vijilan
IT Security: Enabled

24/7 Cyber-Security Intelligence Services

Detection and removal of threats from the corporate network, 24/7.

Cyber-security by the numbers

- **76%** of websites contain vulnerabilities
- **496,657** Web attacks blocked per day
- **1 in 965** Emails is a phishing attack
- **317M** New malware variants yearly
- **113%** Increase in ransomware / CryptoLocker style attacks in 2014
- **28%** of malware is virtual-machine aware
- **23%** increase in breaches in 2014
- **1.9M+** Malicious web robots

Source: Symantec Internet Security Threat Report, April 2015

Traditional / typical security measures

- Firewall
  - Monitors incoming and outgoing network traffic and acts as a barrier to traffic that doesn’t meet certain requirements.
- Intrusion Detection System / Intrusion Prevention System
  - Looks for suspicious patterns in network traffic.
- Anti-Virus
  - Identifies malware based upon known patterns or suspicious program behaviors.
- Securely Configured Routers and Switches
  - Ensure security gaps don’t form at connection points with the internet or other network area.

Why the small and medium business?

“We are absolutely facing an epidemic of attacks on our nation's infrastructure and attempts to gain access to information. But smaller organizations tend to be easier and more attractive targets for cyber criminals.”

Jason Oxman, CEO

Electronic Transactions Association

- Fewer resources
- Minimal security expertise
- Inferior (or freeware) anti-virus
- Less advanced security layers
- Prone to bank online
- Less stringent security policies

Attacks could have been prevented

> “In nearly all examples of successful breaches, evidence of compromise was readily available in the device log data.”

Source: Verizon Data Breach Investigation Report

The requirements for effective security

Infrastructure

- Firewalls
- IDS/IPS
- Anti-Virus

Technology

- SIEM

(Security Information and Event Management)

- Log Collection
- Log Correlation

Human Expertise

- Threat Experience
- Advanced Training
- 24/7 Vigilance

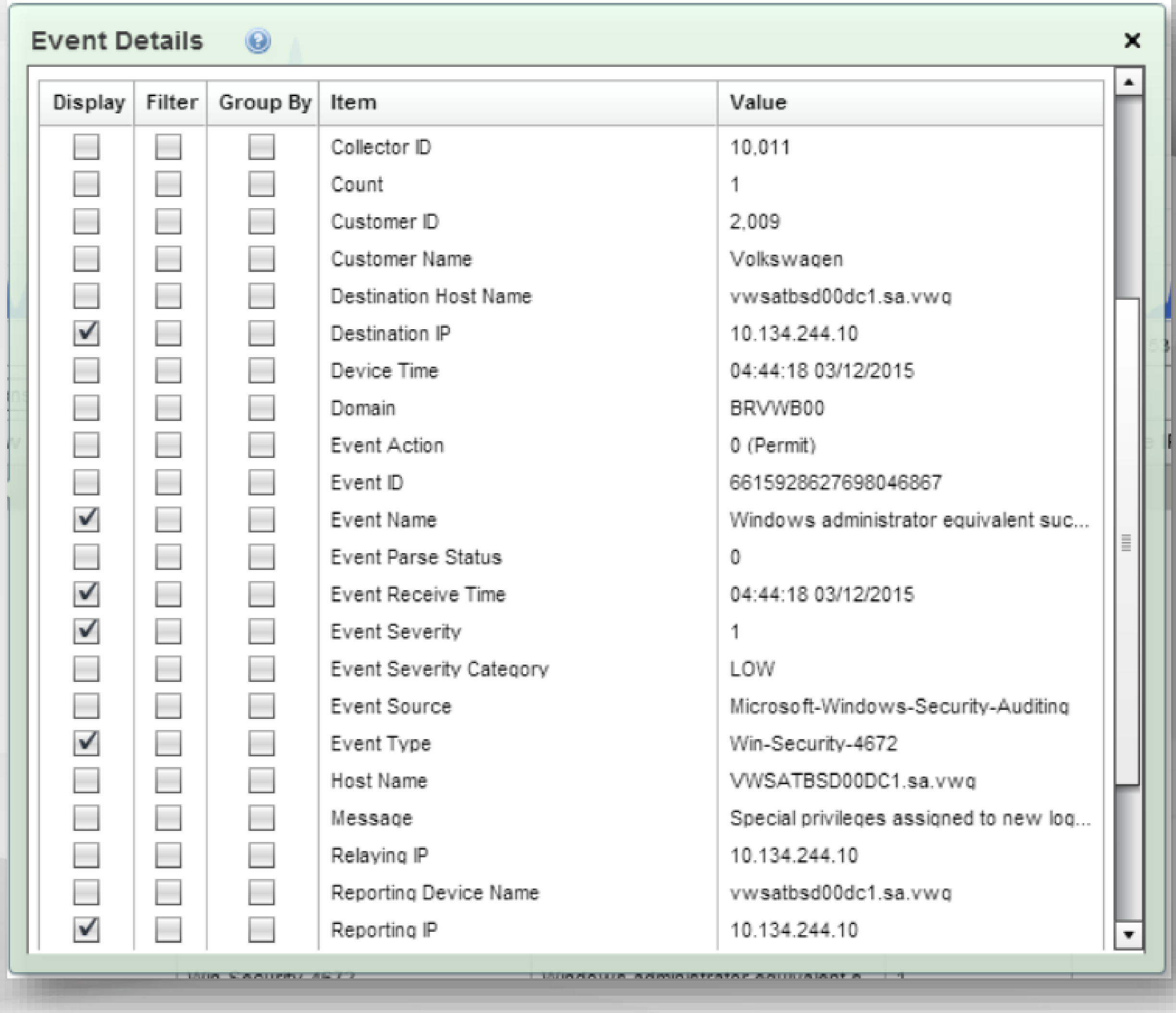
What is a log / event file?

- Machine language that records each event a device performs
- Generated several times per second
- Example:

```
[ComputerName]="VWSATBSD00DC1.sa.vwg" [Data]="NULL" [EventCode]="4672"
[EventIdentifier]="4672" [EventType]="4" [Logfile]="Security" [RecordNumber]="1255306321"
[SourceName]="Microsoft-Windows-Security-Auditing" [TimeGenerated]="20150312084346.907957-
000" [TimeWritten]="20150312084346.907957-000" [Type]="Audit Success" [User]="(null)"
[Message]="Special privileges assigned to new logon." [[Subject]] [Security ID]="S-1-5-18" [Account
Name]="VWSATBSD00DC1$" [Account Domain]="BRVWB00" [Logon ID]="0xe79eda1c"
[Privileges]="SeSecurityPrivilege,SeBackupPrivilege,SeRestorePrivilege,SeTakeOwnershipPrivilege,SeDe
bugPrivilege,SeSystemEnvironmentPrivilege,SeImpersonatePrivilege,SeLoadDriverPrivilege,SeEnableDel
egationPrivilege,SeCreateTokenPrivilege,SeAuditPrivilege,SeTcbPrivilege"
```

Event Data Normalization (Parsing)

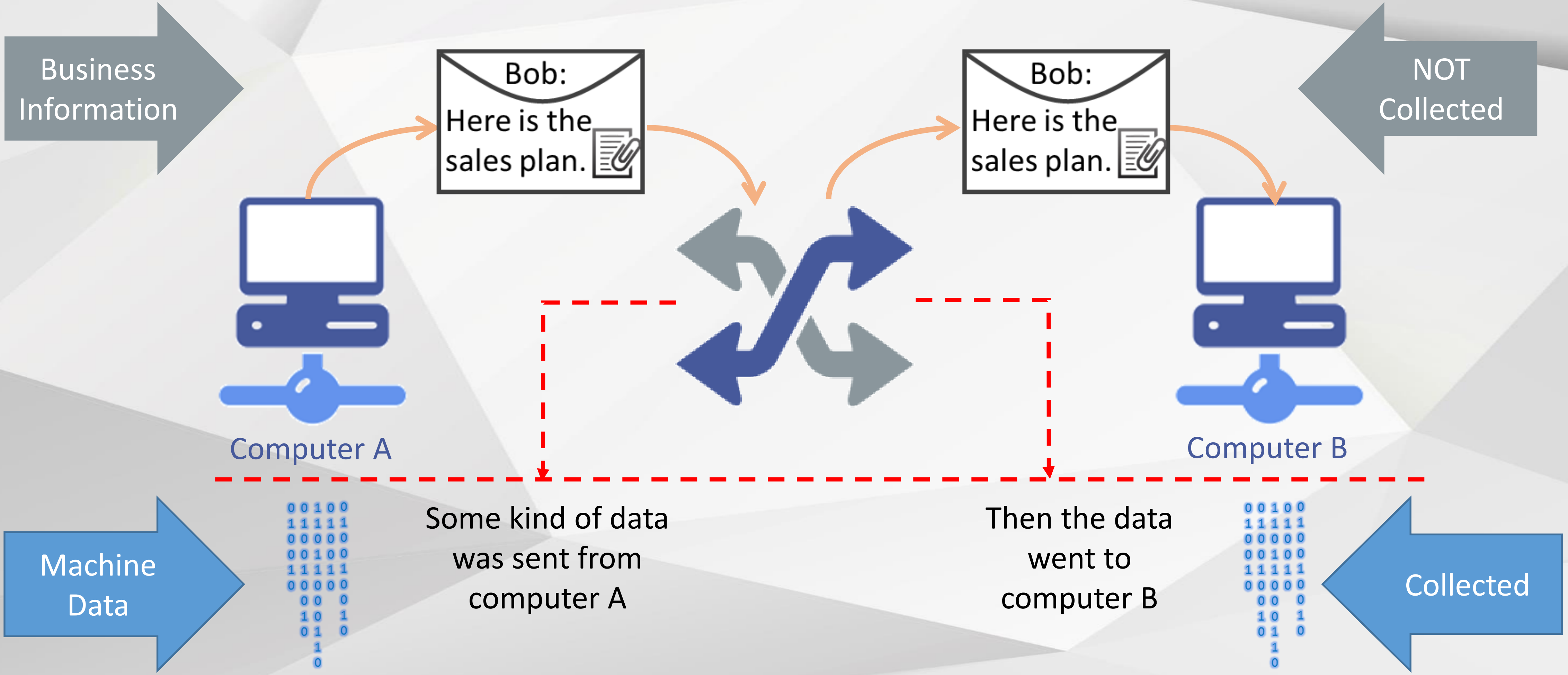
```
 [ComputerName]="VWSATBSD00DC1.sa.vwg" [Data]="NULL"
[EventCode]="4672" [EventIdentifier]="4672" [EventType]="4"
[Logfile]="Security" [RecordNumber]="1255306321"
[SourceName]="Microsoft-Windows-Security-Auditing"
[TimeGenerated]="20150312084346.907957-000"
[TimeWritten]="20150312084346.907957-000" [Type]="Audit
Success" [User]="(null)" [Message]="Special privileges
assigned to new logon." [[Subject]] [Security ID]="S-1-5-18"
[Account Name]="VWSATBSD00DC1$" [Account
Domain]="BRVWB00" [Logon ID]="0xe79eda1c"
[Privileges]="SeSecurityPrivilege,SeBackupPrivilege,SeRestoreP
rivilege,SeTakeOwnershipPrivilege,SeDebugPrivilege,SeSystem
EnvironmentPrivilege,SeImpersonatePrivilege,SeLoadDriverPri
vilege,SeEnableDelegationPrivilege,SeCreateTokenPrivilege,Se
AuditPrivilege,SeTcbPrivilege"
```



Event Details

Display	Filter	Group By	Item	Value
□	□	□	Collector ID	10,011
□	□	□	Count	1
□	□	□	Customer ID	2,009
□	□	□	Customer Name	Volkswagen
□	□	□	Destination Host Name	vwsatbsd00dc1.sa.vwg
☑	□	□	Destination IP	10.134.244.10
□	□	□	Device Time	04:44:18 03/12/2015
□	□	□	Domain	BRVWB00
□	□	□	Event Action	0 (Permit)
□	□	□	Event ID	6615928627698046867
☑	□	□	Event Name	Windows administrator equivalent suc...
□	□	□	Event Parse Status	0
☑	□	□	Event Receive Time	04:44:18 03/12/2015
☑	□	□	Event Severity	1
□	□	□	Event Severity Category	LOW
□	□	□	Event Source	Microsoft-Windows-Security-Auditing
☑	□	□	Event Type	Win-Security-4672
□	□	□	Host Name	VWSATBSD00DC1.sa.vwg
□	□	□	Message	Special privileges assigned to new log...
□	□	□	Relaying IP	10.134.244.10
□	□	□	Reporting Device Name	vwsatbsd00dc1.sa.vwg
☑	□	□	Reporting IP	10.134.244.10

What kind of data is collected and stored?



Business Information

NOT Collected

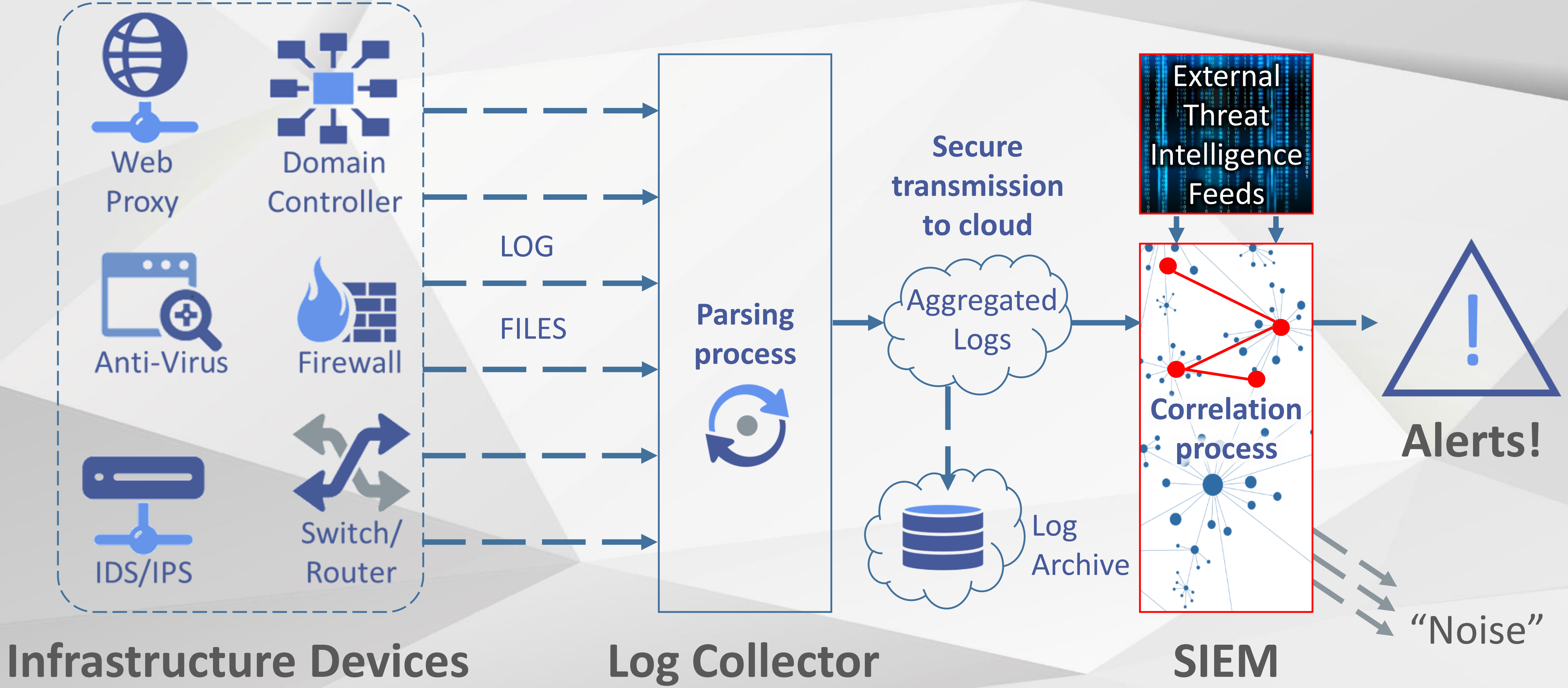
Machine Data

Collected

Some kind of data was sent from computer A

Then the data went to computer B

What is SIEM?

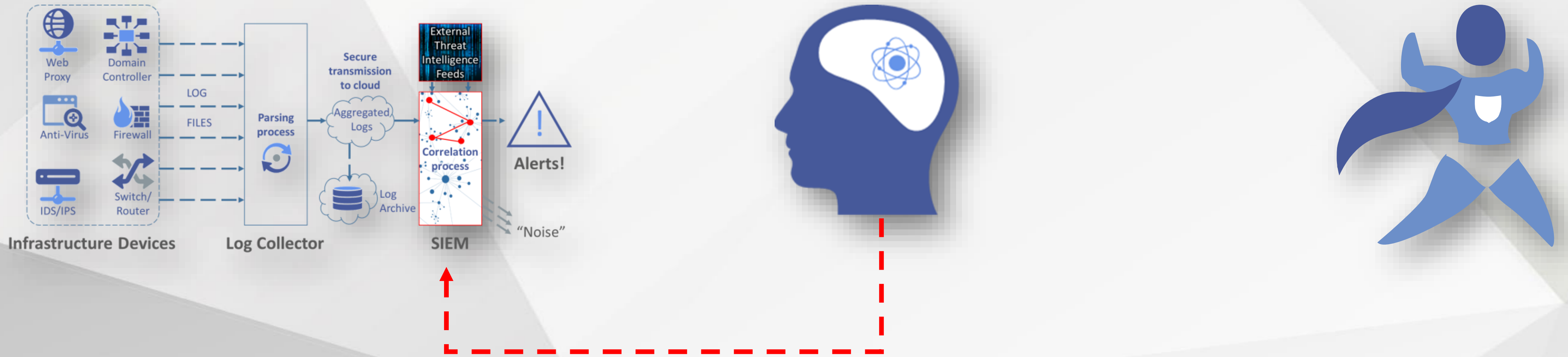

Web Proxy
Domain Controller
Anti-Virus
Firewall
IDS/IPS
Switch/ Router
LOG
FILES
Parsing process
Secure transmission to cloud
Aggregated Logs
Log Archive
External Threat Intelligence Feeds
Correlation process
Alerts!
"Noise"
Infrastructure Devices
Log Collector
SIEM

24/7 Cyber-security process

Automated Detection

Human Expert Analysis

Timely Incident Response

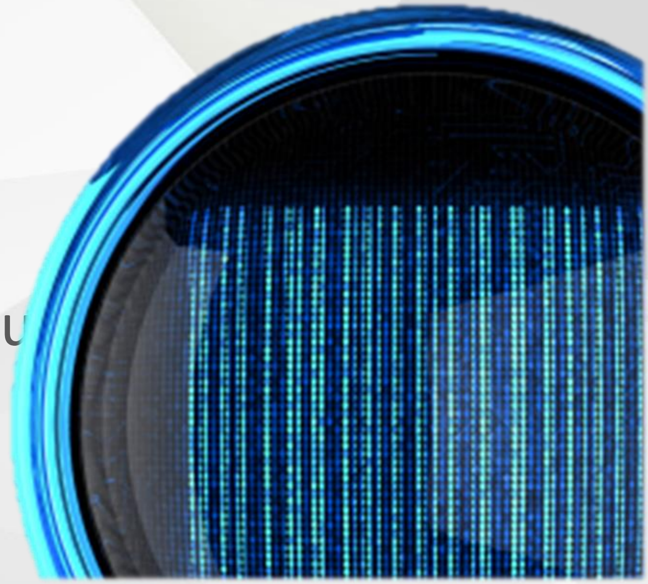


Web Proxy
Domain Controller
Anti-Virus
Firewall
IDS/IPS
Switch/ Router
LOG
FILES
Parsing process
Secure transmission to cloud
Aggregated Logs
Log Archive
External Threat Intelligence Feeds
Correlation process
Alerts!
"Noise"
Infrastructure Devices
Log Collector
SIEM

- New Threat Intelligence
- Advanced Correlation Rules
- New Malicious URL Data

Benefits of 24/7 Security Services

- Optimize your existing security investment
  - Insight into the interactions of your complex environment
- Be assured hackers and cyber-criminals don’t go un-noticed
  - Experts can see hacking, espionage and malicious actions as they occur in real-time
- Limit the impact of zero-day malware outbreaks
  - Spots malware patterns and provides alerts before extensive damage is done
- Ensure security policies are enforced
  - Complements other tools to aid in spotting rogue employee/u behaviors



Aids in regulatory compliance

PCI-DSS

Payment Card Industry-Data Security Standards

SOX

Sarbanes-Oxley

GLBA

The Gramm–Leach–Bliley Act

NCUA

National Credit Union Code of Federal Regulations part 748

FDIC

IT Risk Management Program (RMP)

HIPAA

Health Insurance Portability and Accountability Act

We can help!

Our organization provides:

- “Hand’s-off” Security
  - Leave it to us!
- Consultation on 24/7 monitoring options
- Around-the-clock cyber-threat detection
- Advanced threat analysis
- Rapid cyber-threat remediation

Our key service offering

Threat
RESPOND

- Consultation on monitoring priority
- Log collector in virtual appliance form factor
- 24/7 Real-time, automated cyber threat detection
- Incident notification
- 24/7 Threat analysis and reporting by human engineers
- Basic device performance data
- Advanced Security Engineers provide threat response and remediation around-the-clock

Don’t delay

- A 2014 survey of 59 US firms by the Ponemon Institute and HP found the average annual cost of responding to cyber attacks was $12.7 million, up 96 percent over the previous five years.
- McKinsey research shows that companies are struggling with their capabilities in cyber-risk management.
- Norse Security recently showed - in just 45 minutes, the U.S. was the victim of 5,840 cyberattacks.

Source: Business Insider. Norse Hacking Map, June 2014
Source: HP Cost of Cybercrime Study, 2014
Source: McKinsey - The Rising Strategic Risks of Cyberattacks, May 2014

Thank You!

We’d like to be your trusted provider of 24/7 Cyber-Security Services