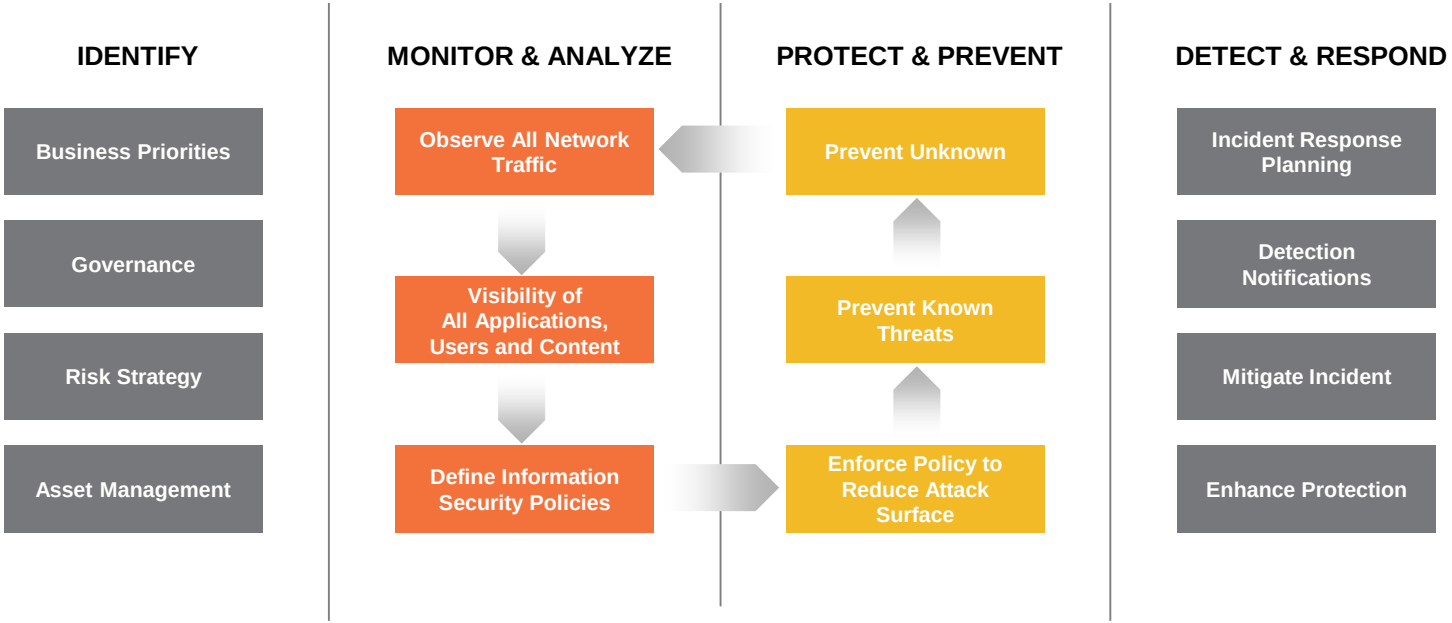
Security Framework: A Guide for Business Leaders

Palo Alto Networks/PwC
May 2016

Security Framework: A Guide for Business Leaders



Security Framework: Identify

DETERMINE BUSINESS PRIORITIES & REQUIREMENTS	ESTABLISH GOVERNANCE STRUCTURES	DEVELOP RISK MANAGEMENT STRATEGY	IMPLEMENT HARDWARE/SOFTWARE ASSET MANAGEMENT
Identify priorities for organization mission, objectives and activities	Establish security roles/responsibilities for board, management and workforce	Integrate cybersecurity into enterprise risk management process	Inventory and classify all enterprise hardware and software
Identify critical functions, applications and dependencies	Identify legal/regulatory cybersecurity requirements	Identify key technical risks and their business impacts	Catalog external information systems
Establish resilience requirements and determine organizational cyber risk tolerance	Align corporate governance and risk management processes to address cybersecurity risk	Assess productivity versus risk implications of security controls for information assets	Map organizational data flows

Security Framework: Monitor & Analyze

OBSERVE ALL NETWORK TRAFFIC

- Monitor and log all network traffic of all internal segmentations
- Monitor and log all network traffic of on- and off-premise users
- Monitor and log all network traffic accessing corporate cloud and SaaS resources

ESTABLISH VISIBILITY OF ALL APPLICATIONS, USERS AND CONTENT TRAVERSING NETWORK

- Map and log all network traffic to specific user identities
- Map and log all network traffic to specific application usage
- Decrypt all inbound and outbound data flows to facilitate full visibility of network traffic
- Manage identities and credentials for authorized devices and users

DEFINE AND/OR REFINE ORGANIZATIONAL INFORMATION SECURITY AND TECHNOLOGY ACCEPTABLE USE POLICIES

- Use observed data to build list of approved business-enabling applications with input from management and technical staff
- Implement employee cybersecurity awareness training

Security Framework: Protect & Prevent

DEVELOP & ENFORCE TECHNICAL POLICIES TO REDUCE ATTACK SURFACE

- Construct whitelist to enable critical business applications; default deny all other applications
- Inspect and judge unknown traffic against determined policies
- Enforce role-based access to applications and data and ensure compromised credentials cannot be used to access applications and data

PREVENT KNOWN THREATS

- Establish logical security perimeter not bound to physical or logical location of devices and data
- Block known threats with existing signatures and intelligence
- Integrate cloud access security with threat detection
- Match newly created signatures to block previously unknown malicious payloads
- Automate defensive reprogramming of all security technologies to incorporate newly created protection mechanisms

PREVENT UNKNOWN THREATS

- Protect endpoints by preventing exploit and malware techniques
- Identify and block malicious lateral movement between components of network, endpoint and cloud
- Incorporate external threat intelligence sources to security monitoring system
- Automate analysis of external threat intelligence

pwc | paloalto NETWORKS

Security Framework: Detect & Respond

ESTABLISH, TEST AND EXECUTE INCIDENT RESPONSE PLAN	INVESTIGATE NOTIFICATIONS FROM DETECTION ENGINES	LEVERAGE TECHNOLOGY TO AUTOMATE DETECTION	CONTAIN AND MITIGATE INCIDENT	INCORPORATE MITIGATIONS INTO PROTECTION MECHANISMS
Establish and conduct regular tests of incident response and recovery plans with executive team and technical staff	Incorporate contextual information around security alerts to determine priority level	Implement log collection capabilities to consume a variety of feeds from the network, endpoint and application layers	Take corrective action to halt ongoing incident	Automate creation of protection mechanism for contained threat
Execute response and recovery plans when deemed necessary	Correlate external data around alerts to provide additional analysis	Aggregate internal logs and external threat intelligence feeds to identify known, signature-based attacks	Mitigate vulnerability or point of compromise and undertake necessary remediation	Automate dissemination of protection mechanism to relevant defensive technologies
Incorporate cross-functional input and lessons learned into incident response plan	Elevate security incidents based on established policy	Identify and investigate anomalous, non-standard behavior in network, endpoint and cloud environments for evidence of malicious activity	Disseminate mitigation and threat information to external parties according to established policy	Automate necessary reprogramming of defensive technologies to reflect new mitigation

pwc

paloalto NETWORKS

About Palo Alto Networks
As the next-generation security company, we are leading a new era in cybersecurity by safely enabling all applications and preventing advanced threats from achieving their objectives for tens of thousands of organizations around the world.

Find out more by visiting www.paloaltonetworks.com

About PwC
At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with more than 208,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details. This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.