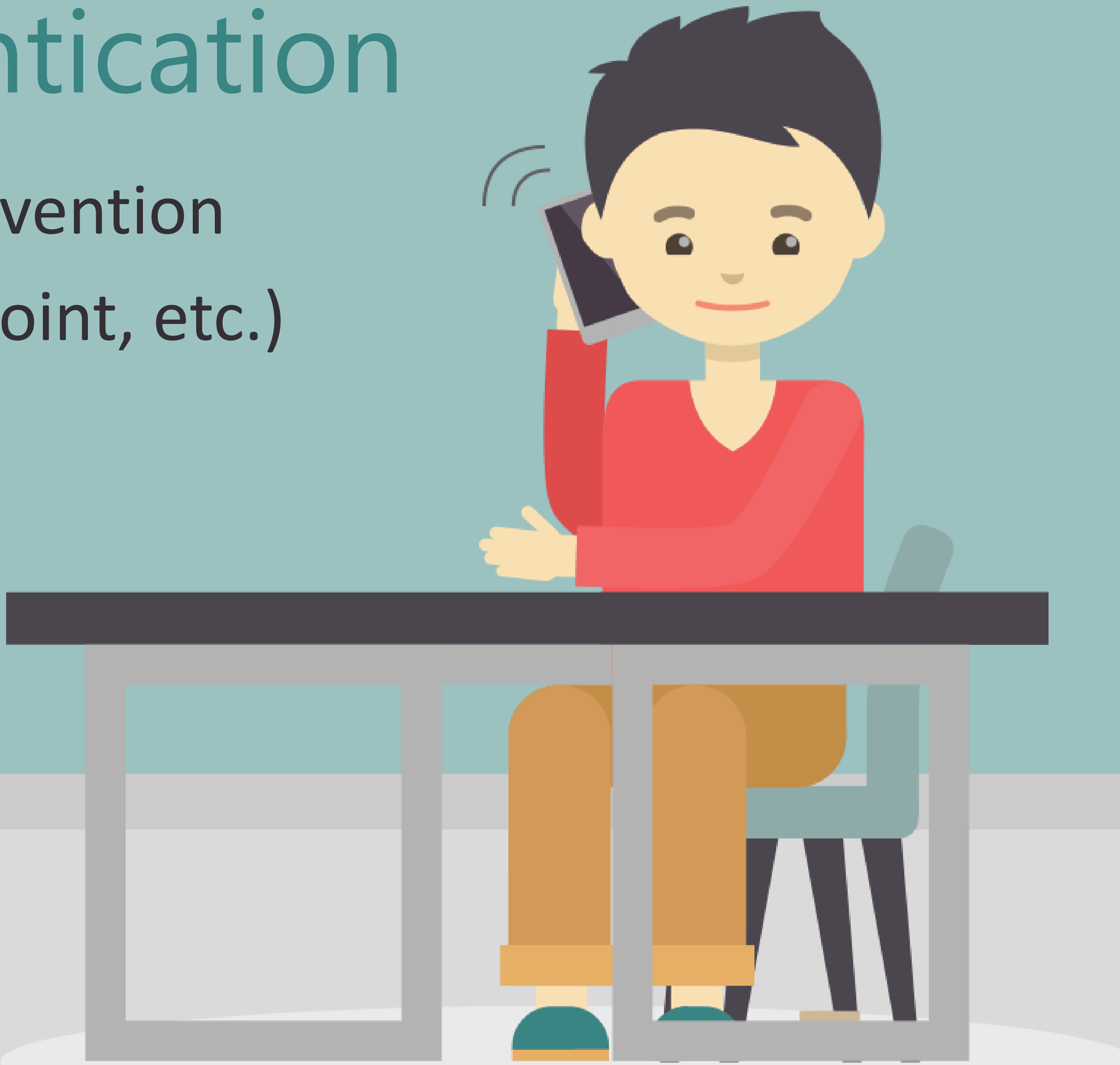
Monitor Key Areas:

Network Services (Firewalls/Core Switches), Authentication services (Domain Controllers), Security Services

(MDM, MFA, Web Applications, IDS/IPS, AV, vulnerability data)

Mobile Device Management
Multi-Factor Authentication

- Data exfiltration / Data loss prevention
- Cloud (AWS, 365, OWA, Sharepoint, etc.)
- Google SMS 2-factor Phishing



Device Auditing

The type of data being logged is critical.

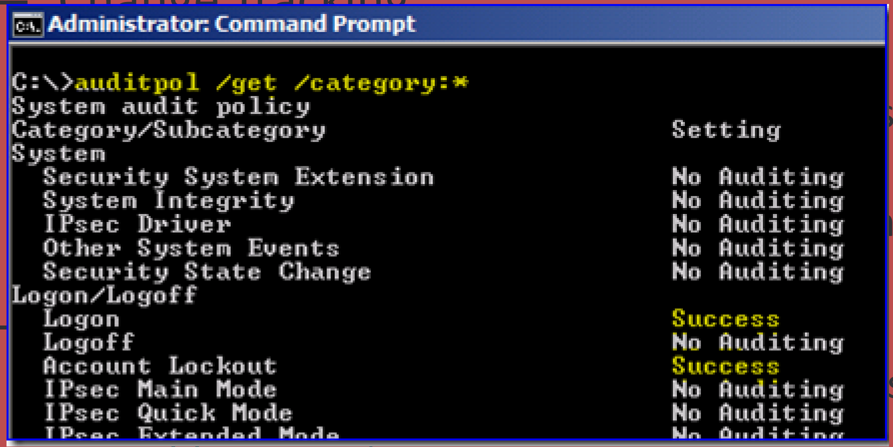
- Successful AND Failed Events
- Permitted Traffic AND Denied Traffic
- Change Tracking

s

heir own

–

ses,



Administrator: Command Prompt

```
C:\>auditpol /get /category:*
System audit policy
Category/Subcategory                      Setting
System
  Security System Extension               No Auditing
  System Integrity                        No Auditing
  IPsec Driver                            No Auditing
  Other System Events                     No Auditing
  Security State Change                   No Auditing
Logon/Logoff
  Logon                                   Success
  Logoff                                  No Auditing
  Account Lockout                         Success
  IPsec Main Mode                         No Auditing
  IPsec Quick Mode                        No Auditing
  IPsec Extended Mode                     No Auditing
```

Auditpol.exe /get /category:*

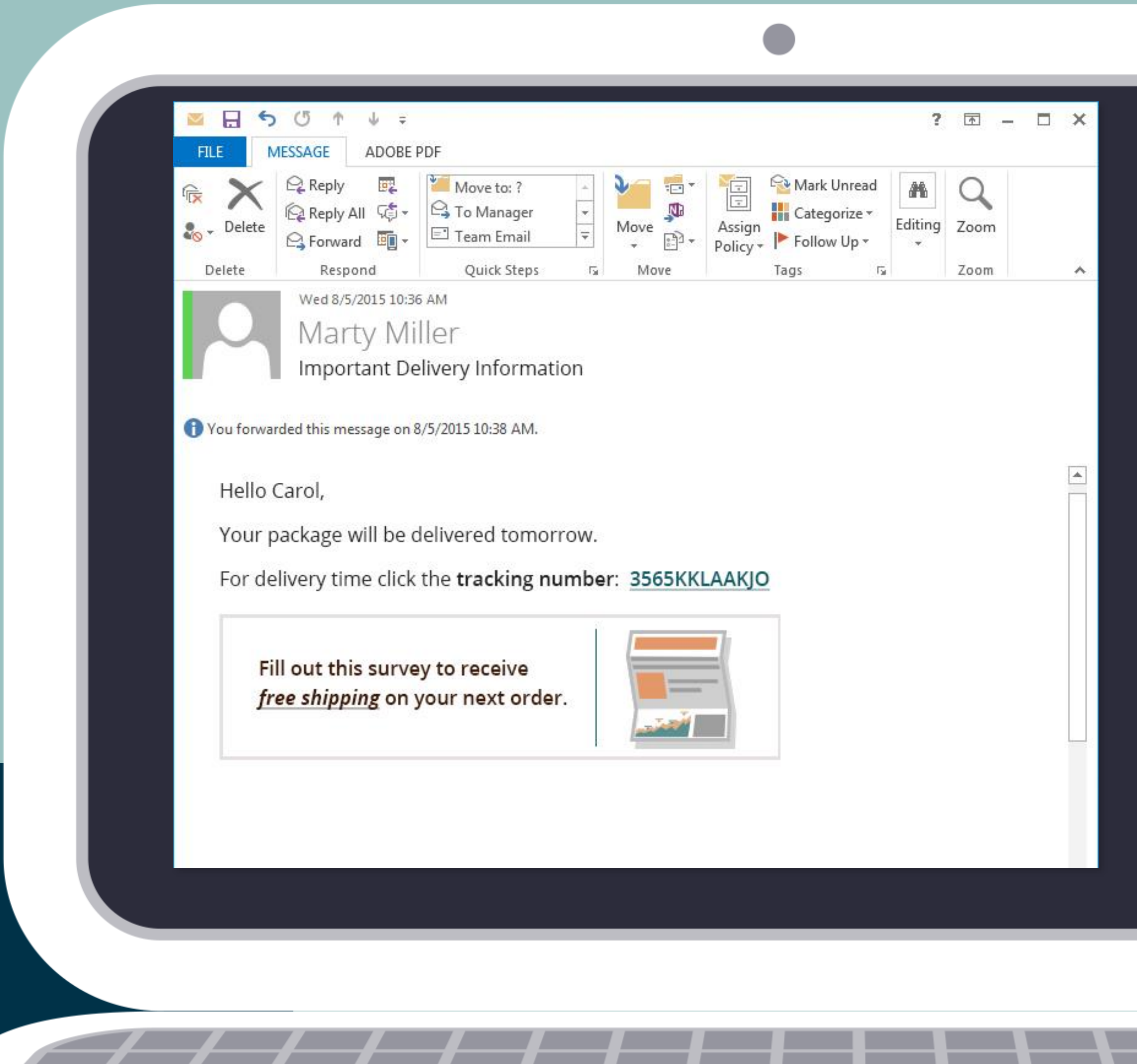
Evaluate Risk Scenarios

Social engineering is a component of the attack in nearly 1 of 3 successful data breaches, and it's on the rise.

Source: 2016 Verizon Data Breach Investigation Report

Ninety percent of data breaches seen by Verizon's data breach investigation team have a phishing or social engineering component to them. Not coincidentally, one of the hottest commodities on underground or dark web marketplaces are credentials, which attackers can use to log into enterprises and make it appear that they're legitimate users.

How would your SIEM help to identify this type of successful or failed attack?



Wed 8/5/2015 10:36 AM

Marty Miller

Important Delivery Information

You forwarded this message on 8/5/2015 10:38 AM.

Hello Carol,

Your package will be delivered tomorrow.

For delivery time click the **tracking number**: 3565KKLAAKJO

Fill out this survey to receive *free shipping* on your next order.

Benefits of deeper auditing

- Carol.Lorac attempted access to the folder ‘Payroll’ in the HR share
- Service ryuxiouerlruyerlljkrr.exe was added to the registry’s startup path
- The whoami command was executed on the domain controller at 2:48 AM, followed by ipconfig, tasklist, and net use

You’ve been compromised, now what?

The SIEM is one of the best tools to assist with incident response. An investigator can quickly sift through data much faster.

- Visibility
- Data is readily available for investigation
- Answers can be obtained
  - Is the threat contained?
  - What data, how much?
  - How did they get in?
  - Who was it?

Sysmon - SysInternals

```
<14>May 16 09:48:49 DC03 MSWinEventLog        1         Microsoft-Windows-
Sysmon/Operational  136785325     Tue May 16 09:48:49 2017    1          Microsoft-
Windows-Sysmon      SYSTEM            User    Information    DC03   Process Create
(rule: ProcessCreate)             Process Create:  UtcTime: 2017-05-16 14:48:49.013
ProcessGuid: {23AC7C4B-1151-591B-0300-00105DAB2337}  ProcessId: 2153028
Image: C:\Windows\System32\whoami.exe  CommandLine: whoami
CurrentDirectory: C:\Users\shealey\  User: INTEGRITY\shealey  LogonGuid:
{23AC7C4B-1146-591B-0300-0020663C1F37}  LogonId: 0x3371F3C66
TerminalSessionId: 10  IntegrityLevel: Medium  Hashes:
MD5=D609D59A042C04A50EB41EC5D52F7471  ParentProcessGuid: {23AC7C4B-
114F-591B-0300-001043142237}  ParentProcessId: 2152948  ParentImage:
C:\Windows\System32\cmd.exe  ParentCommandLine:
"C:\Windows\system32\cmd.exe"   299968125
```

Advanced Audit Policies

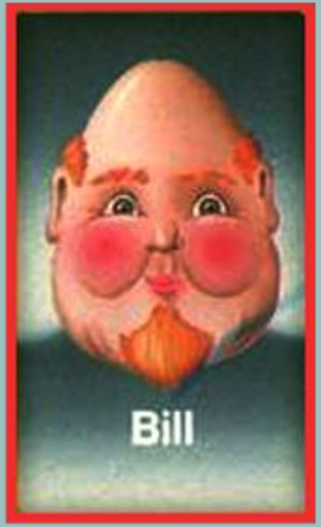
Windows advanced audit policy settings allow you to select only the behaviors that you want to monitor. You can exclude audit results that are not needed.

- Changes to user and computer accounts – Account Management
- Activities of individual applications and users – Detailed Tracking
- Directory Services access/changes – DS Access
- Logon/Logoff, Object Access, Policy Change, Privilege Use, System, SACLs.
- Registry, Services, Processes, Firewall/network, Alerts

False Positives/Exceptions

Ensure exceptions being created don’t hinder the original intent of the security rule. Find the balance and enhance the logic.

Alex
Alfred
Anita
Anne
Bernard
Bill
Charles
Claire
David
Eric
Frans
George
Herman
Joe
Maria
Max
Paul
Peter
Philip
Richard
Robert
Sam
Susan
Tom



THREAT

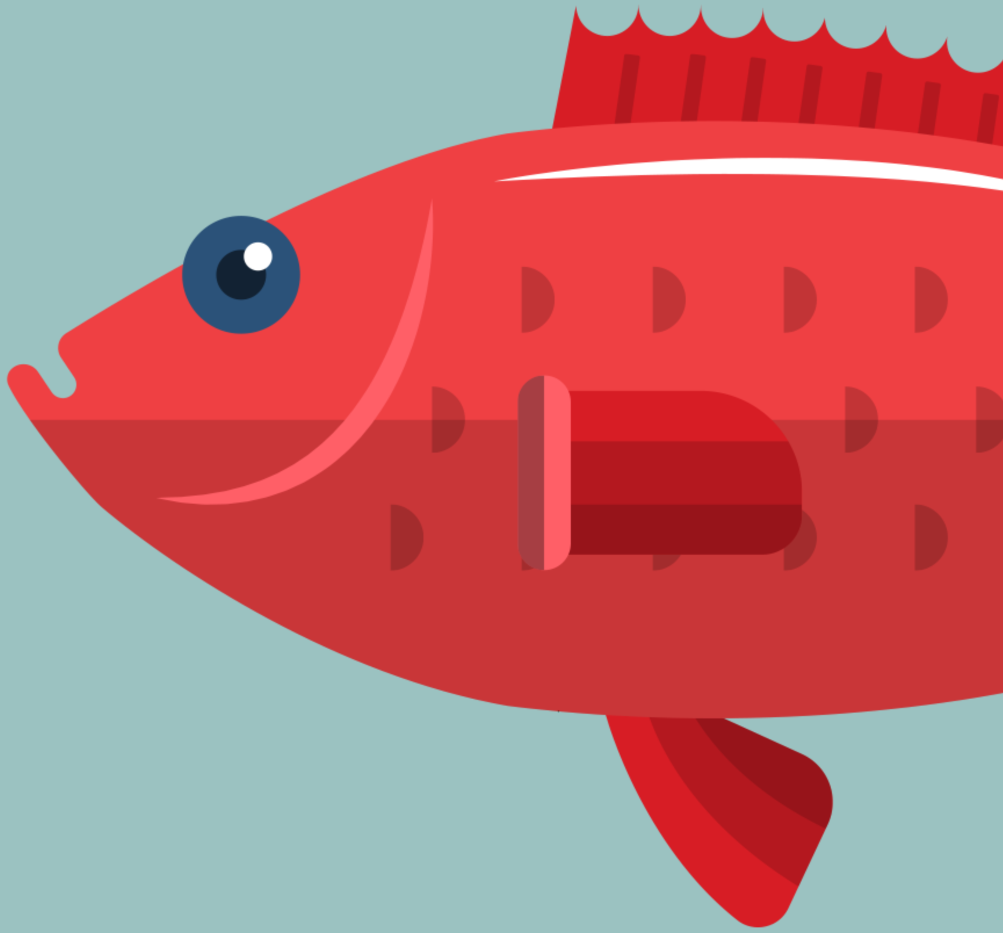
FALSE POSITIVE

Security Monitoring takes time

False positives, true positives, actual security incidents.

Incidents should be generating frequently as businesses are dynamic and so are employees.

Example Alert: Successful VPN Logon from Outside the Country from Herman Miller.



Reporting

- Integrate the SIEM into business processes such as change management/user access review.
- Embrace compliance reports
  - Don’t simply check the box
  - Allow the SIEM to provide checks and balances
- Answers to questions

Takeaways

- Implement a SIEM (Gain visibility into your business)
- Send data from the correct devices
- Audit the correct types of events from each device
- Tune the rules and review them

OR

- Contact Pratum for a fully managed SIEM as a service offering.

Questions?

steve.healey@pratum.com

www.pratum.com/blog

515-965-3756