Escalation Chart														
Event	Action	Capacity	Preparation capability	Man lab	auto lab	Not WB	WB	Remote analysis	Isolation	Integrity calc	Report to authorities	Inform authorities	Sample Isolation	Severity
potentially unwanted programs (PUP)	remove program	monitor for recurrence	Corporate image					x		x				1
warning banners	remove program	monitor for recurrence	Corporate image					x		x				3
clean alerts from antimalware solution	remove program	monitor for recurrence	Corporate image					x		x				3
Adware	remove program	monitor for recurrence	Corporate image					x		x				4
Phishing	Rely on Spamfiltering	monitor for recurrence	Corporate image					x		x				5
Spear Phishing	analyse threat	analyze with detached system	Lab			x		x		x	x	x	x	8
malware detected and deleted	re-install system	monitor for recurrence	Corporate image		x			x	x	x				2
malware partially detected	re-stablish system from backup	monitor for recurrence	Corporate image		x			x	x	x				7
malwarebehaviour and not detected	re-install system	monitor for recurrence	Corporate image	x	x			x	x	x			x	10
Macro viruses	re-install system	monitor for recurrence	Corporate image					x		x			x	8
Copyright infringement	Withhold HW ans secure user traces	physical secure evidence	Writeblocker	x		x		x		x			x	10
Passwords leaks with e-mail	Change passwords and enable MFA	monitor for recurrence	Awareness plan			x		x		x				5
Spear phishing and data not delivered	Change passwords and enable MFA	monitor for recurrence	Awareness plan			x		x		x				4
Attempts to escalate privileges	Determine MO and escalate to IR	DFIR plan	Forensic analysis	x		x		x		x	x	x	x	9
Attempts of lateral movement	Determine MO and escalate to IR	DFIR plan	Forensic analysis	x		x		x		x	x	x	x	10
Usage of CVE 7+ vulnerabilities	re-stablish system from backup	inform senior management of risk	Corporate image + patch			x		x		x			x	9
CVE 7+ vulnerabilities identified	Create Risk analysis	governance plan	Forensic analysis and monitor	x		x		x		x				6
Rootkits detected on system	Determine MO and escalate to IR	datacollect and re-install	Forensic analysis and monitor	x		x		x		x	x	x	x	9
Remote Access Trojan (RAT)	Determine MO and escalate to IR	DFIR plan	Forensic analysis and monitor	x		x		x		x	x	x	x	10
Zero days (internal systems/network)	Create Risk analysis	governance plan	vulnerability scanner			x		x		x				5
Zero days (Facing Internet)	Determine MO and escalate to IR	DFIR plan	Forensic analysis and monitor	x		x		x		x				10
APT	Determine MO and calculate risk	restore from backup	Forensic analysis and monitor	x		x		x		x	x	x	x	10
unpached systems	Roll into patch mangement	governance plan	Monitor activity			x		x		x				5
Malware not detected and activated	Determine action and severity	DFIR plan	Forensic analysis and monitor			x		x		x			x	10
Spear phishing and data delivered detected	Determine MO and calculate risk	inform senior management of risk	Monitor activity	x	x	x	x	x	x	x	x	x	x	10
Services have been breached	Analyze logs and periphials - restore	DFIR plan	Corporate image			x		x	x	x			x	10
Accounts have been escalated	Determine MO and escalate to IR	DFIR plan	Forensic analysis and monitor			x		x	x	x	x	x	x	8
Targeted attacks (unsuccessful)	Determine MO and calculate risk	inform senior management of risk	Forensic analysis and monitor	x	x	x		x		x			x	7
Targeted attacks (successful)	Determine MO and escalate to IR	DFIR plan	Forensic analysis	x	x	x		x	x	x	x	x	x	10
Insider threats or paid actors	Determine MO and escalate to IR	DFIR plan	Forensic analysis	x		x	x	x		x	x	x	x	10
EOL software (Internal)	Create Risk analysis	governance plan	vulnerability scanner			x		x		x				5
EOL software (external)	Determine MO and calculate risk	inform senior management of risk	vulnerability scanner			x		x		x				8
EOL hardware	Create Risk analysis	governance plan	vulnerability scanner			x		x		x				4
Legacy systems	Create Risk analysis	governance plan	vulnerability scanner			x		x		x				5
User violated AUP	Determine MO and escalate accordingly	warn and inform (monitor)	Plan from HR	x	x	x	x	x	x	x	x	x	x	7
User violated AUP intentional	Determine MO and escalate accordingly	datacollect	Plan from HR	x	x	x	x	x	x	x	x	x	x	10