RED TIGER SECURITY

Incident Management Workshop

2012 SANS SCADA Summit

Orlando, Florida

Jonathan Pollet – CISSP, PCIP, CAP

- 12 Years of Electrical Engineering, SCADA, Industrial Controls, and IT Experience
  - PLC Programming and SCADA System Design and Commissioning
  - Wireless RF and Telecommunications Design and Startup
  - Front-end Web Development for SCADA data
  - Backend Database design for SCADA data
  - Acting CIO for Major Oil Company for 2 years – Enterprise IT Management
- Last 8 Years Focused on SCADA and IT Security
  - Published White Papers on SCADA Security early in 2001
  - Focused research and standards development for SCADA Security since 2002
  - Conducted over 120 security assessments on Critical Infrastructure systems
  - Conducted over 75 International conferences and workshops on CIP
  - Developed safe security assessment methodology for live SCADA Systems
  - Co-developed the SCADA Security Advanced 5-day training course

Outline

- Why is Incident Management so Important? (30 min)
  - Dive into several recent real-world cyber incidents to find out how the attackers got in, and why they were not detected for over 18 months.
- How to Extract Meaningful Cyber Incident data from SCADA Components? (30 min)
  - SCADA System elements are not like IT systems and they do not all generate logs and alerts in the same way as IT systems. This session will discuss how to leverage SNMP, Syslog, and data hidden inside embedded devices and application-specific logs to extract cyber incident data.
- Intrusion Detection, End Point Security, and Security Event Management Systems for SCADA Systems (30 min)
  - Deploying IDS and IPS Solutions within SCADA Systems are different than the typical IT deployments. This session will not only define the difference between IDS and IPS systems, but also provide practical tops as to where to place these components. End Point Security technologies such as Antivirus and Application Whitelisting will be compared and contrasted, and this session will end up with best practices for implementing SEM (Security Event Management) Systems as a Central Repository for all incident data.
- Building an Effective Internal CERT Team (30 min)
  - The last section of the workshop will discuss setting up an effective CERT (Computer Emergency Response Team), the types of skill sets required in the team, and scenarios that can be practiced that start with Incident Response and follow through with Incident Recovery.

RED TIGER SECURITY

Why is Incident Management so Important? (30 min)

New SCADA Attacks - APT, Night Dragon, and Stuxnet – everybody is kung fu fighting ☺

RED TIGER SECURITY

wall of shame….

what were they thinking….

RED TIGER SECURITY

notice anything?

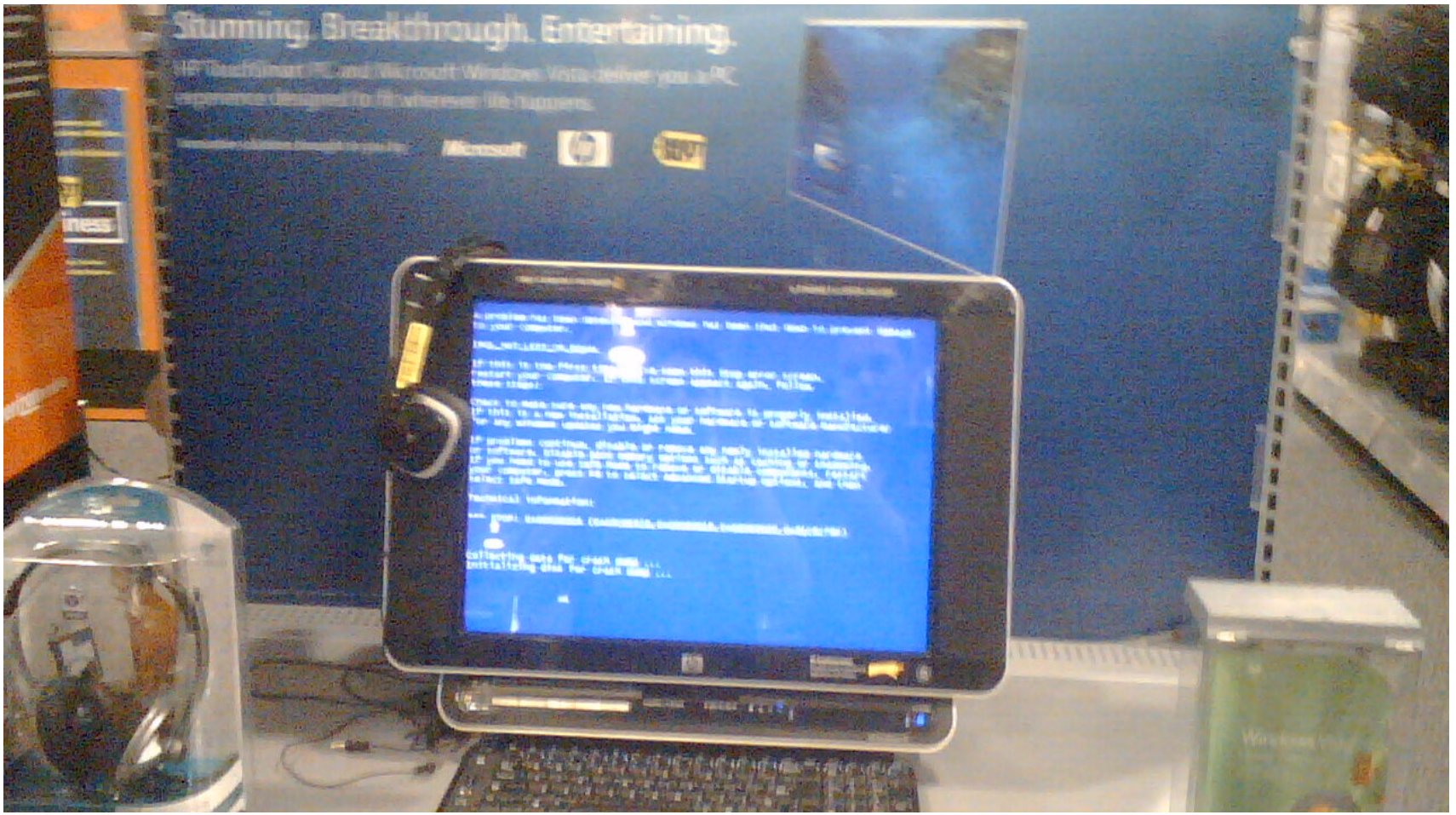
RED TIGER SECURITY

this machine is used to swipe credit cards, is connected to the Internet, and has the username/ password in clear sight…

RED TIGER SECURITY

microsoft vista...

you want to run your control system on this – right?



RED TIGER SECURITY

employees are lazy

RED TIGER SECURITY

…or malicious… this was a female showering facility…

RED TIGER SECURITY

vendors aren't any better…

who builds a cash register with an Ethernet port dangling from it?

RED TIGER SECURITY

attackers assume smart people make mistakes

the bad stuff

update on the Threat Landscape with a focus on
APT, Night Dragon, and Stuxnet

the bad stuff

- Threat Profile
  - External Threats
    - Intentional Targeted Advanced Persistent Threats (APT)
    - Unintentional External Threats
  - Internal Threats
    - Contractors
    - Employees
  - Financial Threats
    - FERC fines
    - Impact on shareholder value
    - Cost of APT infection remediation

Entry Points for the Attacker

- Malware / Worms
  - 2009 May – July
  - 1335 Unique variants and infections
    - Inclu. Conficker Worm / Conficker A, B, C, D and E
    - Malicious AV Advertisements/Products
    - Segmentation of the Network (ITSG-ITSB)
- Mobile Devices
  - USB drives
    - U3 Devices
  - Stolen or lost Laptops
- Insecure Builds
  - Devices that are mis-configured / unpatched before activation

RED TIGER SECURITY

Entry Points for the Attacker (Con't)

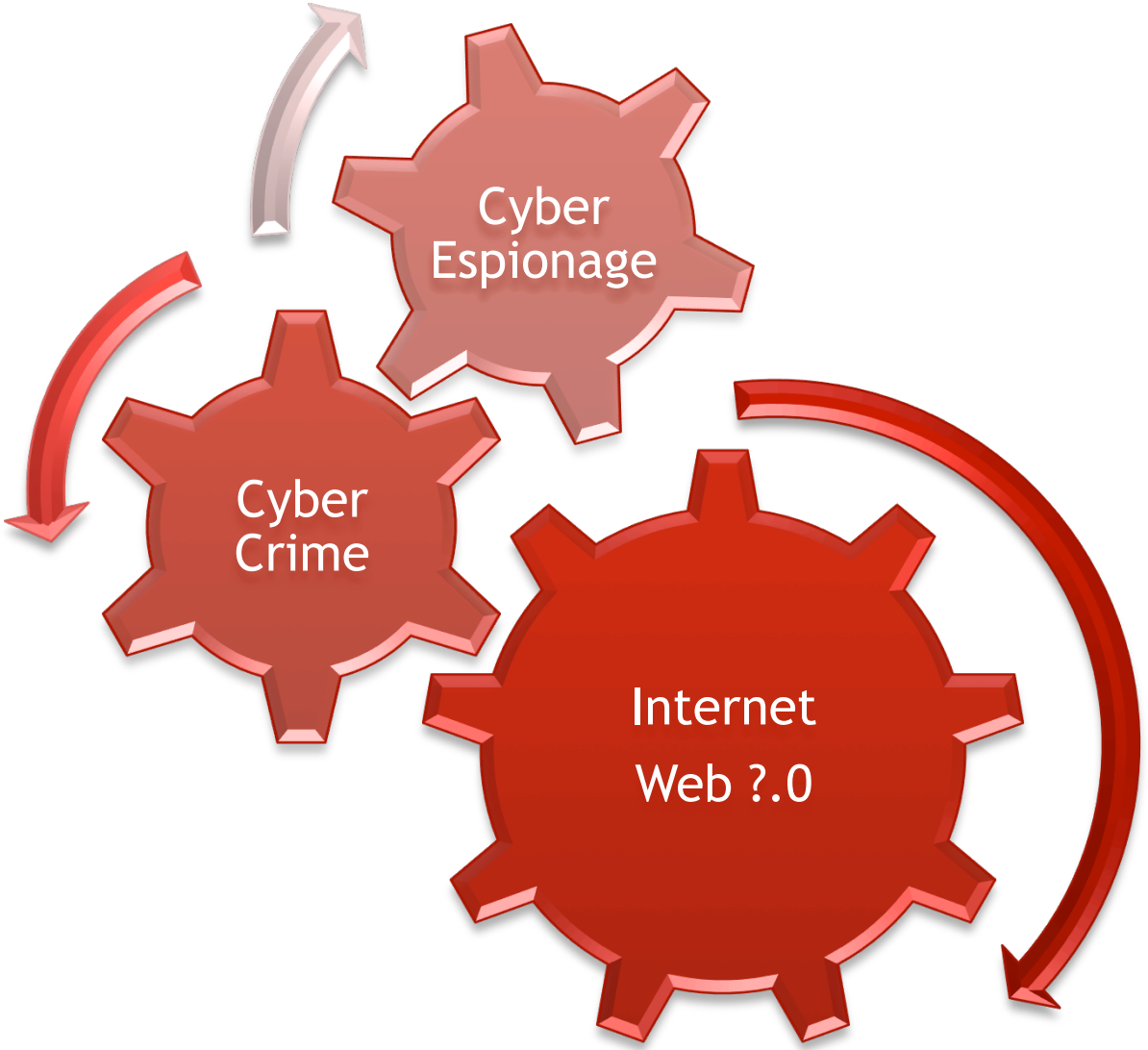
- Information leakage
  - Exposure of sensitive media / material online
  - Small / Irrelevant
- Application Security
  - Fuzzing / Reverse Engineering
  - Overflows, Cross Site Scripting,
- Social Engineering
  - Spear phishing
  - Social Engineering Toolkit (SET) Framework

RED TIGER SECURITY

Tools of the Trade

- Open Sourced Information
- Search Aggregators
- Malware:
  - Botnets
  - Crimeware
  - Rootkits
  - Malicious Attachments
- Live DVD – Distributions
  - Backtrack
  - A.P.E.

Symbiotic Progression



Don’t take my word for it…

- General Keith Alexander
  - Head, US Cyber Command
  - On Operation Buckshot Yankee
  - "probed by unauthorized users approximately 250,000 times an hour, over six million times a day.”

- Richard A. Clark
  - "It is the public, the civilian population of the United States and the publicly owned corporations that run our key national systems, that are likely to suffer in a cyber war."

- William J. Lynn III,
  - Deputy Secretary of Defense
  - "Computer-induced failures of U.S. power grids, transportation networks, or financial systems could cause massive physical damage and economic disruption”

- Jonathan Evans
  - Head MI-5
  - Both traditional and cyber espionage continue to pose a threat to British interests, with the commercial sector very much in the front line along with more traditional diplomatic and defense interests

attack methodology

skills and methodology used in construction of APT

RED TIGER SECURITY

Techniques

- OSINT
- Social Engineering
- Targeted “Spear Phishing”
- Malicious Attachments
- USB devices
- Websites

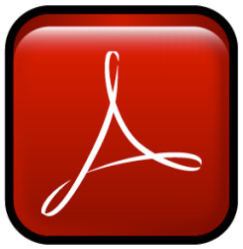
RED TIGER SECURITY

Targeted Spear Phishing

- Require in-depth knowledge of the target
- Sophistication based on posted / known information
- Seemingly benign small amounts of information leveraged to gain trust and access to specific people / groups

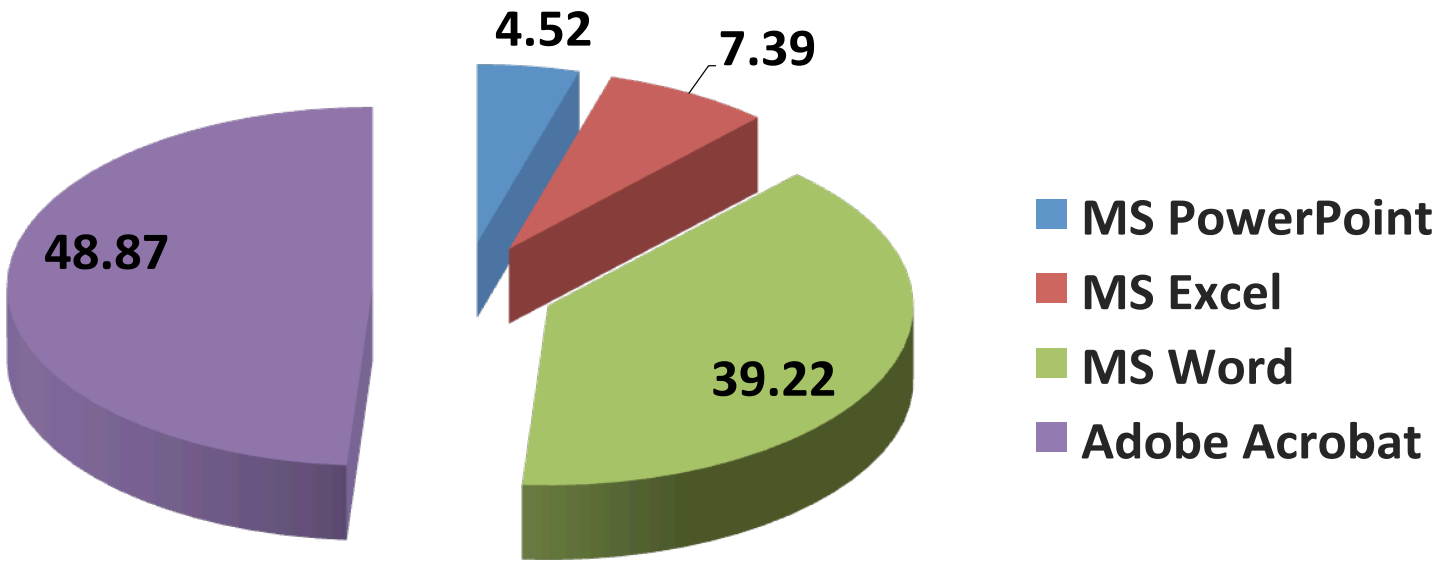
Malicious Attachments (Malware)

- PDF
- MS Products
  - Word, Excel, etc…



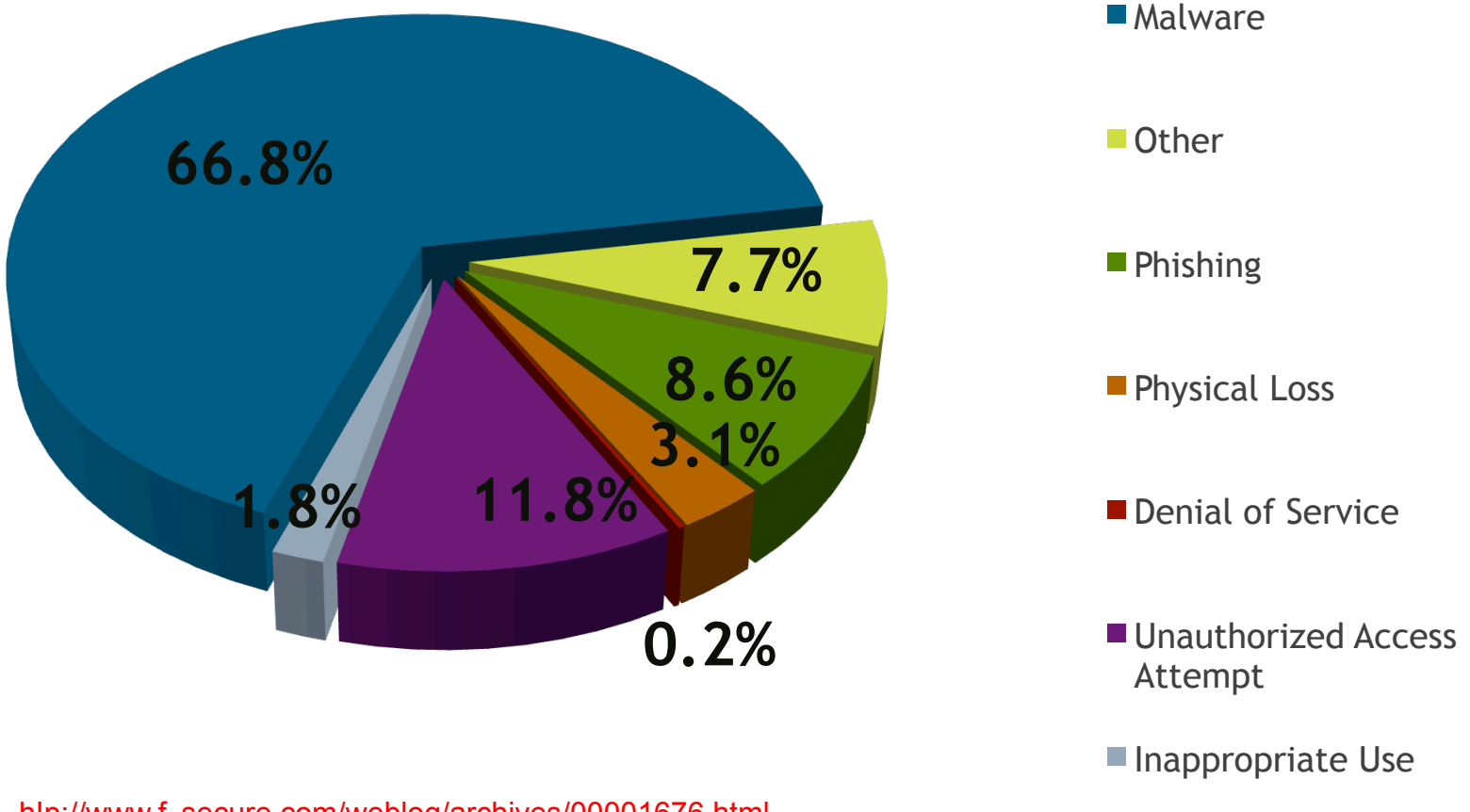
- The usual suffixes…
  - mp3, exe, lnk, dll, mov, com, mp4, bat, cmd, reg, rar, emf, shs, js, vb, yourcompany.com.zip, cab, mda, zip, mdb, scr, aiff, mde, cpl, msi, vbs, aif, m4p, msp, fdf, mdt, sys, wmf, hlp, hta, pif, jse, qef, scf, chm, <#>.txt, wsf, fli, vbe

Infection Point (by app)



hlp://www.f-secure.com/weblog/archives/00001676.html

Malware favored as attack vector



hIp://www.f-secure.com/weblog/archives/00001676.html

Hardware backdoor

- Provision of devices/ equipment that have “malware” already
  - Projectors
  - Printers
  - Photocopiers
    - Flash memory
  - W32 Spybot worm

- http://en.community.dell.com/dell-blogs/Direct2Dell/b/direct2dell/archive/2010/07/21/dell-on-the-server-malware-issue.aspx

Malware Kits

- Proliferation of cheap and easy to use
  - Free (Webattacker)
  - Torrents, P2P
- Complex $7,000 kits
  - 12+ kits available every 3-4 months
  - Zeus (ZBOT)
  - GHOSTNET (GHOSTRAT)
  - MUMBA (Zeus v3)
  - Mariposa

Command and Control (C&C)

- Leverages communication systems to relay messages
- Command Vectors
  - **Twitter**
  - IRC
  - Facebook
  - Google Groups

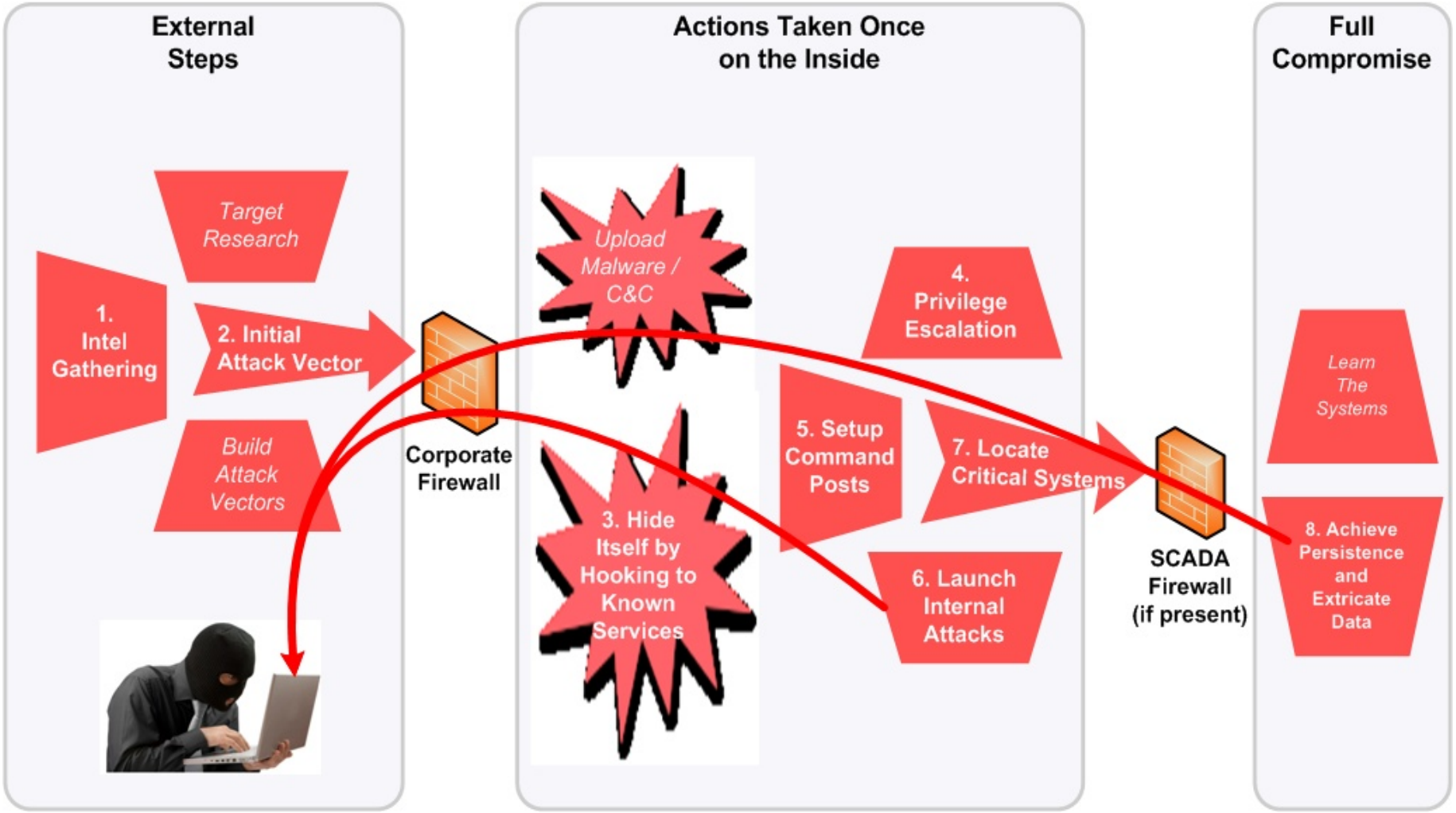
Night Dragon… Staged attack

- Series of weeks/months to fully compromise a system
- Incremental uploads/downloads/xchanges
- Results are fully “rooted” devices
- Random “radio” silence
  - Remain hidden,

What are they after…

- Intellectual Property
  - Code
  - Applications
  - Protocols
- Designs
  - Schematics
  - Drawings
  - Illustrations
- Chemical / Biological
  - Formula's
  - Equations
  - Chemical Compounds

APT – Steps to compromise

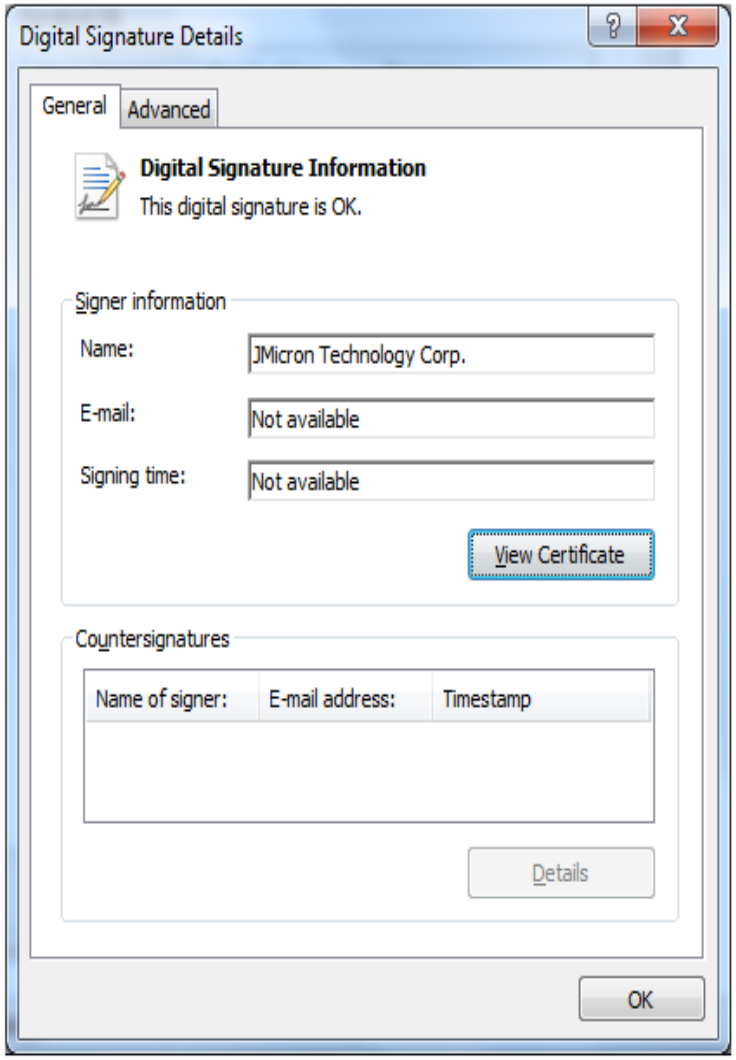


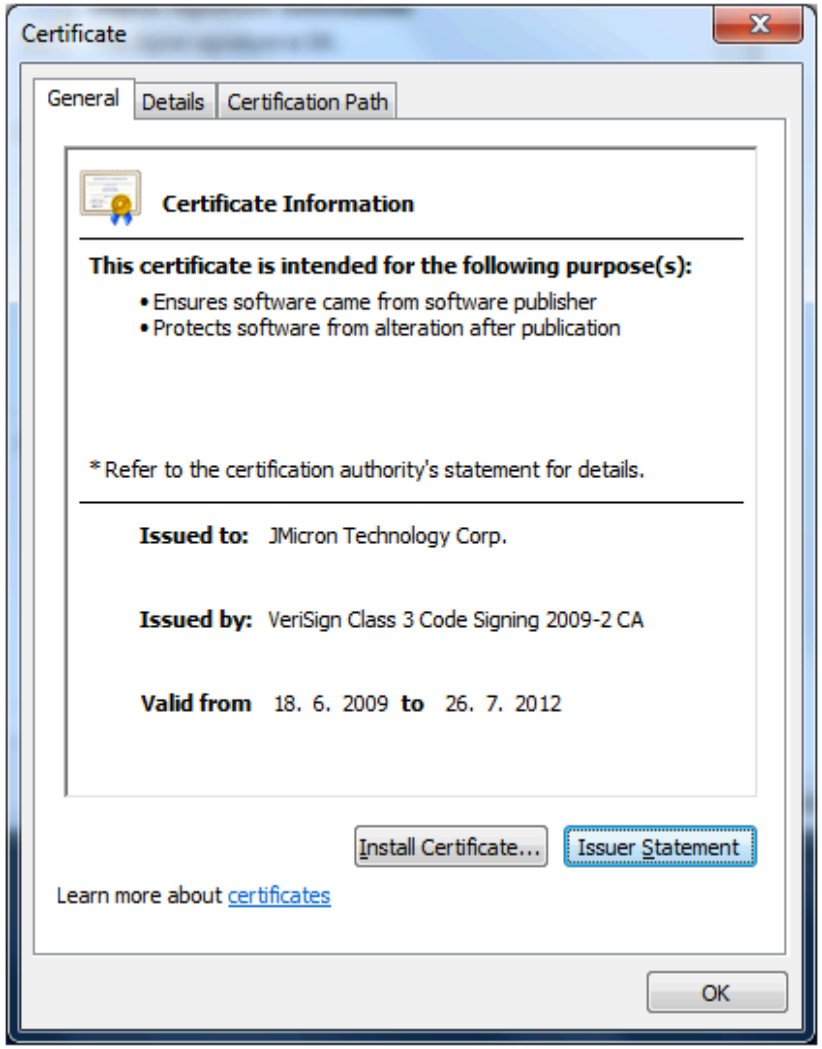
RED TIGER SECURITY

Stuxnet Dissected

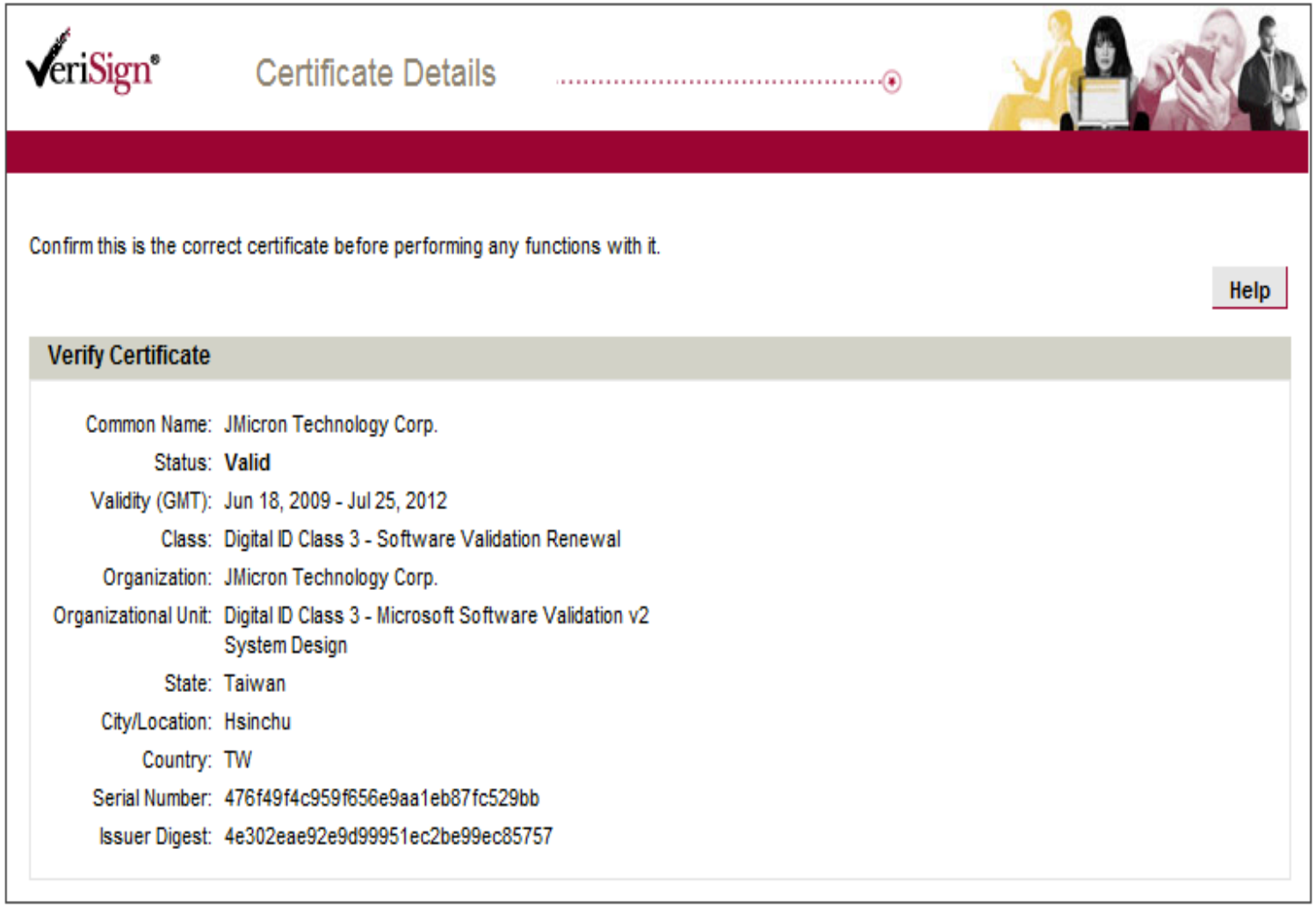
- STUXNET
  - Took advantage of Jmicron / Realtek private keys to hack drivers that were signed by these companies
  - Legitimate signatures
  - Leveraged 4 Windows 0day vulnerabilities
  - Flexible to spread and infect over USB or over connected networks
  - Targeted specific Siemens applications, DLLs, and PLC code

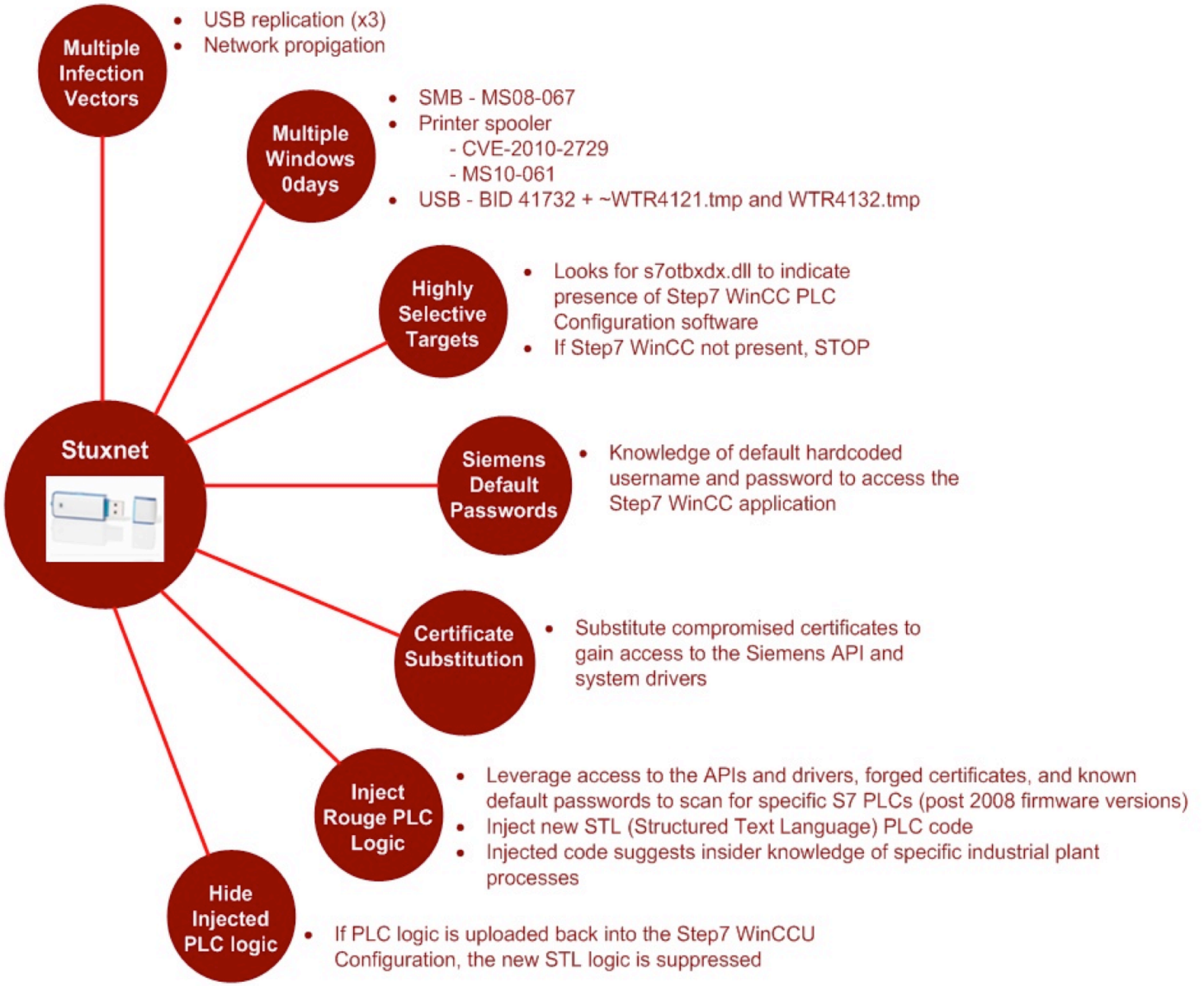
Valid Certificates ?!?!





Certificates – Con't




Multiple Infection Vectors
USB replication (x3)
Network propigation
Multiple Windows 0days
SMB - MS08-067
Printer spooler
- CVE-2010-2729
- MS10-061
USB - BID 41732 + ~WTR4121.tmp and WTR4132.tmp
Highly Selective Targets
Looks for s7otbxdx.dll to indicate presence of Step7 WinCC PLC Configuration software
If Step7 WinCC not present, STOP
Stuxnet
Siemens Default Passwords
Knowledge of default hardcoded username and password to access the Step7 WinCC application
Certificate Substitution
Substitute compromised certificates to gain access to the Siemens API and system drivers
Inject Rouge PLC Logic
Leverage access to the APIs and drivers, forged certificates, and known default passwords to scan for specific S7 PLCs (post 2008 firmware versions)
Inject new STL (Structured Text Language) PLC code
Injected code suggests insider knowledge of specific industrial plant processes
Hide Injected PLC logic
If PLC logic is uploaded back into the Step7 WinCCU Configuration, the new STL logic is suppressed

The Horizon

- Mutating Bots / Command & Control
  - Quiet installation
  - Obfuscated Exfiltration (HTTP, DNS, Masked)
- Directed Social Engineering
  - Staggered Attack
  - Combined with other styles
  - Building relationships over time
- Leverage of Social Networks (SOCNET)
  - Facebook is not your friend
  - Twitter or Linkedin aren't too fond of you either…

How to Extract Meaningful Cyber Incident data from SCADA Components? (30 min)

New SCADA Attacks - APT, Night Dragon, and Stuxnet – everybody is kung fu fighting ☺

System Logs

- Discuss event notification and log aggregation techniques for SCADA Systems that can greatly aide in system troubleshooting and incident response
- Many devices create logs and alerts, so this session will cover this in three categories:
  1. Network devices
  2. Computing devices
  3. SCADA devices
- Incident Response is also covered after the Event and alert monitoring technology is discussed

Types of Devices That Create Logs

- Security Event Monitoring – what systems create logs/events?
  - Network devices
    - Switches
    - Routers
    - Firewalls
    - IDS/IPS devices
  - Computing devices
    - Data Historians
    - SCADA Operator consoles
    - SCADA Master Servers
    - SCADA Protocol Servers (OPC)
  - SCADA field devices
    - Telemetry equipment (radios, satellite, and telephony devices)
    - PLCs, RTUs, and other embedded devices
- Alert Management – Incident Response
- Breakout Discussion Session

Network devices - SNMP

- Fortunately, most Switches, Routers, Firewalls, and IDS/IPS devices all support SNMP and Syslog with fairly standardized output formats
- An SNMP-managed network consists of three key components:
  - Managed device = Slave device
  - Agent = software which runs on Slave device
  - Network management system (NMS) = software which runs on Master
- A managed device is a network component that has a SNMP interface that allows unidirectional (read-only) or bidirectional access to security, health, or performance information.
- An agent is a network-management software module that resides on a managed device. An agent has local knowledge of management information and translates that information to or from an SNMP specific form.
- A network management system (NMS) executes applications that monitor and control managed devices. Network Management Systems provide the bulk of the processing and memory resources required for network management. One or more NMS consoles may exist on any managed network.
- SNMP NMS consoles can convert SNMP trap data to Syslog format and forward to a Syslog server

Network devices - Syslog

- Syslog is a client/server protocol that transmits a text message with a maximum size of 1024 bytes to the syslog receiver. The receiver is commonly called syslogd, syslog daemon or Syslog server. Syslog messages may be sent using either User Datagram Protocol (UDP) or the Transmission Control Protocol (TCP).
- Syslog data is typically sent in cleartext, but an SSL wrapper can be used to provide for a layer of encryption through SSL/TLS.
- Syslog typically uses the port number 514.
- Syslog is typically used for computer system management and security auditing.
- Syslog is supported by a wide variety of devices and receivers across multiple platforms. Because of this, Syslog can be used to integrate log data from many different types of systems into a central repository.
- With the capability to convert SNMP-to-Syslog, and the ability to take OPC data and convert it to Syslog, the final repository of all event and performance data for Ethernet networks should be a Syslog server.

Computing devices

- Data Historians, SCADA Operator consoles, SCADA Master Servers, and SCADA Protocol Servers (OPC) operate on known standard operating systems that are either based on Windows or *NIX variants.
- SNMP and syslog agents are readily available for all modern versions of Windows, Unix, and Linux.
- These OS Agents support syslog and SNMP with fairly standardized output formats

SCADA and Embedded devices

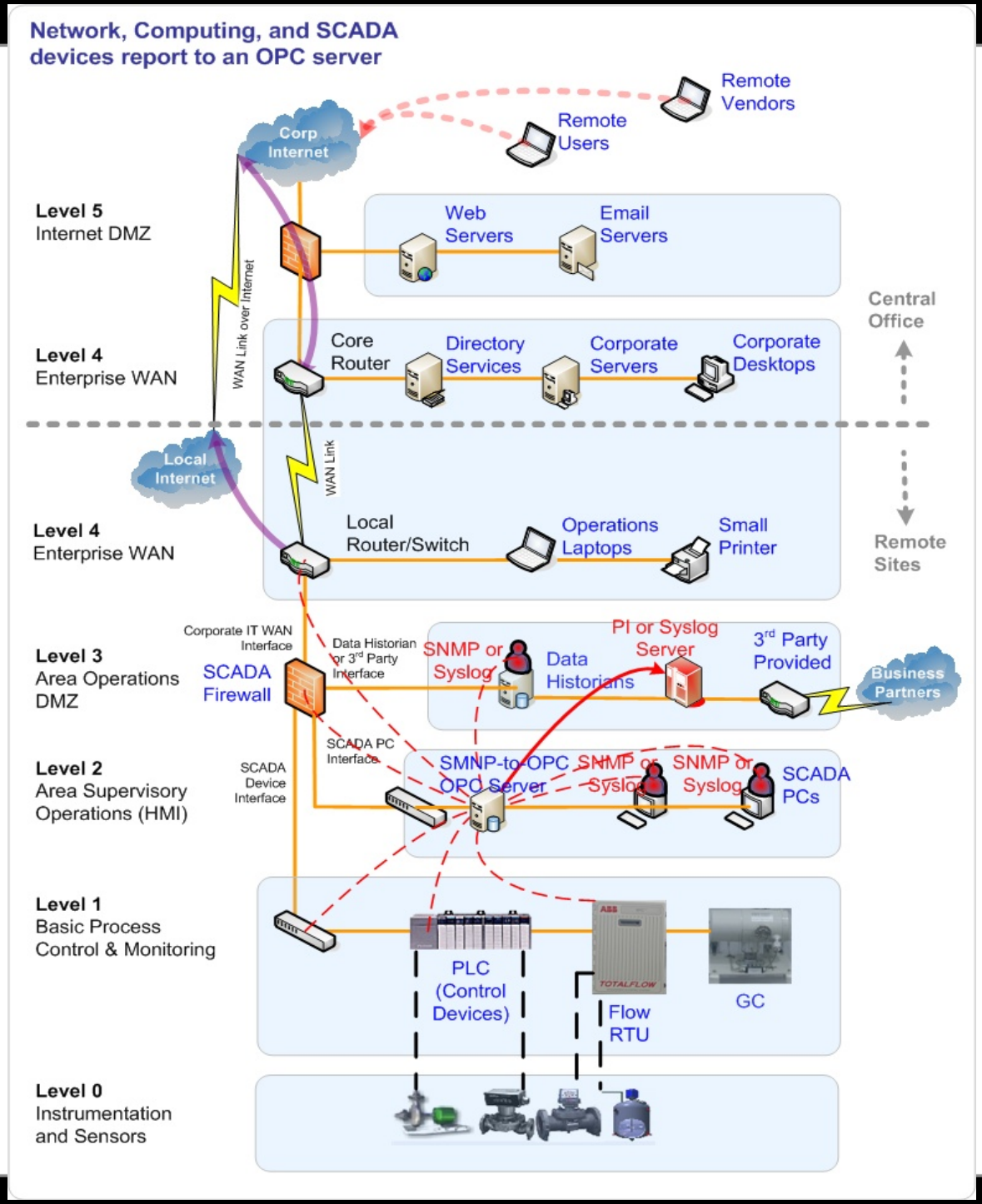
- Telemetry equipment (radios, satellite, and telephony devices)
  - Ethernet
    - Radios and telemetry devices that have Ethernet TCP/IP interfaces typically support SNMP, but may or may not support Syslog.
  - Serial
    - Legacy telemetry devices that only have serial interfaces do not support either SNMP or Syslog. Their status and performance can only be monitored by the vendor-specific software that ships with the hardware
- PLCs, RTUs, and other embedded devices
  - Ethernet
    - PLC and RTU devices that have Ethernet TCP/IP interfaces typically support SNMP, but may or may not support Syslog.
  - Serial
    - Legacy telemetry devices that only have serial interfaces do not support either SNMP or Syslog. Their status and performance can only be monitored by the SCADA protocol drivers. Some have specific internal registers for monitoring the status of the devices.

RED TIGER SECURITY

SNMP-to-OPC drivers from Kepware and Matrikon offer an interesting way to bring in security and performance events into the SCADA system.

The SNMP alerts can be logged and trending right along with other SCADA data.

Logged data can be forwarded onto the data historian or a Syslog server.

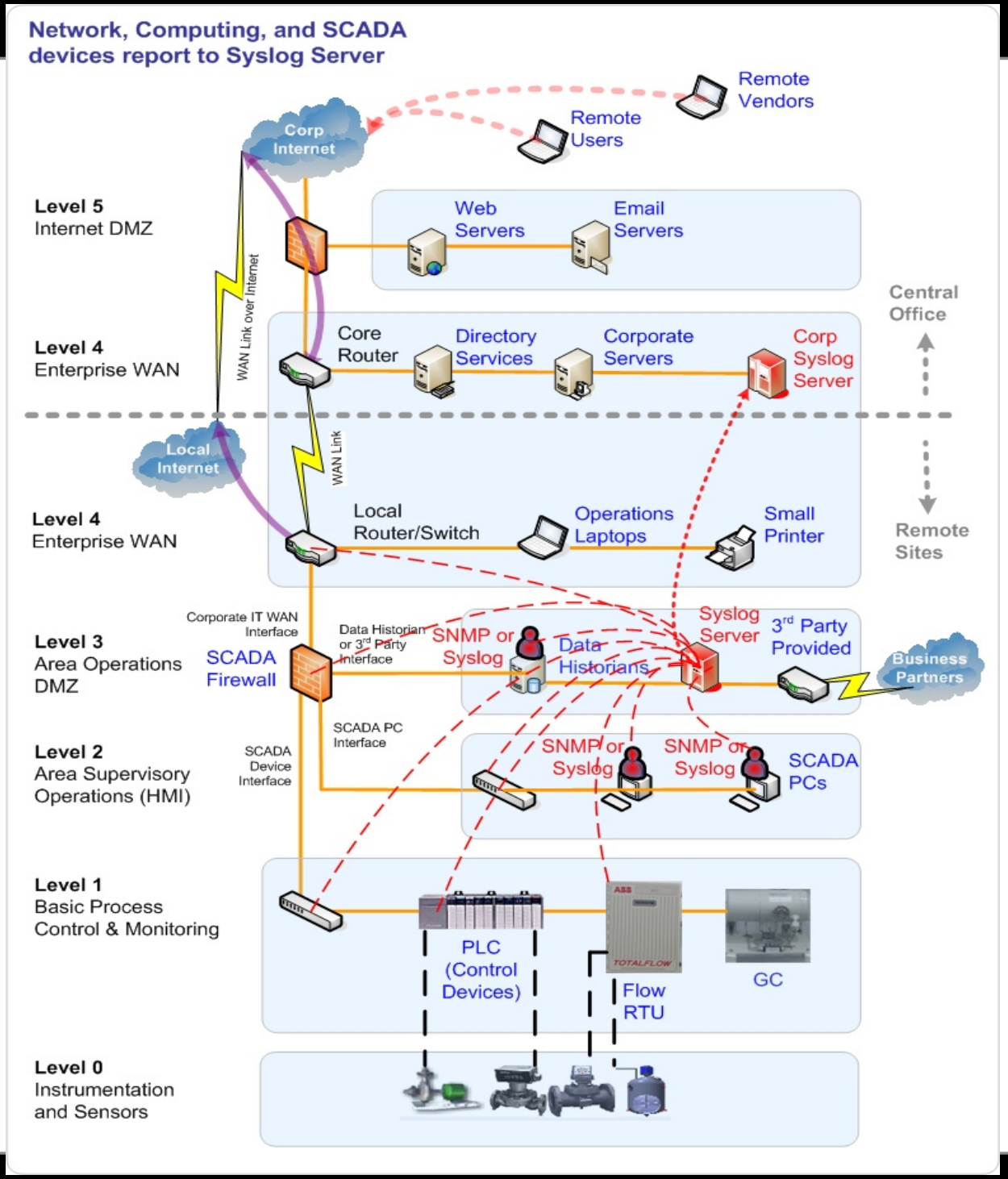


RED TIGER SECURITY

If a majority of the network, computer, and SCADA devices support Syslog, then you can also deploy a very inexpensive Syslog server.

Even the “free” Syslog servers provide useful filtering, alert management, and reporting options.

Logging system alerts and routinely reviewing the logs are requirements for NERC CIP and CFATS compliance.



Intrusion Detection, End Point Security, and Security Event Management Systems for SCADA Systems (30 min)

Centralizing all log, IDS, and alert notifications

RED TIGER SECURITY

2-sides to Security/Performance – Prevention and Detection

- **Prevention** > Firewalls and IPS systems are like locks - they are devices that actively "LOCK" out unauthorized attempts.
  - Like Locking Doors on Your Car
  - In most cases, just **locking the doors** will create enough hassles to deter most people from even attempting to break in.
- **Detection** > IDS and Monitoring Systems are like Alarm Systems
  - Monitors the health and performance of the network, host systems, and even applications and devices, and send out alerts when anything is abnormal.
  - Provides notification if someone or something get through the defense
  - Allows historical trending of system performance and security
  - Having banners on all digital access that indicate that any unauthorized access will be prosecuted, and IDS systems in place let cyber criminals know that you mean business.

RED TIGER SECURITY

IPS

- Intrusion Prevention System (IPS) is a session based appliance that complements a firewall by performing deep packet inspection of the payload or content of the data communications going through a known firewall port
- IPS systems are typically signature-based, but some are becoming intelligent enough to start to learn what is abnormal traffic
- Actively BLOCKS traffic it thinks is not healthy for the inside of the network by dropping packets
- Typically best to deploy at the perimeter of the network

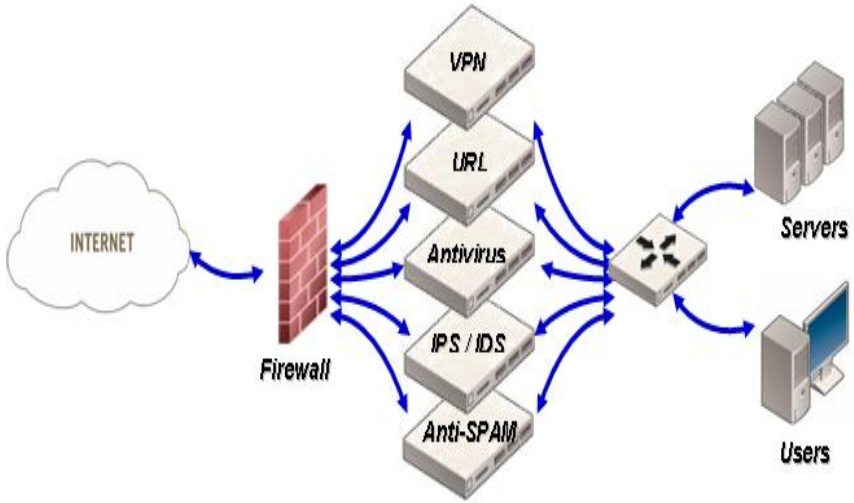
RED TIGER SECURITY

Network-based AV

- Network-based AV works similar to AV installed on a laptop, desktop, or server, EXCEPT, it scans all network traffic before the traffic even touches the host systems
- Several vendors sell Network appliances with AV on-the-wire, and malicious viruses, worms, or known malware will be effectively dropped at the network border before the traffic is even seen by any servers on the inside
- Signatures are often updated automatically as a service from the vendors for a monthly fee, and most updates occur within 3 hours of a new signature release
- Can be used to complement firewalls, IPS Systems, and Host AV to prevent malware before it even gets to the internal network
- Must be placed in-line so that all communications goes through it or a pair of devices in high-availability mode.

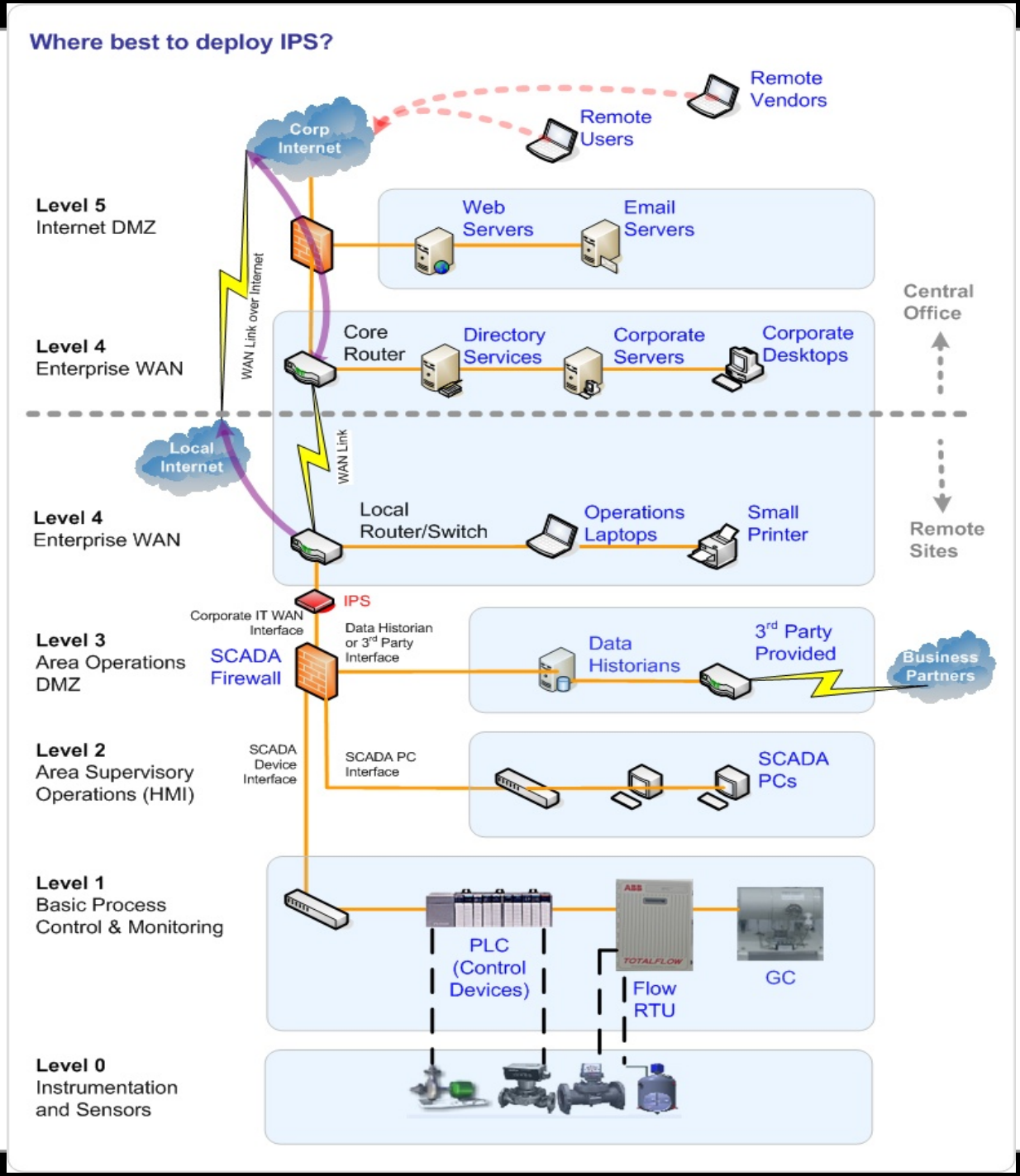
UTM – Unified Threat Management

- Basically leverages firewall, VPN, web proxy, AV, IPS/IDS, and anti-spam all within one appliance
- Supports plug-and-play with other traditional firewalls
- Typically has high-availability mode to support multiple devices on the same choke point, and have one system back up the main system



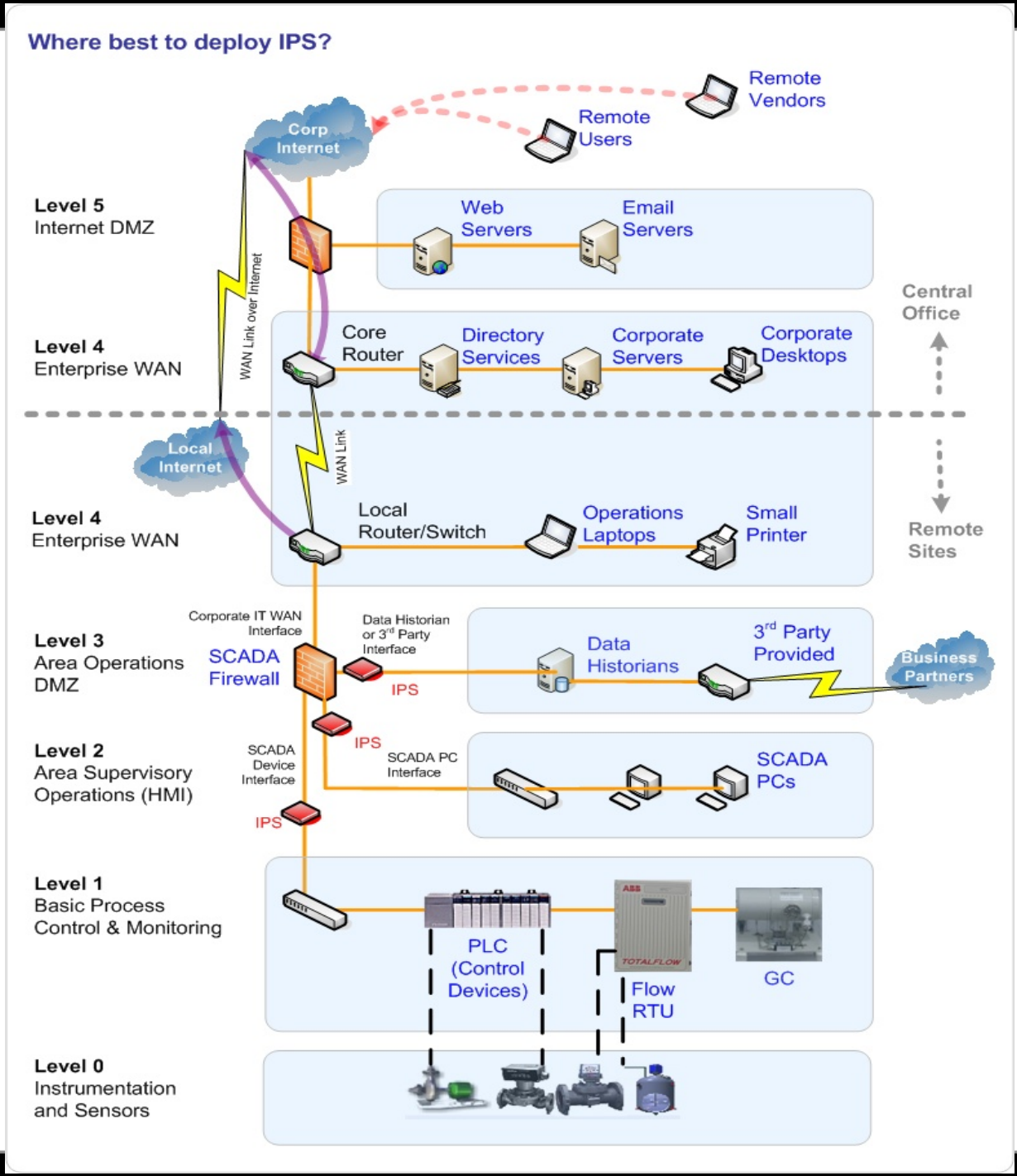
RED TIGER SECURITY

The ideal location for SCADA IPS is upstream of the SCADA firewall. The IPS sensor will filter out known malicious traffic before it hits the SCADA firewall.



RED TIGER SECURITY

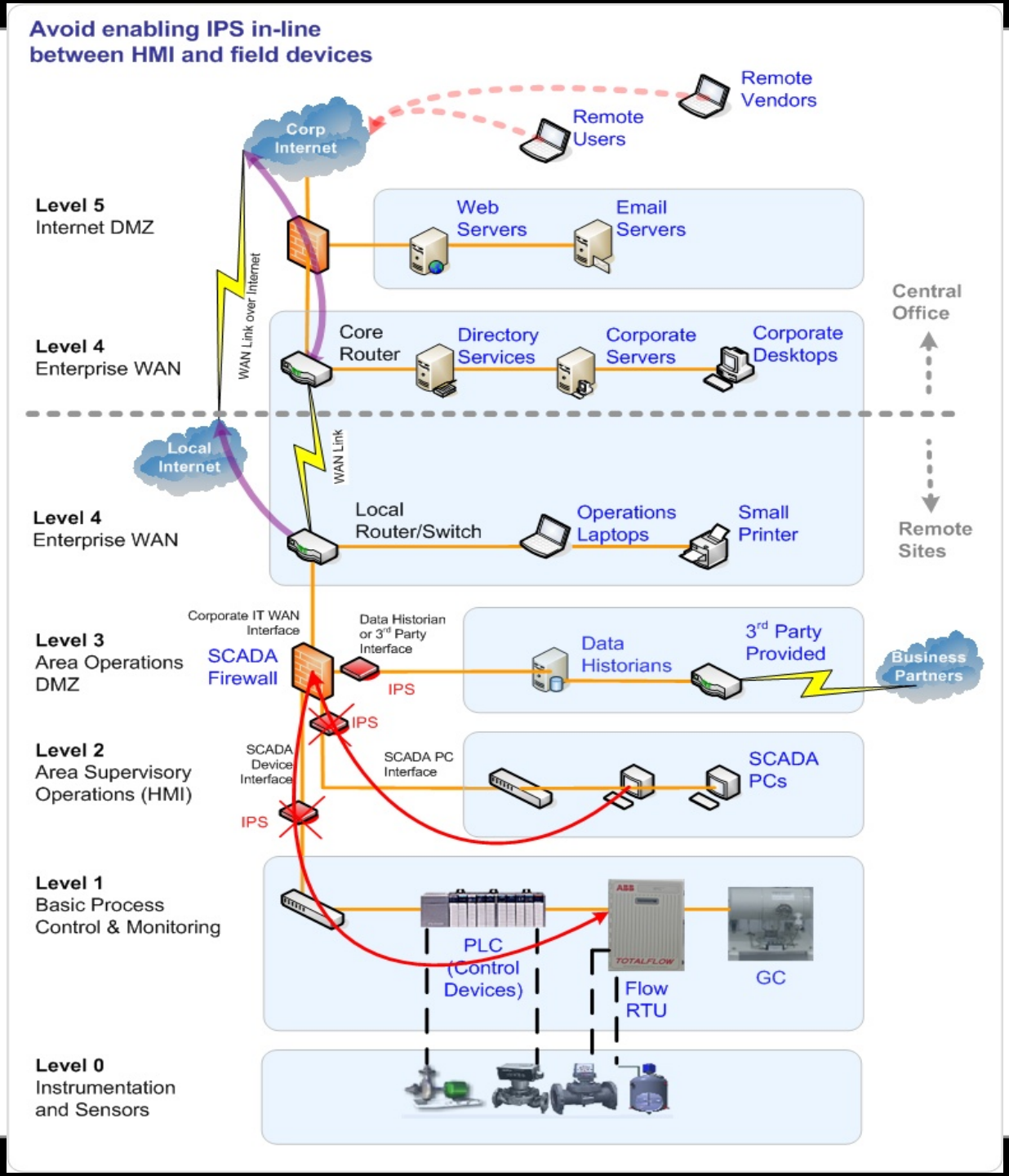
What is wrong with placing the IPS function downstream of the SCADA firewall?



RED TIGER SECURITY

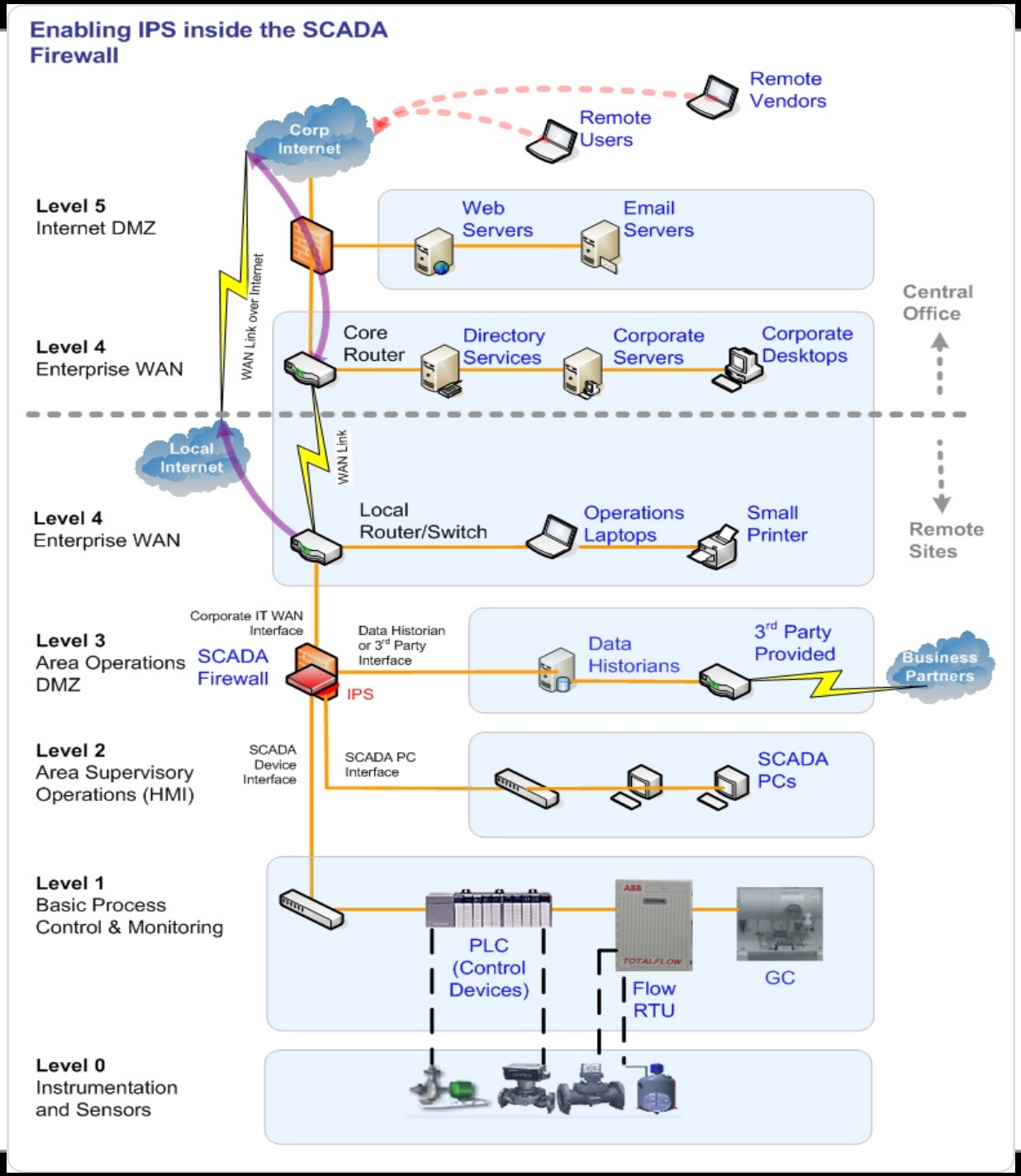
We want to avoid applying “prevention” or packet filtering technologies in-line between the SCADA HMI servers and the field controllers.

Some IPS appliances have been known to actively block certain SCADA protocols and commands thinking they were malicious packets.



RED TIGER SECURITY

What if we are using a UTM appliance that allows IPS to be enabled inside the SCADA firewall?

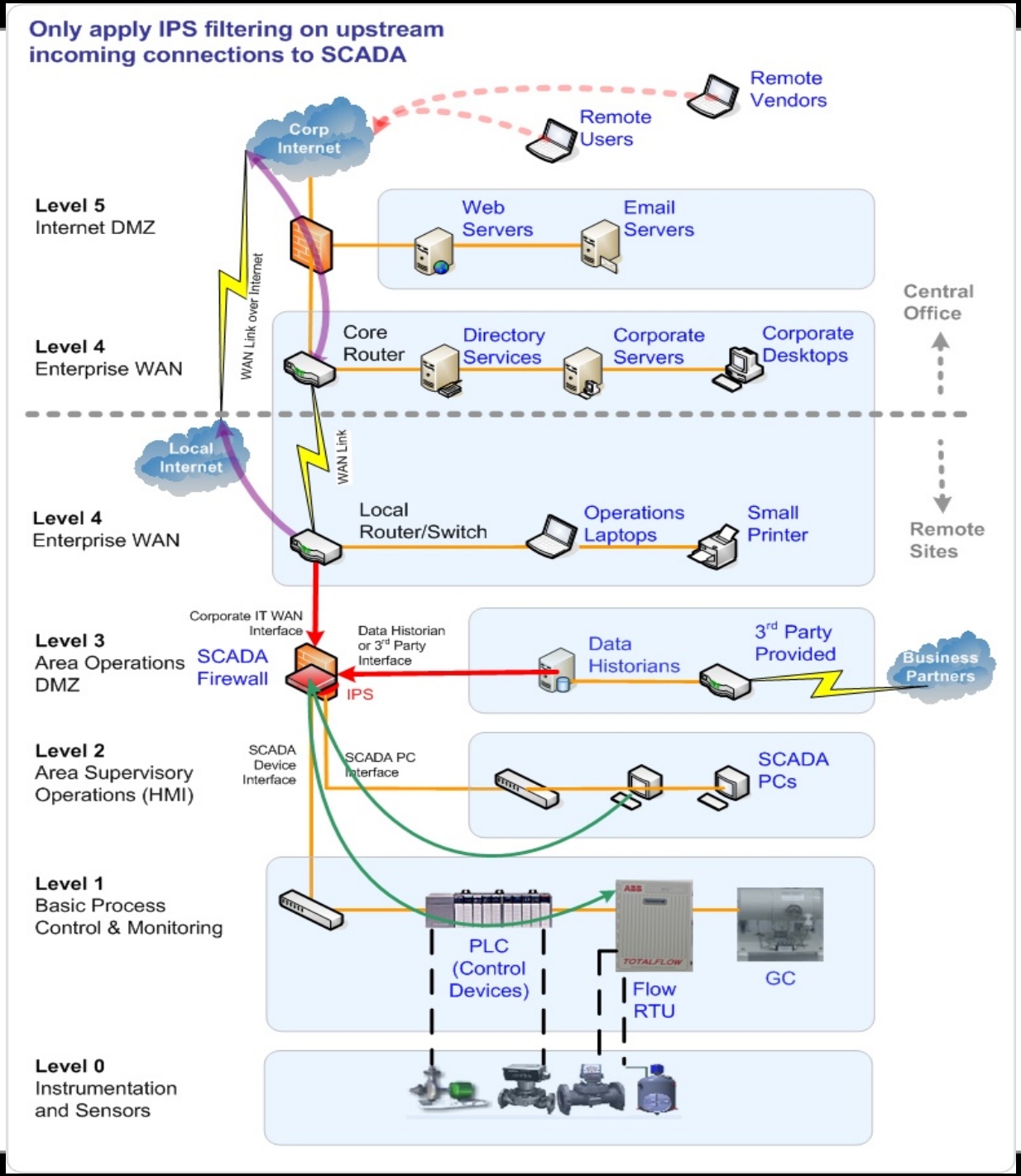


RED TIGER SECURITY

Only enable IPS filtering on the upstream links coming into the SCADA firewall from external connections like the Corporate IT WAN and 3rd Party networks.

Allow the path from the SCADA HMI to the field controllers to not have IPS enabled.

Or if you want to try it, test the IPS in a "report-only" mode and not enable active blocking.



IDS

- An **Intrusion Detection System** (**IDS**) detects the unwanted manipulations of computer systems, mainly through network packet inspection and host monitoring
- Possible attack vectors are:
  - vulnerable services,
  - data driven attacks on applications,
  - host based attacks such as privilege escalation,
  - unauthorized logins and access to sensitive files,
  - and Malware (viruses, Trojan horses, and worms).
- Multiple components:
  - **Sensors** which generate security events,
  - **Console** to monitor events and alerts and control the sensors,
  - **Central Engine** that records events logged by the sensors in a database and uses a system of rules to generate alerts from security events received.
- There are multiple categories of IDS depending on the type and location of the sensors and the methodology used by the engine.

IDS

- Intrusion Detection System (IDS)
  - Technology that detects and reports on attacks
    - NIDS (Network Intrusion Detection Sensor)
      - Dedicated network appliance
    - Host Intrusion Detection Sensor
      - Software runs on the host
  - Components
    - Network Sensor (NIDS)
    - Host Sensor (HIDS)
    - Analysis Engine

Network IDS (NIDS)

- A **Network Intrusion Detection System** (**NIDS**) detects malicious activity such as denial of service (DOS) attacks, port scans by the monitoring network traffic.
- HOW DOES IT WORK?:
  - NIDS reads packets at the Application layer
  - Looks for patterns : PROTOCOL, PORT
  - Looks for shell codes

  (Examines outbound activity as well)
- Integrated with firewalls, NIDS can be configured to update Blacklists and ACL's (access control lists) to block suspected IP addresses.

RED TIGER SECURITY

Host Based IDS (HIDS)

- **A HOST Intrusion Detection System** (**HIDS**) detects potentially malicious activity such as new processes or applications starting on the host computer
- HOW DOES IT WORK?:
  - HIDS agents typically watch a specific file folder for changes, hard disk space, available/committed memory, applications running (whitelist)
  - HIDS also checks for removable media insertion
  - Will usually report its alerts to the same central log console that the NIDS sensors are reporting to
- HIDS can help keep the users of SCADA systems honest by having an automated software tool that constantly watches the performance and security of the computer that it resides on.

RED TIGER SECURITY

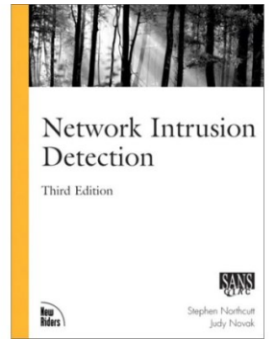
Analysis Engines (Heuristics)

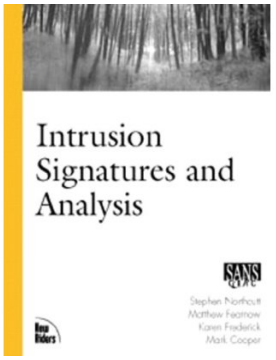
- Signature based
  - AKA Rule-, Knowledge-, Pattern-matching-based
- Patterns of known attacks
  - Installed in IDS, updated periodically
  - Match-response action
  - Vulnerable to new attacks
  - Low false positives
- Behavior based
  - AKA anomaly- or Statistical- or Heuristics-based)
  - “Learns” what is “normal”
  - Compares activity to reference model
  - Does not match-response action
  - Can detect new attacks
  - High false positives

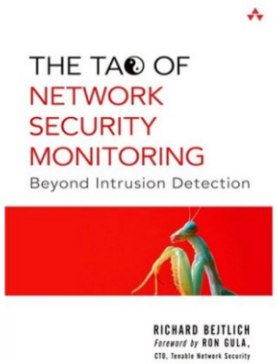
RED TIGER SECURITY

Signatures

- Signature Based
  - Limited to vendor updates unless you have specific skills to write custom signatures.
  - http://www.amazon.com/exec/obidos/tg/detail/-/073571265/ref=pd_sr_ec_ir_b/104-5466513-1143959?v=glance&s=books&st=*
  - http://www.amazon.com/exec/obidos/tg/detail/-0735710635ref=pd_bxgy_img_2/104-5466513-1143959?v=glance&s=books
  - http://www.amazon.com/exec/obidos/ASIN/0321246772/qid=1114003856sr=2-6ref=pd_bbs_b_2_6/104-5466513-1143959





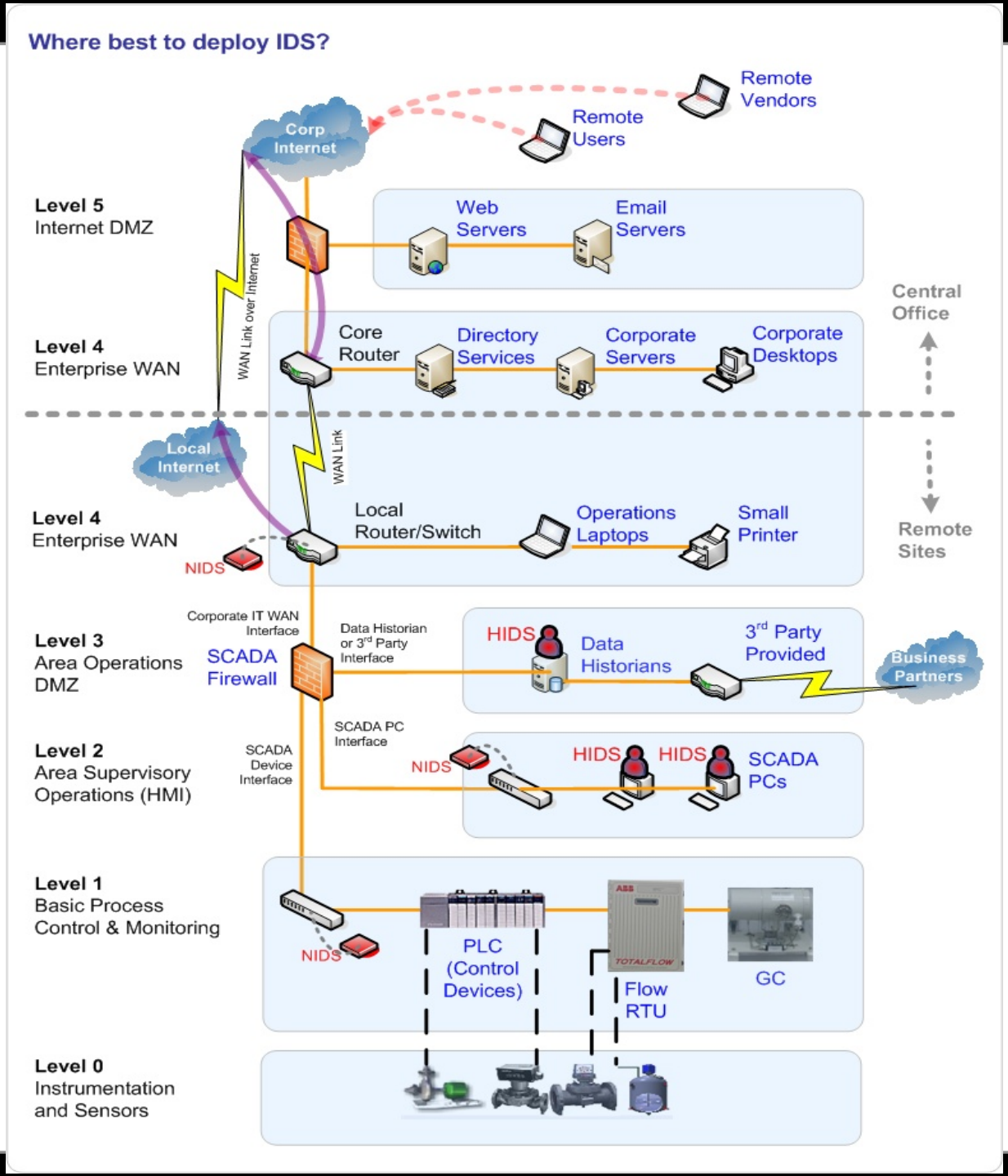


RED TIGER SECURITY

IDS systems use both NIDS and HIDS to detect malicious or non-standard behavior at the network and host level.

NIDS sensors passively take a copy of the network traffic (usually on a spanning port of a switch), analyzes the traffic, and only sends an alert to the SEM if any packets are a match to known signatures.

HIDS sensors are installed on SCADA servers and workstations, but must be tuned to the normal use of the computer to avoid a flood of alerts.

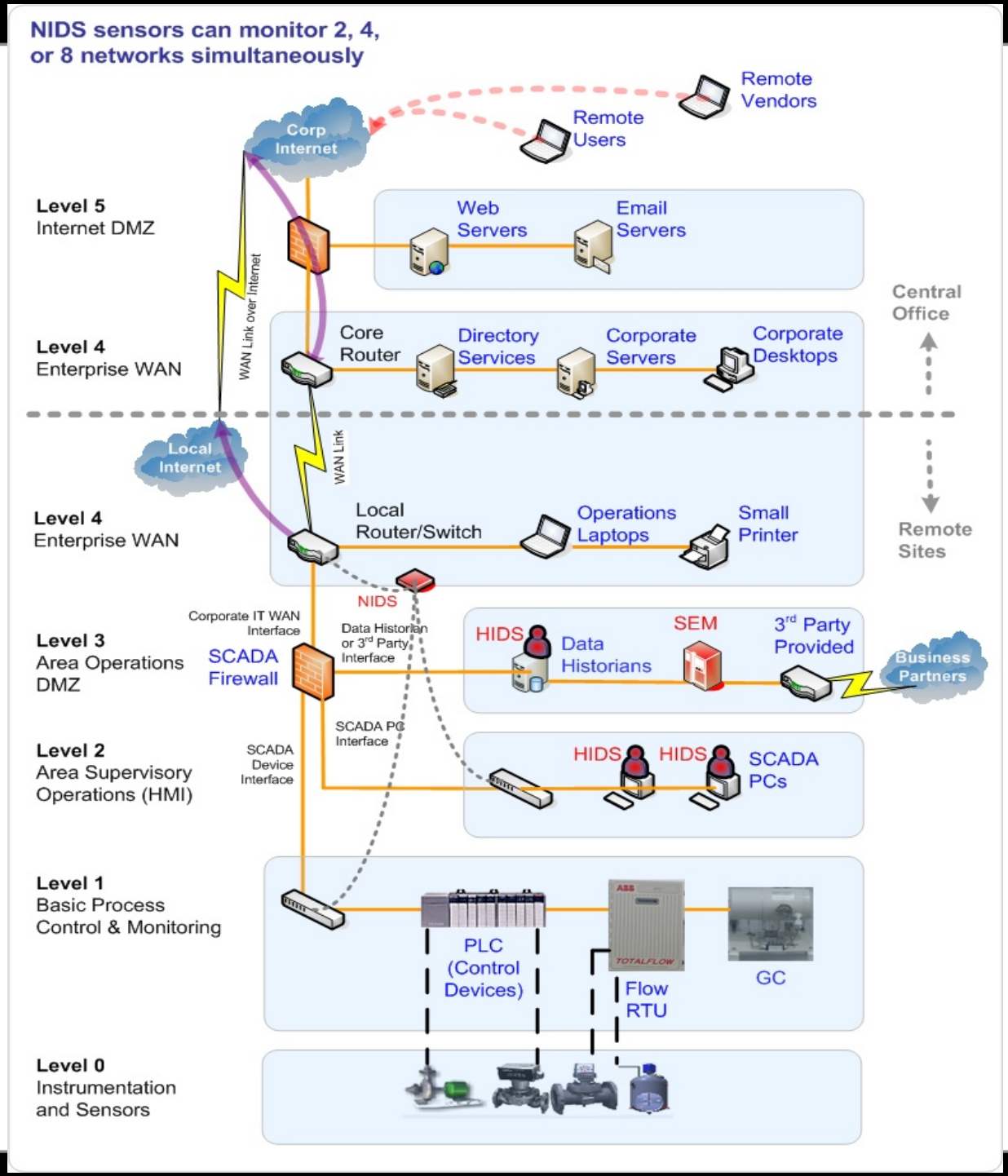


RED TIGER SECURITY

NIDS sensors can monitor 2, 4, or 8 networks simultaneously. If the monitoring ports on all of the switches or VLANs can be routed back to one location, then only one NIDS is required.

The SEM (Security Event Monitoring) console is typically installed within the SCADA DMZ, which is not in the SCADA LAN or in the Corporate IT LAN.

The SEM should also be able to get to outside networks for sending out alerts or for being monitored by a 3rd party.

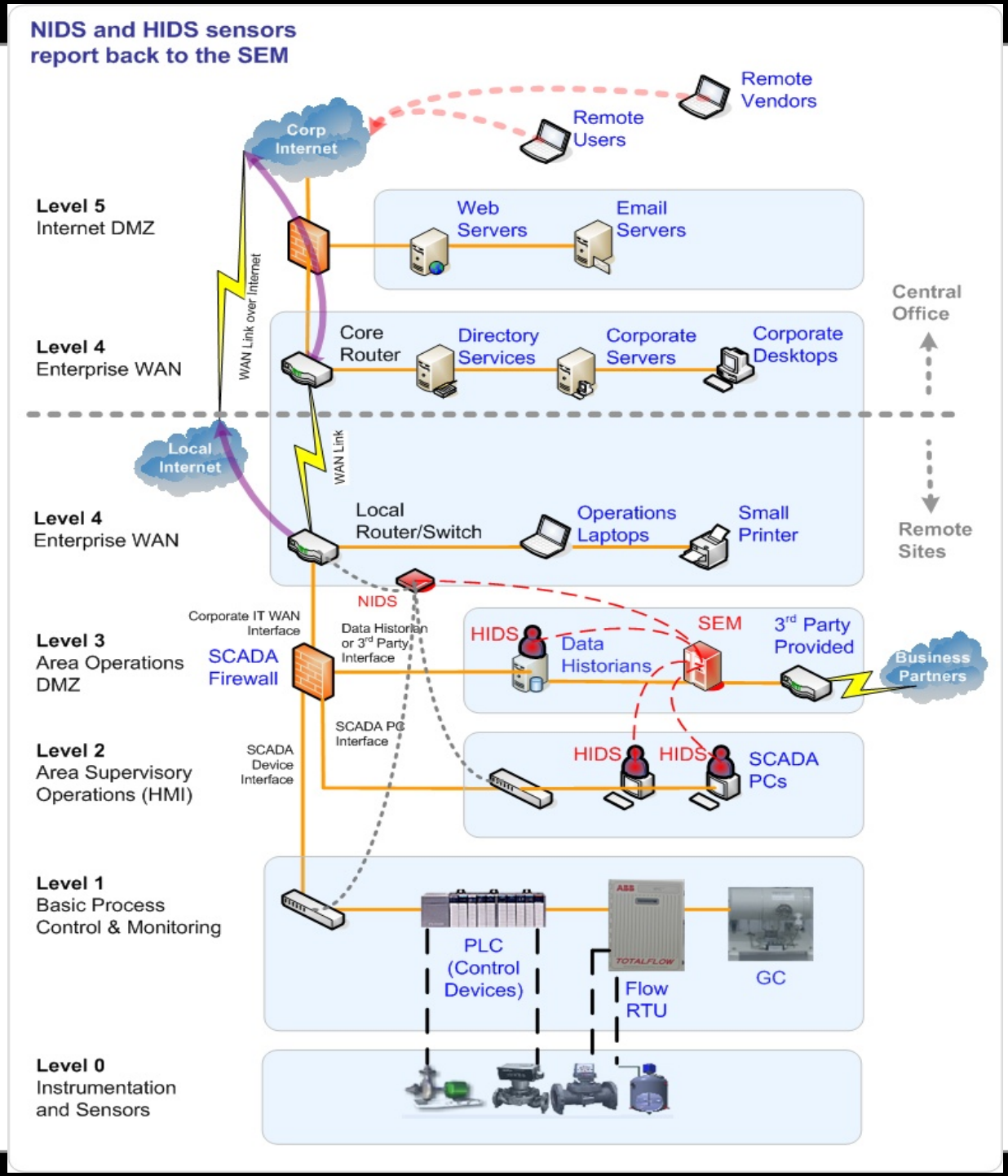


RED TIGER SECURITY

NIDS sensors can monitor 2, 4, or 8 networks simultaneously. If the monitoring ports on all of the switches or VLANs can be routed back to one location, then only one NIDS is required.

The SEM (Security Event Monitoring) console is typically installed within the SCADA DMZ, which is not in the SCADA LAN or in the Corporate IT LAN.

The SEM should also be able to get to outside networks for sending out alerts or for being monitored by a 3rd party.



HIDS vs. Application Whitelisting

- HIDS
  - Software agent that typically works by passively watching and reporting on the following OS and Application behaviors:
    - Use and access to Administrator accounts
    - Starting/stopping of services
    - Monitoring of the Event Log, Security Log, and Application Logs
    - File change watch on certain directories
  - Difficult to tune > can throw off a large amount of false positives
- Application Whitelisting
  - Software agent that typically works by actively monitoring a set list of approved application (PIDs), and restricting any application not on the “whitelist” from executing on the computer
  - Can be tedious to setup initially > some SCADA applications (like Wonderware) require over 1800 individual processes to be allowed to run

Building Blocks of an Incident Response Program (30 min)

Including tips for detecting when you have been infected..

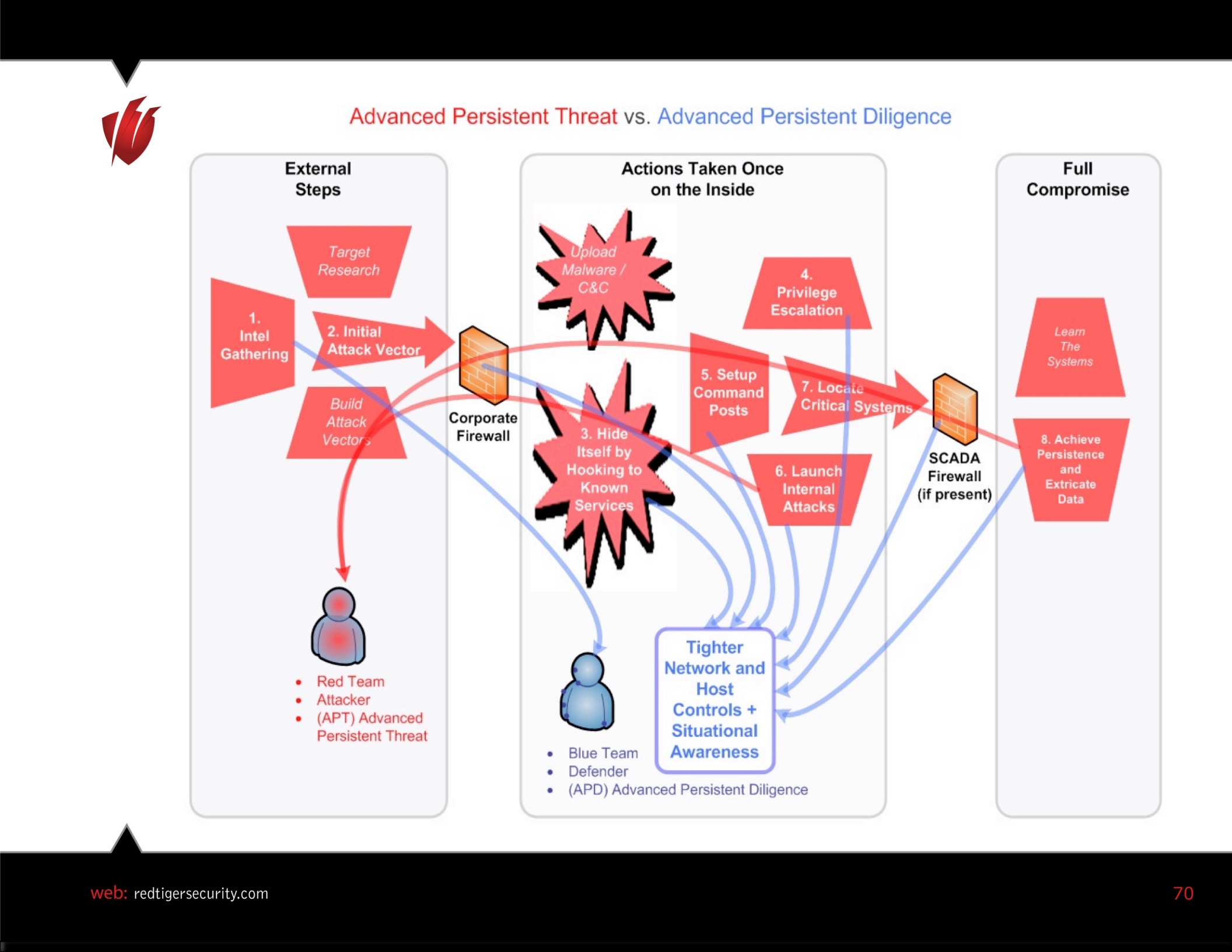
What to do about it

- Advanced Persistent Diligence
- Security Frameworks (NERC CIP, CFATS, ISA S99)
- How Recent Cyber Attacks Evade Security Controls
- Thoughts on setting up IR for SCADA

APT meet APD

Advanced Persistent Diligence

- Defense in Depth Approach is required
  - Active Network Defense systems such as firewalls, UTMs, and IPS are not enough, since APT threats can easily slide through these cyber defenses.
  - Having situational awareness of what is attempting to connect to the system, as well as what is going on within the system is the only way to start to regain control of the system.
- Testing patches before pushing
  - Development of a lab environment
  - Functional
  - Compressed version of ACTUAL devices and configuration
- Cyber Security Awareness
  - Employees are the best security barometer


Advanced Persistent Threat vs. Advanced Persistent Diligence
External Steps
Actions Taken Once on the Inside
Full Compromise
Target Research
1. Intel Gathering
2. Initial Attack Vector
Build Attack Vectors
Corporate Firewall
Upload Malware / C&C
3. Hide Itself by Hooking to Known Services
4. Privilege Escalation
5. Setup Command Posts
6. Launch Internal Attacks
7. Locate Critical Systems
SCADA Firewall (if present)
Learn The Systems
8. Achieve Persistence and Extricate Data
Tighter Network and Host Controls + Situational Awareness
Red Team
Attacker
(APT) Advanced Persistent Threat
Blue Team
Defender
(APD) Advanced Persistent Diligence

How to Detect if Your System is Infected

- **Watch for unauthorized changes being made to any system accounts**. If new domain controller accounts are added to the system, or if user accounts are randomly locked, then unlocked, or if the administrator account starts to be used when the administrators are clearly not on the network, then the APT attacker has already established a bi-directional link with the network.

- **Analyze the server(s) or workstation(s) involved**. Typically the logs will point out specific systems by IP address that are exporting data or used to escalate system privileges. Often, the malware and command and control (C&C) rootkits used by APT are not discovered by rootkit detectors because they hook into and hide behind known services. On Windows systems, analyze the following commonly-used services files for size (to see if they're too large) and number of instances (too many) on Windows systems:
  - **svchost.exe** (most common)
  - **iexplore.exe**
  - **iprinp.dll**
  - **winzf32.dll**

- I**nvestigate**. By using a combination of network and host investigative tools, determine how many instances of these files are running in memory, the size of those files, and what specific process identifiers (pids) are associated with them. Before shutting infected systems down, follow calls the malware is making to other computers, and to their command and control in order to determine scope of intrusion.

How Recent Cyber Attacks Evade Security Controls

- We understand that NERC CIP and most security standards require several physical and cyber controls that could prevent and detect APT attacks including tight access controls at the perimeter, logging and monitoring of all access points, malicious software detection at the host level, administrator account monitoring, and change controls.
- However, these controls are often not enough to thwart a motivated attacker, since they are gambling on some of the following assumptions about typical cyber defenses…

Typical Weak Links in the Chain

1. Most corporations are not aware about what information can be found about them in public available open source channels

2. Even though end uses are provided security awareness training, a large majority of internal users will click on attachments and links that they should not trust

3. Typical local host defenses such as Antivirus do not detect modifications to known good windows services and most APT attacks can avoid detection by AV

4. Most system administrators do not pay close attention to misuse of administrator accounts, so privilege escalation attempts are also often not detected

Typical Weak Links in the Chain

5. Once on the inside, malware can move fairly freely to setup command posts, deploy drones, and begin looking for useful data since internal network traffic monitoring can not pick up slow attacks that can hide within the same corporate traffic patterns
6. Most firewalls are programmed focusing on blocking incoming traffic, but allow unfettered outbound communications. When configuring the communications to outbound C&C servers, attackers use ports commonly left open through firewalls like 53 (DNS), 80 (HTTP), and 443 (HTTPS).

   Command and Control communications tend to use benign communication channels such as Twitter. Attack commands just appear as legitimate traffic. Attackers also bet on the fact that in most cases outbound firewall traffic is not monitored, nor are any traps placed to alert on abnormally high amounts of traffic going to any one particular external source.

Typical Weak Links in the Chain

7. Lack of internal network monitoring and centralized logging allows the attacker to launch NMAP scans and other searches through firewalls to detect the presence of SCADA protocols, applications, and devices.

8. SCADA systems often lack appropriate end point security technology like UTM (Unified Threat Management) code, operating system level firewalls, HIDS (Host Intrusion Detection Sensors), HIPS (Host Intrusion Prevention Sensors), AV (Antivirus), and application whitelisting technology. Since security event logging is rarely enabled on SCADA servers and workstations, APT attacks can achieve persistence and extricate data off of the system without detection.

Alert Management – Incident Response

- Incident Response is a required component of all major Security Compliance Frameworks including NERC CIP, CFATS, ISO 270001, NIST 800-53, and others.
- Understanding the unique risk involved with SCADA and Control Systems throws a curve ball at the subject, and the CSIRT should have representation from both SCADA Operations as well as Corporate IT Security
- The first step in establishing an Incident Response system is installing the monitoring sensors/agents and centralized alert console
- The saying “You can’t control what you don’t measure” applies to control systems, but also applies to security solutions
- Before an Incident Response plan can be put into place, what events get treated as “Incidents” much be defined

3 levels of Security Events

- **Normal** - a normal event does not affect critical components or require change controls prior to the implementation of a resolution. Normal events do not require the participation of senior personnel or management notification of the event.

- **Escalation** – an escalated event affects critical production systems or requires that implementation of a resolution that must follow a change control process. Escalated events require the participation of senior personnel and stakeholder notification of the event.

- **Emergency** – an emergency is an event which may:
  - impact the health or safety of people
  - breach primary controls of critical systems
  - materially affect component performance or because of impact to component systems prevent activities which protect or may affect the health or safety of individuals
  - be deemed an emergency as a matter of policy or by declaration by the available incident coordinator

Incident Response Team

- Where should events report to? Help Desk? SCADA Operations Team? Or maybe some Unique Security Team function?
- Each company must decide how they want to handle security events and alerts that involve SCADA and control systems
- Several useful resources out on the web for creating and sustaining a Computer Security Incident Response Team:
  - http://www.cert.org/csirts/Creating-A-CSIRT.html
  - SANS – search on "Computer *Incident Response Team"*
- Some use internal resources, while others outsource the function to companies like CSIRT http://www.csirt.org/
- If your Incident Response Plan involves SCADA and Process Control systems, make sure the team (whether internal or external) understand the risks involved with handling critical infrastructure equipment.

contact info / q & a

Jonathan Pollet, CAP, CISSP, PCIP

Founder, Principal Consultant

Red Tiger Security, USA

office: +1.877.387.7733

mobile: +1.281.748.6401

fax: +1.800.864.6249

jpollet@redtigersecurity.com

www.redtigersecurity.com