"C"

CIPC CYBER SECURITY LANDSCAPE

Pamela Mkosana

November 2017

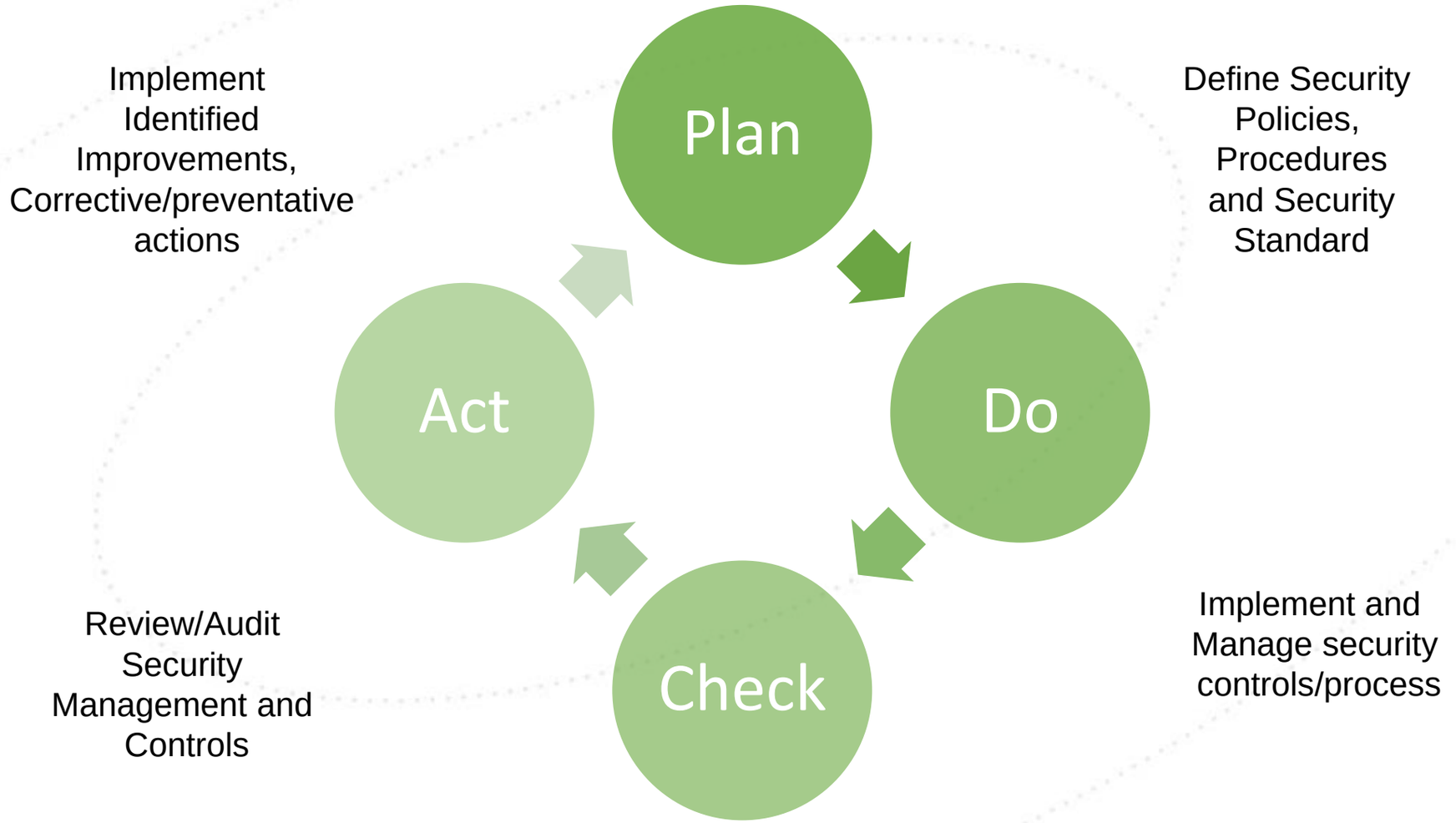
Companies and Intellectual Property Commission

a member of the dti group

CIPC CYBER SECURITY AND ATTACK DEFINITION

- Cyber security is the state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this.
- Cyber security consists of technologies, processes and measures that are designed to protect systems, networks and data from cyber crimes.
- Effective cyber security reduces the risk of a cyber attack and protects CIPC from the deliberate exploitation of systems, networks and technologies.
- Cyber attacks come in various forms and are designed to not only target technological weaknesses (for instance, outdated software) but also exploit people (for instance, uninformed employees who click on malicious links) and a lack of effective organisational processes and procedures.

CIPC INFORMATION SECURITY FUNCTION – PDCA



People

Process

Technology

CIPC INFORMATION SECURITY STRATEGY

Strategic Goal	CIPC Information Security Objectives

Risk Mitigation and Asset Protection	➢ To implement state-of-the-art security technologies in CIPC
	➢ To provide confidence to leadership in the effective and efficient execution of information security responsibilities
	➢ Keep up with new ever-emerging security threats and speed up the response time
	➢ Information security risk mitigation and asset protection
	  o To meet the computing needs of the organization in a secure manner
	  o Safeguarding patient information at rest, in transit, and in use
	➢ Safeguarding the confidentiality, integrity, and availability of the network, systems, and applications
	➢ To move from a reactive to a more proactive response model
	➢ To provide secure computing training and education to the organization

Compliance Obligation	➢ Meet legislative and regulatory requirements, and audit recommendations, for health information custodians ➢ Monitor and validate regulatory compliance

CIPC INFORMATION SECURITY ROADMAP

Roadmap	2017				2018			
	Q1	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
Technology	Anti-Virus ePolicy Orchestrator (ePO)	Drive Encryption (DE)	McAfee Web Gateway (MWG)		Privilege Account Management	Multilayer Authentication		
	McAfee Virus Scan Enterprise (VSE/HIPS)	Network Security Platform (NSP)	Network Threat Behavior Analysis (NTBA)	McAfee SIEM - 1 Year Trial	Acquire New Firewalls			
	DB Security Suite (DAM)	Network Security Manager (NSM)	Network Data Loss Protection (NDLP)				Password Vault Management	
	Threat Intelligence Exchange (TIE),							
		Data Exchange Layer (DXL)	McAfee Active Response (MAR)			24/7 SOC Cyber Intelligence		
		Advance Threat Defense (ATD)						

CIPC INFORMATION SECURITY ROADMAP

Roadmap	2017				2018			
	Q1	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
Process	Proactive Monitoring		Activate Exchange Disclaimer and AD Policy Agreement Issue Notice	Enforce Security Requirement Services Management i.e. Enteprise Project Management or Process Engineering	POPI Implementation		Incident Management	Customer Satisfaction Surveys
	User Account Management	Review of Information Security Policies	Segregation of Duties (IT)			eDiscovery and Forensics	Problem KPI's	
		Measurement Framework	Implement and enforce Data/File/Document Classification	Security Risk KPI's	Penetration Test			External Assessment for Information Security Maturity
		Information Security Management Systems (ISMS)		Black Box Web Application testing				
			ROI Analysis	Security Compliance Programs	Security Problem Management		Incident Management KPI's	
		Key Security Standards	Information Security Governance	Security Knowledge Management		Information Security SOP's		

CIPC INFORMATION SECURITY ROADMAP

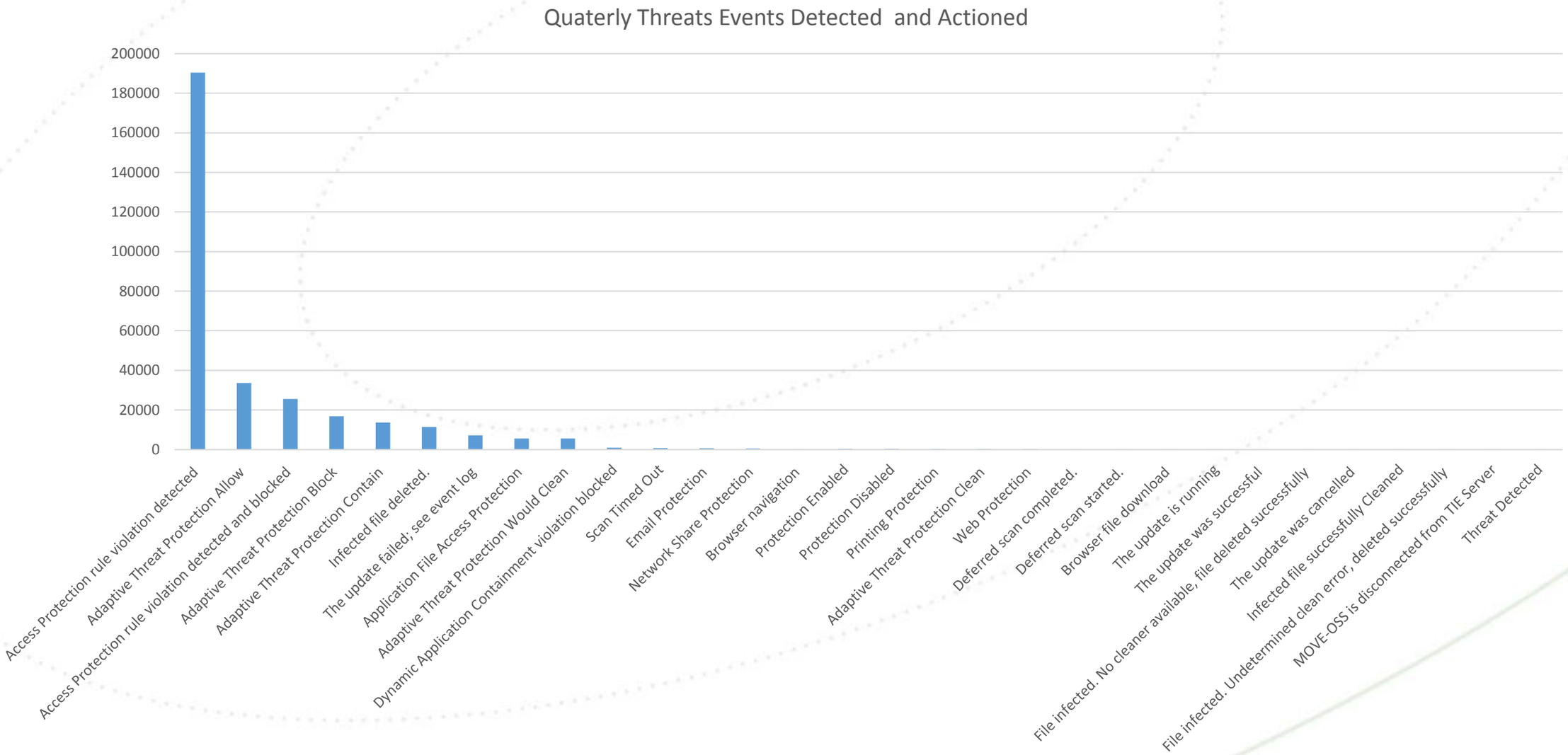
Roadmap	2017				2018			
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
People			Roles and Responsibilities (Ownership)		Introducing Performance Appraisal Points for Risk Champions	Develop Platforms for External Stakeholders to report Privacy issues		
Benefits	Entrance endpoint protection.	Management correlations, and responsiveness to events. Started building the formal SIF Team.	Streamline UAM processes and adding auditability, Kick start user awareness.	Simplify forensic efforts.	Improves Procedural Rigor.	Additional data leakage protection.	Enhanced security intelligence and process maturity to leverage it proactively.	Further enabling Incident management.
	Management and organisational awareness enhancement.		Continue to build SIF team capabilities	Formalise problem management and demonstrate value to CIPC.	Simplified eDiscovery Automated Incident Management	Metrics for reporting to management.	Automate Incident and problem Management Process	
	ISMS Project team capabilities		Enhance protection of sensitive data/documents			Staff retention and engagement.		

CIPC INFORMATION SECURITY RESILIENCE STATUS HIGHLIGHTS

IT Security Projects 2017/2018	Components	Project Status
Implementation of McAfee Security Solution	Integrated Security Components:	
	➢ Anti-Virus ePolicy Orchestrator (ePO)	100%
	➢ McAfee VirusScan Enterprise (VSE)	100%
	➢ Network Security Platform (NSP)	50%
	➢ Network Security Manager (NSM)	100%
	➢ Network Threat Behavior Analysis (NTBA)	100%
	➢ Drive Encryption (DE)	100%
	➢ Intrusion Prevention System (IPS)	100%
	➢ Advance Threat Defense (ATD)	100%
	➢ McAfee Web Gateway (MWG)	100%
	➢ Network Data Loss Protection (NDLP)	50%
	➢ Network Data Loss Protection Endpoint (NDLPe)	50%
	➢ Threat Intelligence Exchange (TIE), Data Exchange Layer (DXL), McAfee Active Response (MAR)	100%
	➢ Database Security Suite (DAM)	100%
Information Security Management Systems (ISMS) Project	➢ Information Security Policy Reviews ➢ Security Domain Standards	60%
Information Security Awareness Program	➢ Information Security Awareness Workshops	50%
Separation of CIPC from DTI network	➢ “To Be” CIPC Network Topology and Implementation ➢ Readiness Assessment Results and Implementation.	20%

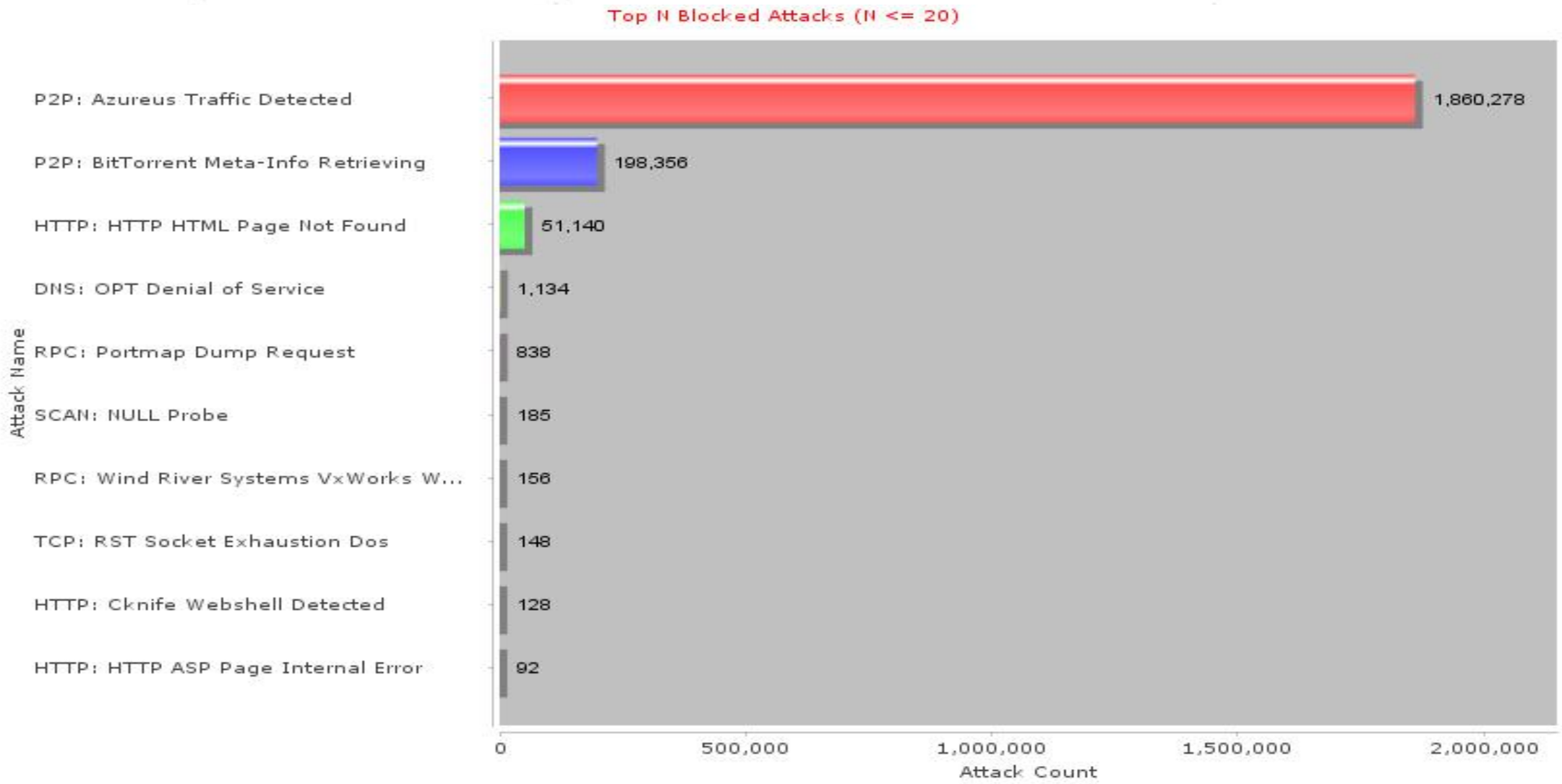
CIPC INFORMATION SECURITY RESILIENCE STATUS HIGHLIGHTS

The following statistics depicts threat events that have been contained in various information resources.



CIPC Information Security Resilience Status Highlights

The following statistics depicts the IPS have successfully detected and blocked 2112958 hacking attempts.



SECURITY ITS NOT AN OPTION
ITS OUR PASSION