Introduction

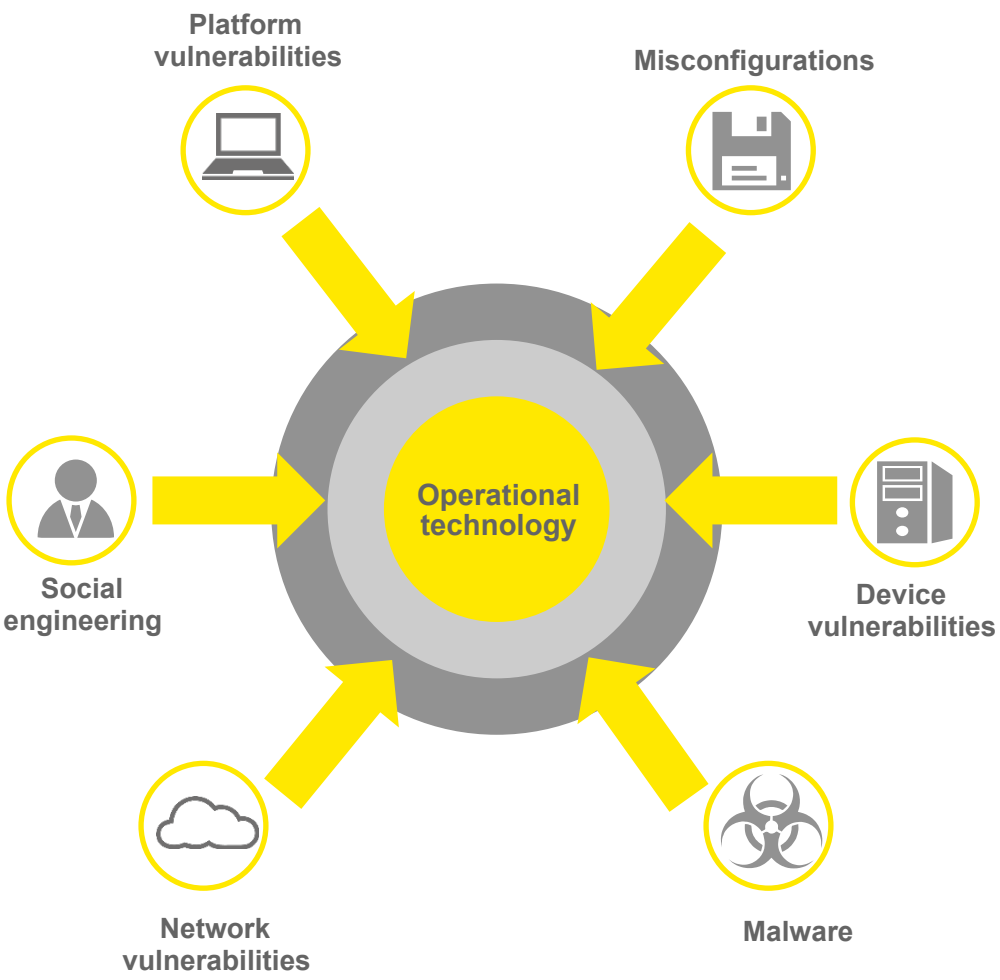
Jason Lawrence, MSISA, CISSP, CISA
Manager, EY Advanced Security Center
Atlanta, Georgia
jason.lawrence@ey.com
Twitter: @ethical_infosec

- More than 20 years of experience in cybersecurity specializing in cyber forensics, incident response and security monitoring
- Prior to EY, worked for Dell SecureWorks as a senior security analyst leading internal IR and forensics
- Led EY's internal Cyber Defense Response Center
- MS in Information Security and Assurance, Western Governors University
- BS in IT with an emphasis on information security, Western Governors University

Who are the attackers?

- **Nation states** – attacks against operational technology, especially in critical infrastructure, could be used in cyber warfare
- **Organized crime** – criminals target you for financial gain or competitive advantage
- **Hacktivists** – cyber activists may attack to disrupt operations as a form of political protest
- **Insider threat** – disgruntled employees or those able to be influenced by other threat actors can pose a significant risk due to the insider's knowledge of the environment and access
- **Script kiddies** – script kiddies running automated tools may attack without fully understanding the impact
- **Terrorist groups** – a potential target for terrorist groups looking to cause mass casualties

How do they accomplish their objectives?



Common attack vectors

Platform vulnerabilities

Critical software running on legacy or unsupported operating systems and platforms

Social engineering

Lack of security awareness and training for operational technology (OT) personnel

Network vulnerabilities

Insufficient network segregation between environments and unnecessary services exposed

Malware

Malware infections are common with some strains specifically designed to target OT

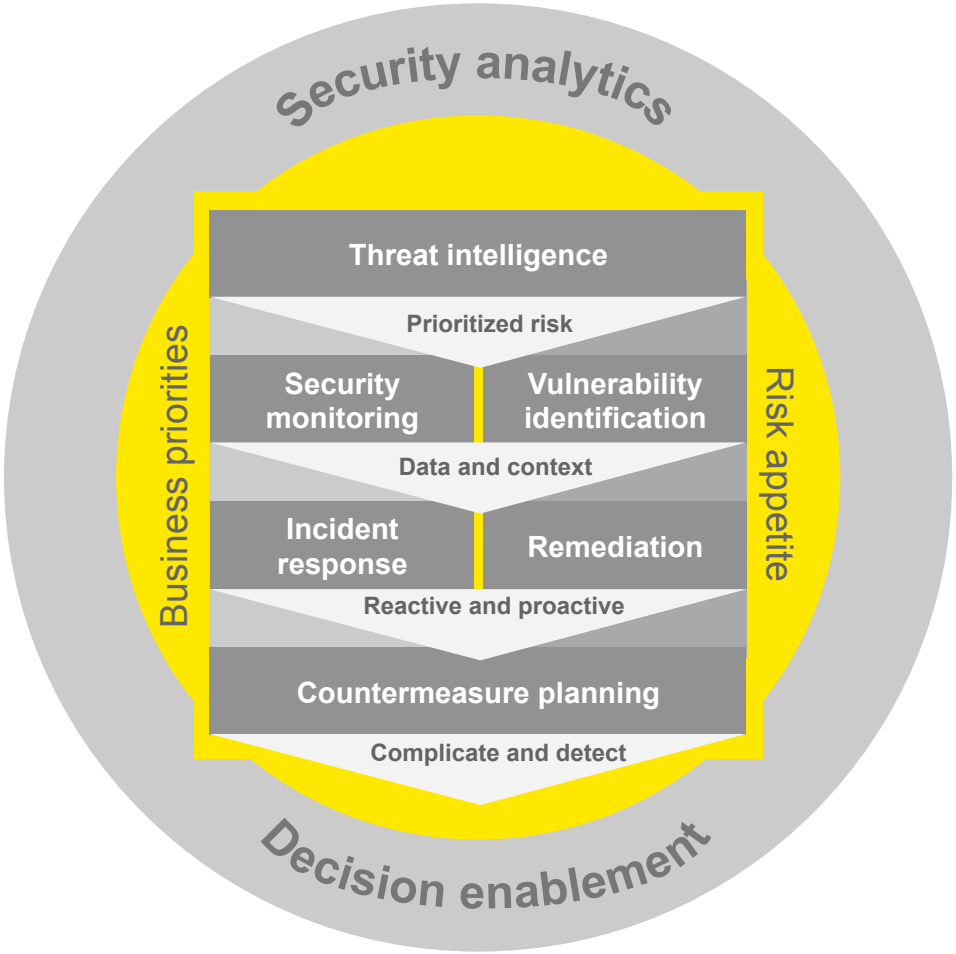
Device vulnerabilities

OT devices are typically low resources and not designed for security

Misconfigurations

Permissive access controls and default configurations can lead to unauthorized access

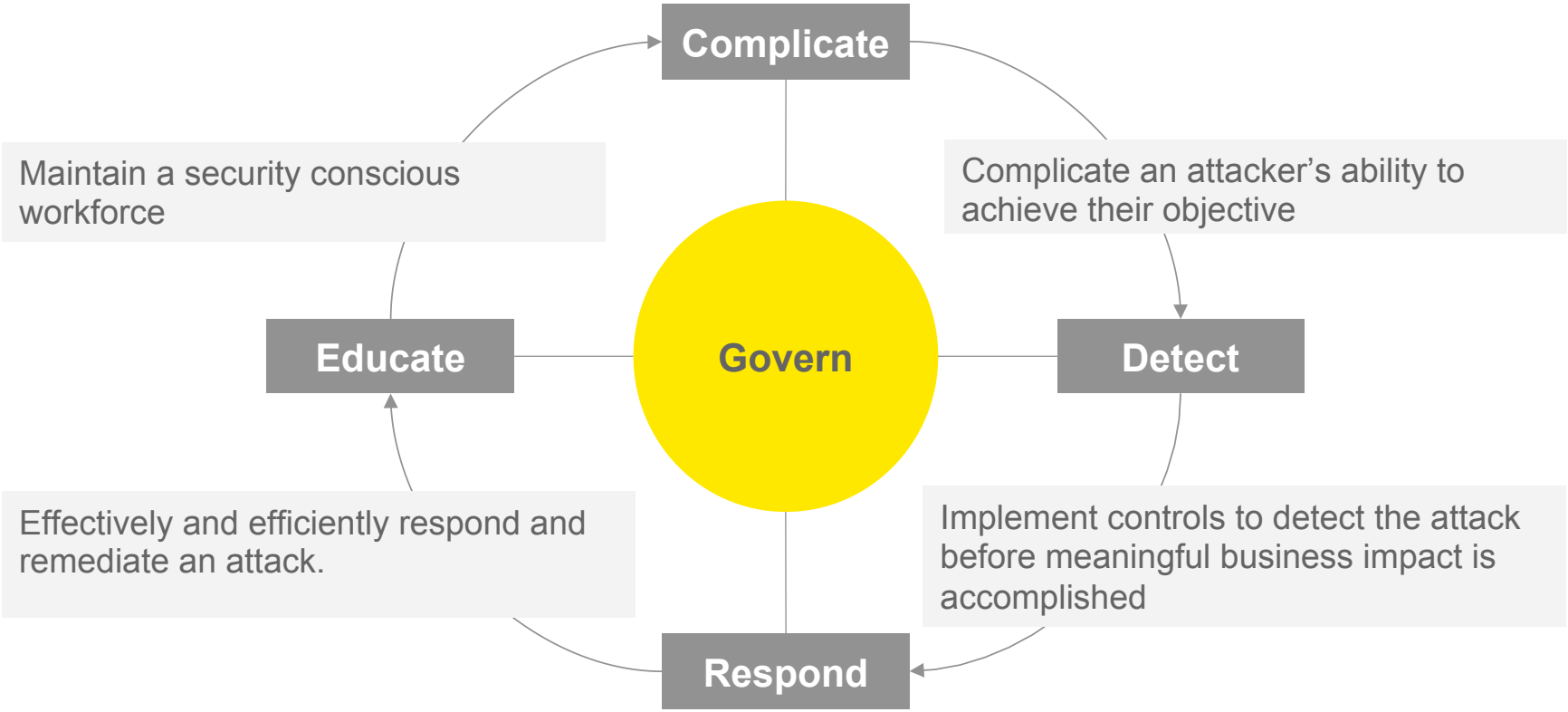
Cyber threat management
A system of integrated service capabilities



Capable security operations requires that key process areas are designed to enable and enhance each other to achieve improved decision enablement and a context rich cyber strategy.

- **EY Pedigree**: we are an embedded security organization with deep knowledge of security operations.
- **Framework**: our framework is designed to support the entire cybersecurity operational life cycle. Supporting and enhancing your investments in risk management and vulnerability management.

Countermeasure framework



Establish a strong governance program to continuously drive and sustain improvements

Critical security controls

The critical security controls for effective cyber defense

- Inventory of authorized and unauthorized devices
- Inventory of authorized and unauthorized software
- Secure configurations for hardware and software
- Continuous vulnerability assessment and remediation
- Malware defenses
- Application software security
- Wireless access control
- Data recovery capability
- Security skills assessment and appropriate training
- Secure configurations for network devices
- Limitation and control of network ports, protocol and services
- Controlled use of administrative privileges
- Boundary defense
- Maintenance, monitoring and analysis of audit logs
- Controlled access based on the need to know
- Account monitoring and control
- Data protection
- Incident response and management
- Secure network engineering
- Penetration tests and red team exercises

Control 1
Inventory of authorized and unauthorized devices

- **Actively manage (inventory, track and correct) all hardware devices on the network, so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access**
- **Configuration management database (CMDB) data**
- **Vulnerability scan results**
- **Active and continuous network discovery**

Control 2
Inventory of authorized and unauthorized software

- **Actively manage (inventory, track and correct) all software on the network, so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution**
- **Software license management**
- **CMDB**
- **Software restrictions**

Control 3

Secure configurations for hardware and software on laptops, workstations and servers

- **Establish, implement and actively manage (track, report on, correct) the security configuration of laptops, servers and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings**
- Create and maintain standard corporate images
- Configuration management databases
- Continuous vulnerability scanning

Control 4
Continuous vulnerability assessment and remediation

- **Continuously acquire, assess and take action on new information in order to identify vulnerabilities, remediate and minimize the window of opportunity for attackers**
- **Sample search for Qualys vulnerabilities on high value assets (HVAs)**
  - Index=main sourcetype=qualysguard qid NOT vuln_type=Info| lookup HVA nt_host AS netbios OUTPUT priority|search priority=*| lookup qualys_vuln QID AS qid OUTPUT SEVERITY_LEVEL AS severity VULN_TYPE as vuln_type CATEGORY as category TITLE as vuln_name|top 20 netbios|addcoltotals

Control 5
Malware defense

- **Control the installation, spread and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering and corrective action**
- **AV logs**
- **Endpoint protection**

Control 6
Application software security

- **Manage the security life cycle of all in--house developed and acquired software in order to prevent, detect and correct security weaknesses**
- **Application scanning results**
- Mostly a manual control

Control 7
Wireless device control

- **The processes and tools used to track, control, prevent and correct the security use of wireless local area networks (LANs), access points and wireless client systems**
- **Wireless IDS logs**
- **Access point logs**
- **Netflow data**

Control 8
Data recovery capability

- **The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it**
- **Mostly a manual process**
- **Test all backed-up data for recoverability**
- **Collect and monitor system logs from backup systems**

Control 9
Security skills assessment

- **For all functional roles in the organization (prioritizing those mission--critical to the business and its security), identify the specific knowledge, skills and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps and remediate through policy, organizational planning, training and awareness programs**
- **Assess awareness through the monitoring of web content**
- **Email gateway logs – detect phishing and correlate against proxy logs**

Control 10
Secure configurations for firewalls, routers and switches

- **Establish, implement and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings**
- **Network CMDB**
- **Continuous vulnerability scanning of network devices**

Control 11

Limitation and control of network ports, protocols and switches

- **Manage (track, control and correct) the ongoing operational use of ports, protocols and services on networked devices in order to minimize windows of vulnerability available to attackers**
- **Use a monitor ACLs on switches**
- **Monitor netflow events**
- **Logging on next-gen IDPS/Firewall for suspicious ports and protocols**

Control 12
Controlled use of admin privileges

- **The processes and tools used to track, control, prevent, and correct the use, assignment and configuration of administrative privileges on computers, networks and applications**
- **Monitor credential use through the lens of Windows or Linux event logs**
- **Account creation monitoring and alerting**
- **Domain controller login monitoring, for example:**
  - Index=DCLogs tag=authentication Logon_Type=2 OR Logon_Type=10|fillnull value="unknown" user, src, dest, dest_nt_domain, action, Logon_Type|top 20 user| sort -count

Control 13
Boundary defense

- **Detect, prevent and correct the flow of information transferring networks of different trust levels with a focus on security-damaging data**
- **Use IDS/IPS data to determine and detect activity**
- **For example to 20 IDPS events:**
  - | tstats `summariesonly` dc(IDS_Attacks.src) as src_count,dc(IDS_Attacks.dest) as dest_count,count from datamodel=Intrusion_Detection where * by IDS_Attacks.signature | drop_dm_object_name(IDS_Attacks)`|sort 20 – count|addcoltotals

Control 14
Maintenance, monitoring and analysis of audit logs

- **Collect, manage and analyze audit logs of events that could help detect, understand or recover from an attack**
- **Monitor log collection and report on any missing logs**
- **Generate reports and create dashboards for logging metrics**

Control 15
Controlled access based on the need to know

- **The processes and tools used to track, control, prevent and correct secure access to critical assets (e.g., information, resources and systems) according to the formal determination of which persons, computers and applications have a need and right to access these critical assets based on an approved classification**
- **Maintain a list of HVAs for both information and physical assets**
- **Use these lists as look-up tables in Splunk and monitor access**

Control 16
Account monitoring and control

- **Actively manage the life cycle of system and application accounts – their creation, use, dormancy and deletion in order to minimize opportunities for attackers to leverage them**
- **Monitor and alert on account creation, deletion and modification**
- **Use HR systems as a data point for employee status changes**
- **Monitor for any deviations from the norm in account naming conventions**

Control 17
Data loss prevention

- **The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and promote the privacy and integrity of sensitive information**
- **Send DLP alerts to Splunk**
- **Use as a data point for security operations**
- **For example, determine what violations are normal business by applying statistics and identifying the least frequency of occurrence**

Control 18
Incident response and management

- **Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications and management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.**
- **This control is only partially automated using the ES incident management dashboard.**

Control 19
Secure network engineering

- **Make security an inherent attribute of the enterprise by specifying, designing and building--in features that allow high confidence systems operations while denying or minimizing opportunities for attackers.**
- **This control is mostly a manual control.**
- **Verify that secure design is used as a guiding principal for any new technology project.**

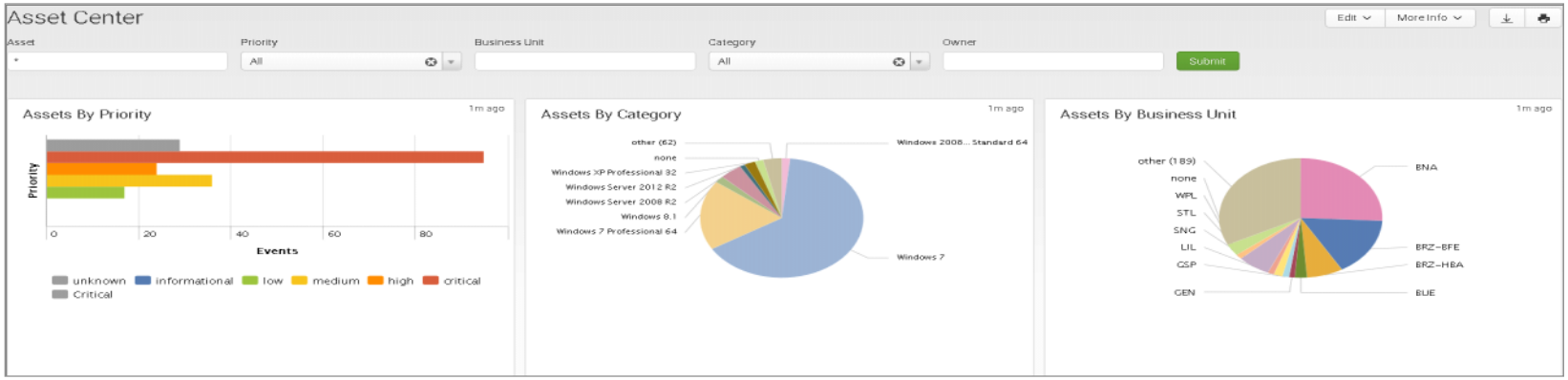
Control 20
Pen testing and red team exercises

- **Test the overall strength of an organization's defenses (the technology, the processes and the people) by simulating the objectives and actions of an attacker.**
- **This control is a litmus test for security operations.**
- **The previous controls should alert and/or block this control.**

Splunk reports and dashboards

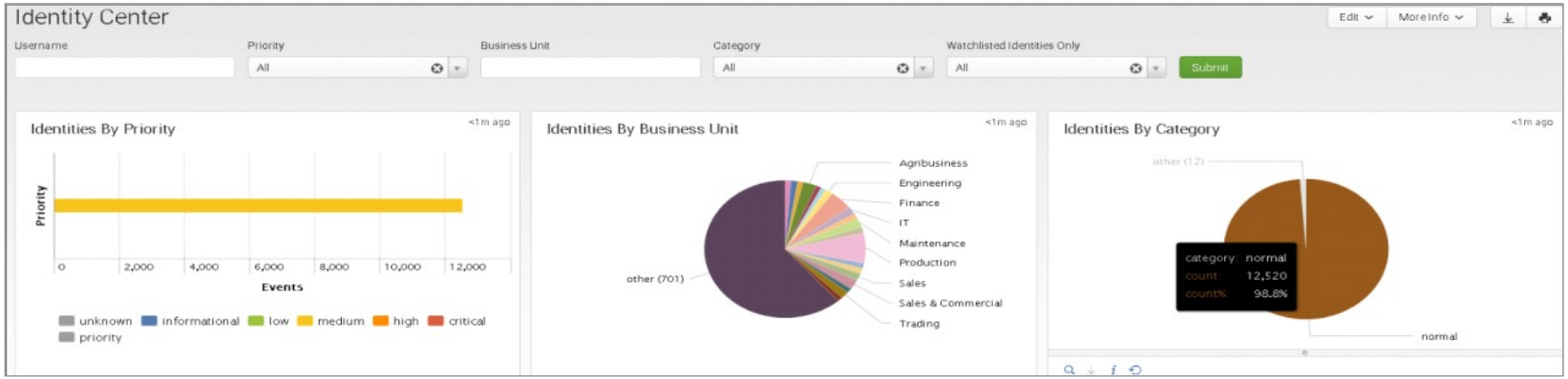
Splunk examples

- Inventory of authorized and unauthorized devices



Source: Splunk

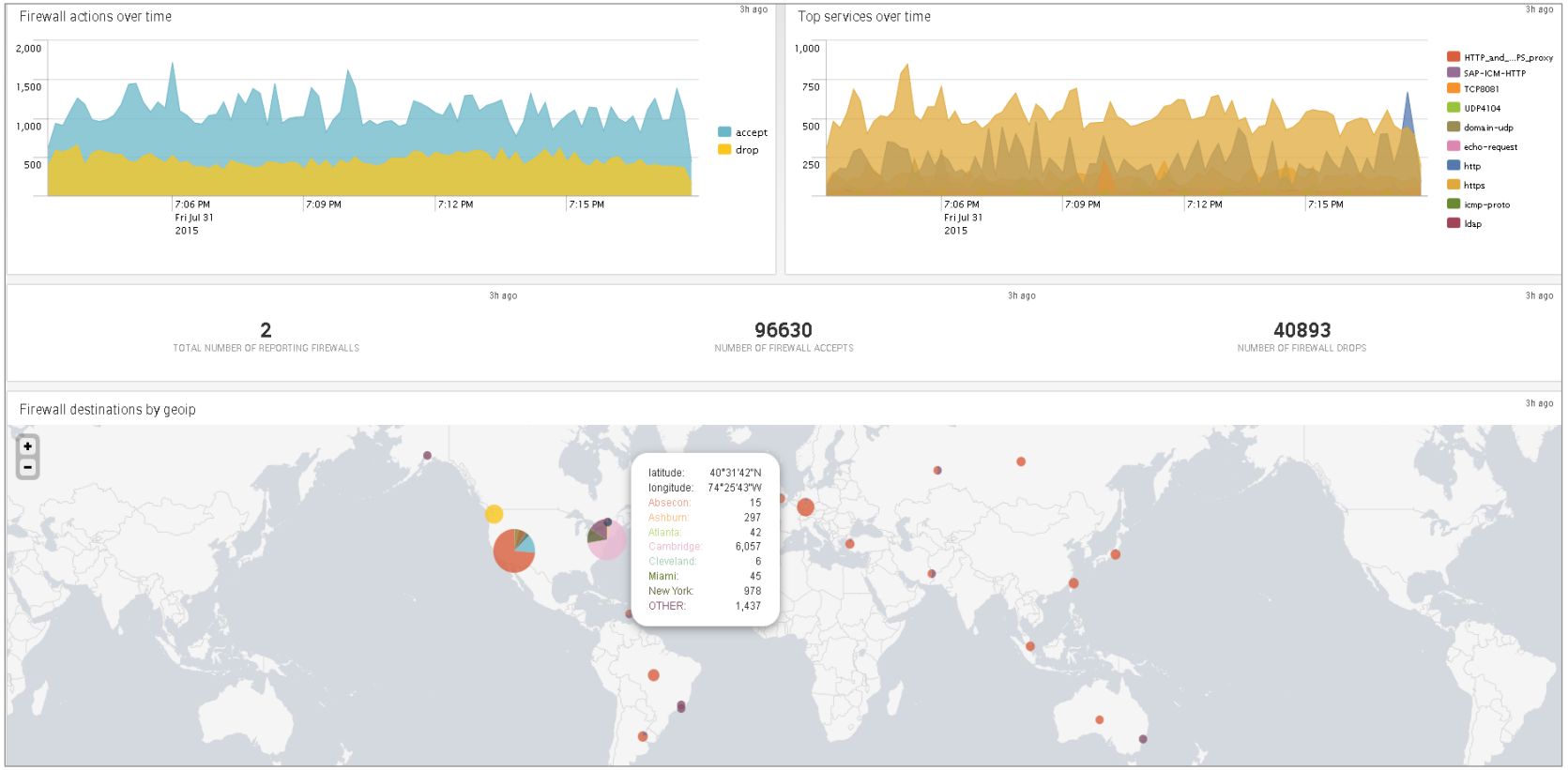
- Controlled use of administrative privileges



Source: Splunk

Splunk examples

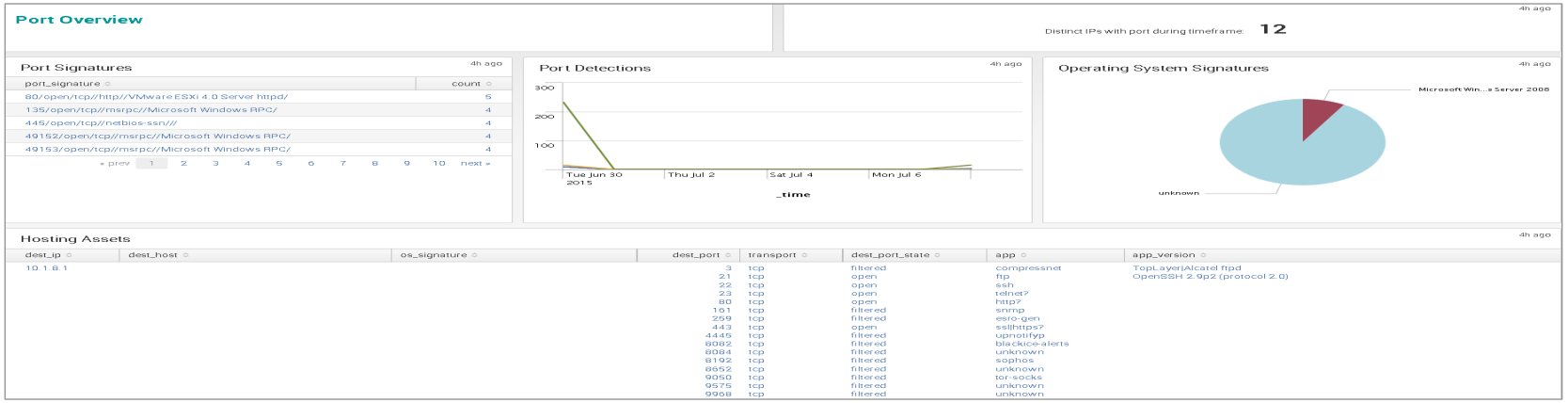
- Maintenance, monitoring and analysis of audit logs



Source: Splunk

Splunk examples

- Limitation and control of network ports, protocol and services



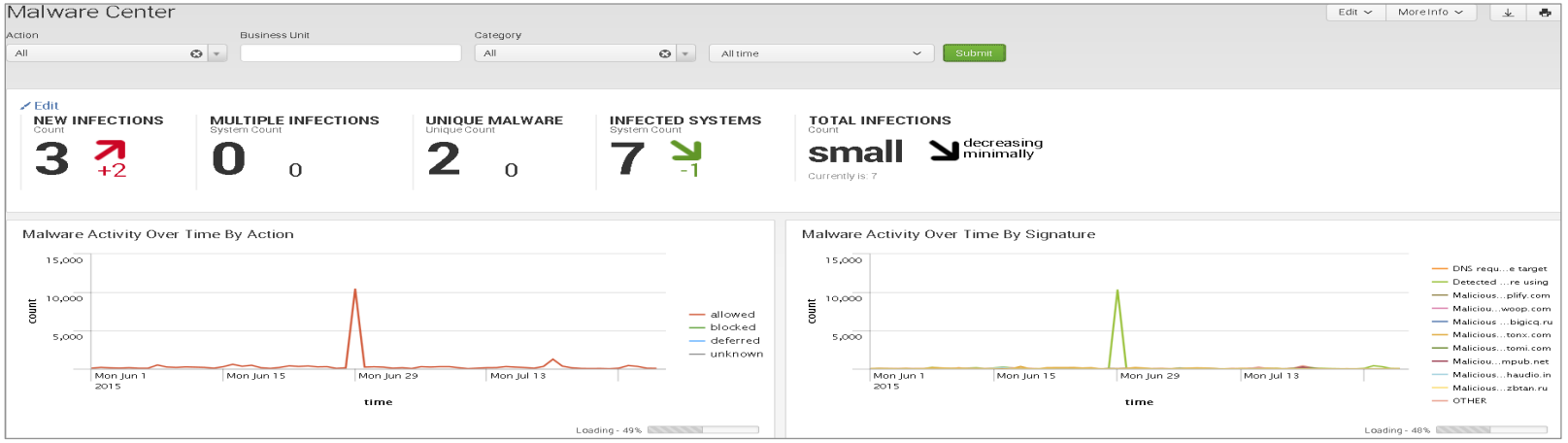
Source: Splunk

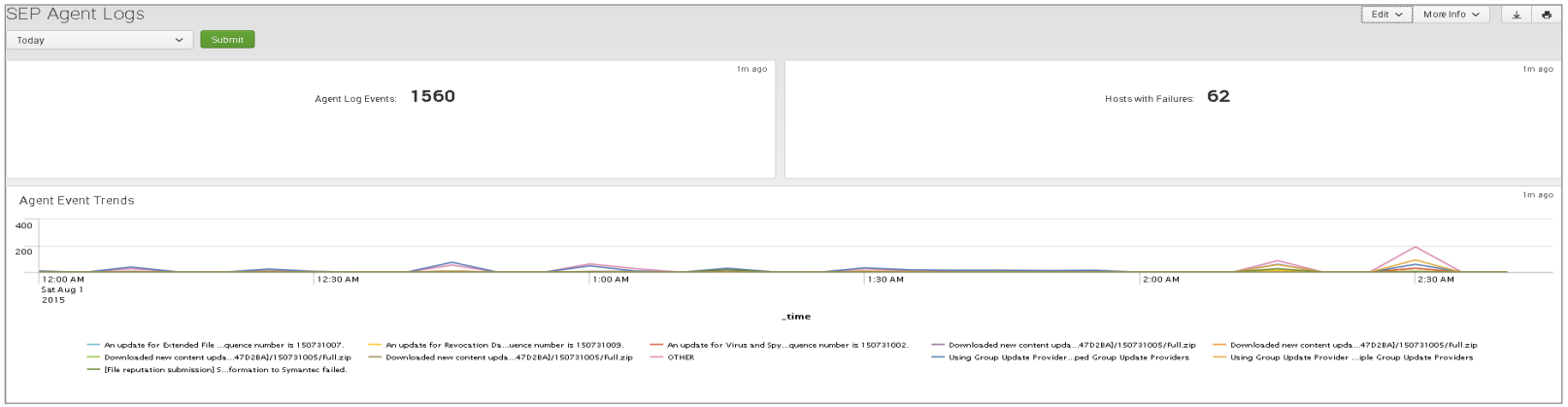
- Continuous vulnerability assessment and remediation

Country	Vulnerability	Count
nu	SSLv3 Padding Oracle Attack Information Disclosure Vulnerability (POODLE)	16,859
GB	SSLv3 Padding Oracle Attack Information Disclosure Vulnerability (POODLE)	28
DE	AutoComplete Attribute Not Disabled for Password in Form Based Authentication	4
DE	JBoss EJBInvokerServlet is Accessible to Unauthenticated Remote Users	4
DE	JBoss HttpAdaptor JMXInvokerServlet is Accessible to Unauthenticated Remote Users	4
DE	SSL Certificate – Signature Verification Failed Vulnerability	4
Total		16,903

Splunk examples

- Malware defenses

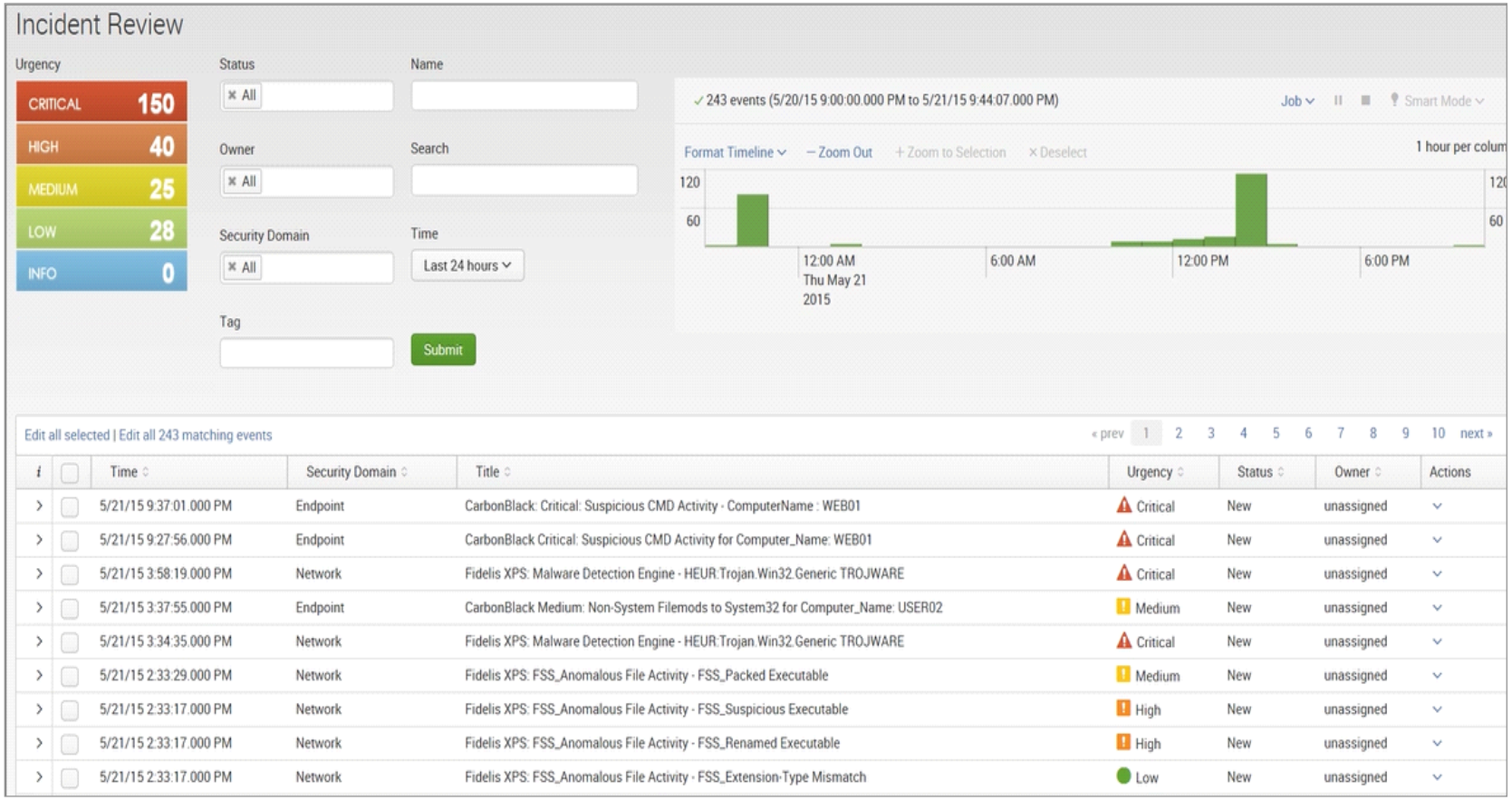




Source: Splunk

Splunk examples

- Incident response and management



Source: Splunk

Questions?

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

1509-1666979
ED None

ey.com