Team 3
CyberSecurity Project

(IMV-CS1002)

Yeong Chung Yee
Lindsay Marsh

Joseph Ramon
Simon Oh

WE CAN NEITHER CONFIRM NOR DENY THE FOLLOWING EVENTS

The story and scenarios portrayed in the presentation are purely hypothetical. Any similarity to people, living or dead, or actual events, is purely coincidental

OUR COMPANY

SIGURNOST CONSULTING

Sigurnost Consulting is one of the world's leading IT Security management consulting firms. We work with top executives to help them make better decisions, convert those decisions to actions, and deliver the sustainable success they desire.

CLIENT PROFILE

ROLLS ROYCE Singapore is a key hub for Civil and Defence Aerospace, Marine and Power Systems.

From here, they manufacture components and assemble engines, support their regional customers and undertake a broad range of Research and Technology activities. It's also the regional headquarters for several Group functions.

Together with their joint ventures, they employ over 2,300 highly talented people in Singapore.

- https://careers.rolls-royce.com/usa/our-locations/singapore/
- https://asianaviation.com/rolls-royce-consolidating-operations-in-singapore-closing-some-operations-in-great-britain/

SCENARIO

Rolls Royce Singapore Seletar Campus is their most modern manufacturing, testing, training and research facility to date and is their main site in Singapore. Covering 65,000 square metres and located on the Seletar Aerospace Park, it represents an investment of over S$700 million and has created hundreds of new jobs in the region.

The Campus is the only place outside the UK to manufacture their hollow titanium wide chord fan blades, and has been awarded Singapore's Distinguished Partner in Progress Award, the nation's highest corporate honour.

The cutting edge research and technology employed by Rolls Royce makes it a prized target for governments and hackers.

This threat is recognised by Rolls Royce and a sophisticated Cybersecurity Department has been deployed complying with Industry Standards (NIST and ISO-27001).

Despite significant investment, Rolls Royce was successfully infiltrated by suspected state-sponsored hackers attempting to exfiltrate highly sensitive data with a sophisticated, well planned Advanced Persistent Threat (APT).

SIGURNOST CONSULTING

KILL CHAIN TIMELINE

Feb 2020

Target identified and spear phishing was used to trick sales staff into installing malware on his work laptop which allows the hacker to enter Rolls Royce corporate via VPN.

Mar 2020

Remote C&C is established with backdoors

Jun 2020

QRadar detected anomalous activity from manufacturing plant server but was not properly addressed.

Sep 2020

SOC discovers breach and prepares sandbox to monitor the breach.

Oct 2020

Hackers realised they have been discovered, DDoS attack launched from compromised hosts to attack Rolls Royce's public facing systems to distract the SOC team.

Nov 2020

Compromised computers patched and malware removed.

Dec 2020

Hackers completely removed from network. All services fully restored.

KILL CHAIN

STAGE 1. RECONNAISSANCE

Event Timeline: February 2020

- Sales staff were targeted via social media such as LinkedIn and Facebook.
- These staff were carefully selected based on their social media activities as well as business contacts.
- This likely included the investigation of IT systems of suppliers and business partners to find possible attack vectors.

KILL CHAIN

STAGE 2. WEAPONISATION

Event Timeline: February 2020

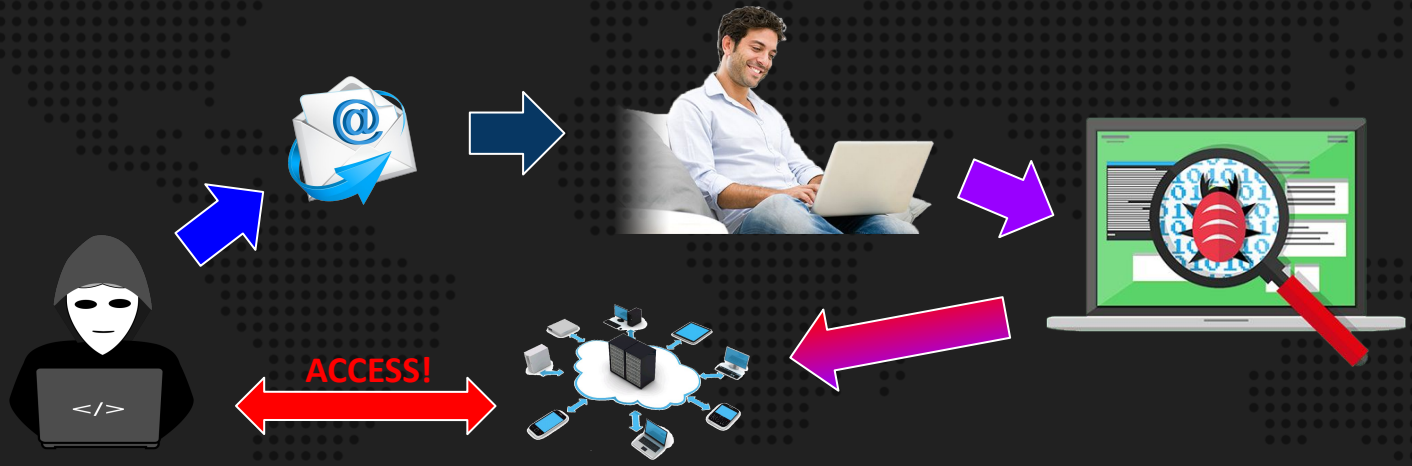
- At this point, the hackers used the information that has been gathered to start preparing the tools they required for the breach.
- This included making modifications to their malware to make it practically undetectable to most defense systems.
- It is also expected that external IT systems have already been exploited to be used at this stage.

KILL CHAIN

STAGE 3. DELIVERY

Event Timeline: March 2020

- Spear phishing was utilised to initiate the process. Upon clicking on a link to a website in an email sent by a spoofed business lead, a Metasploit based malware (Meterpreter) was delivered to the corporate laptop of the sales staff.
- The legitimate website was likely to have been hacked to lead to the source of the malware.
- This allowed the hacker(s) to traverse through the company's VPN.



KILL CHAIN

STAGE 4. EXPLOITATION

Event Timeline: March 2020

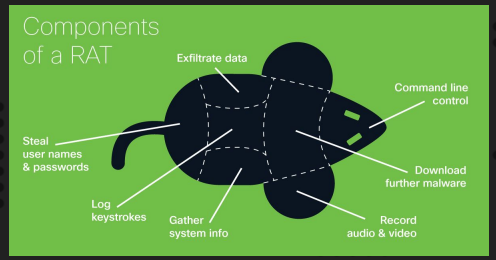
- Hackers carefully probed the network to find computers which were less secure to plant their malware and other breaching tools.
- These were machines where security patches were not promptly applied due to system compatibility issues, especially those in the manufacturing plant.
- Also vulnerabilities on servers were likely to be exploited using hacks like SQL injection, particularly on antiquated systems.

KILL CHAIN

STAGE 5. INSTALLATION

Event Timeline: May 2020

- Backdoors utilising Remote Access Trojans (RAT) were planted on the compromised computers including desktops and servers for the manufacturing plant. These were similar to popular RATs like SubSeven, Back Orifice, ProRat, Turkojan, and Poison-Ivy but were more advanced and updated to bypass the anti-virus software on Windows based computers.
- More indicators of malware were found on several computers in various departments including electrical & controls and R&D.
- These were likely to be data exfiltration malware based on Metasploit such as Meterpreter or those of a polymorphic nature.



The Complete Meterpreter Guide | Privilege Escalation & Clearing Tracks https://youtu.be/xsyeL6xWWy4

KILL CHAIN

STAGE 6. COMMAND & CONTROL

Event Timeline: March-June 2020

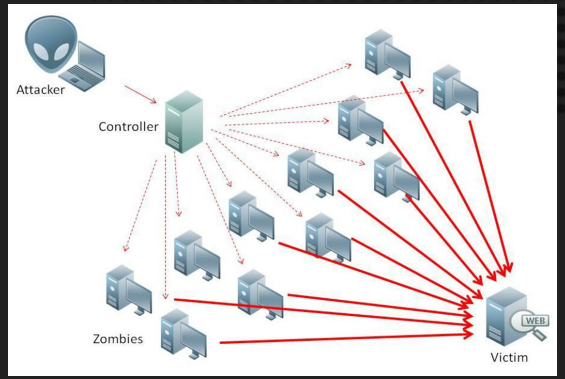
- Hackers searched the network for intellectual assets and they were very careful not to trip any detection systems. And preliminary investigation showed they were targeting R&D plans.
- Hackers also gained a foothold after obtaining admin access to several desktop computers and servers and created hidden users with administrative powers.
- Trail was well obfuscated which made it hard for the IT security forensics team to determine what exactly happened.

KILL CHAIN

STAGE 7. ACTIONS ON OBJECTIVES

Event Timeline: Jun-Dec 2020

- Exfiltration of encrypted draft aerospace R&D documents happened slowly over 6 months at least to prevent detection of large amounts of data.
- Hackers launched a DDoS attack on the public facing servers of Rolls Royce after realising they have been discovered (lost C&C of some victim hosts).
- DDoS was launched from compromised hosts from all over the globe to distract the security team while they made their final attempt to obfuscate their attack.

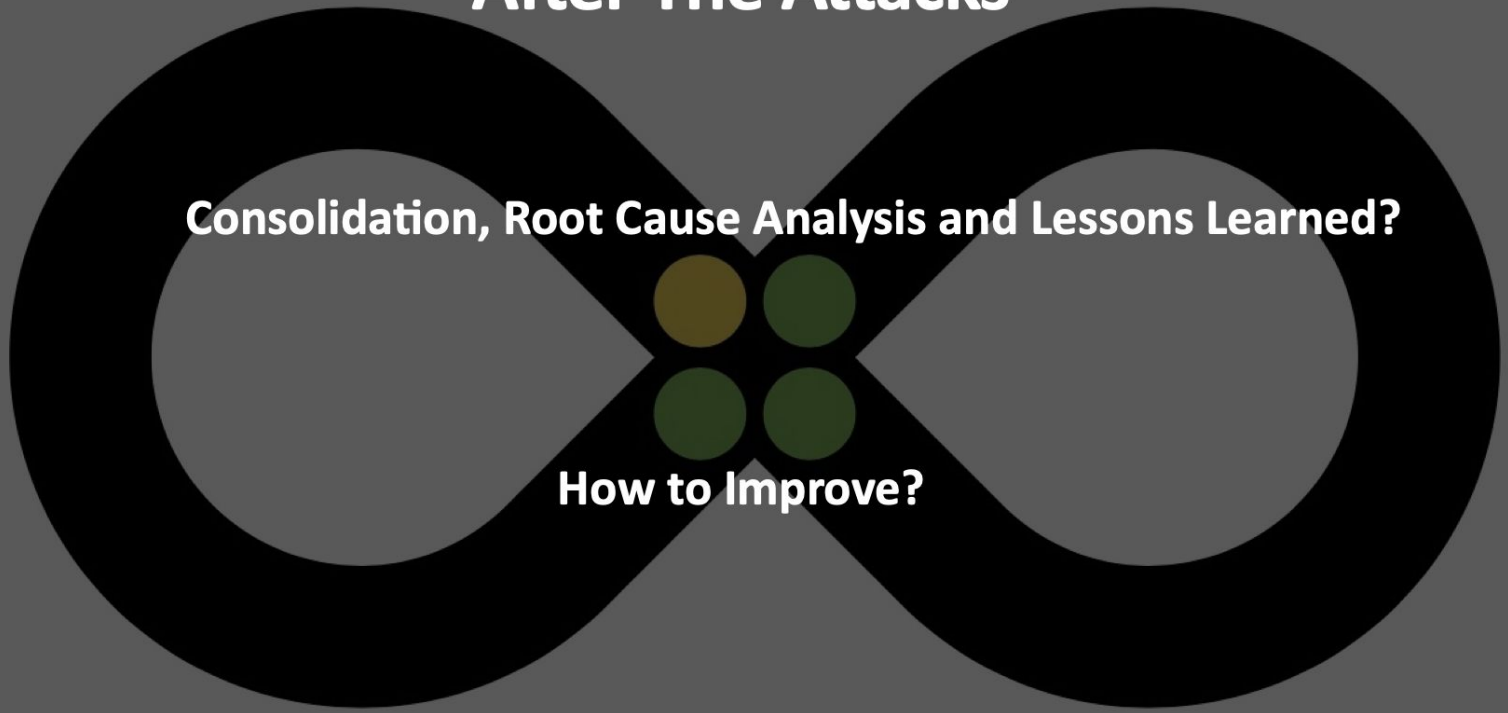


EARLY DAMAGE ASSESSMENT

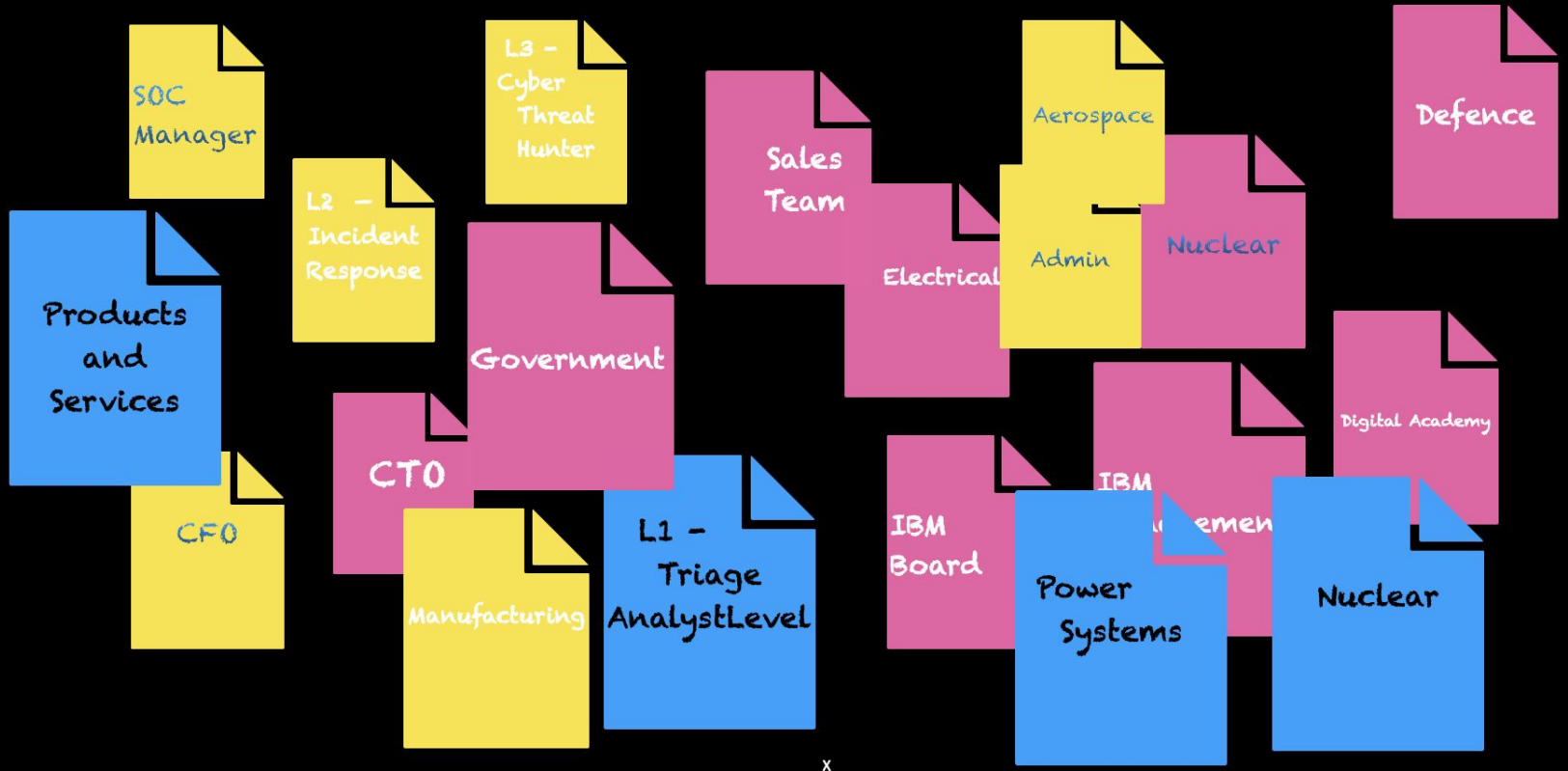
Impact: **MODERATE**

- Indicates several severe vulnerabilities in the network were utilised in the breach.
- Leakage of confidential but strongly encrypted draft R&D plans which would not be of much use to hackers.
- Shows antiquated systems are still very vulnerable even when sitting behind defense systems that are top-notched.
- Any weak point in the network can discovered by hackers given sufficient time.

After The Attacks



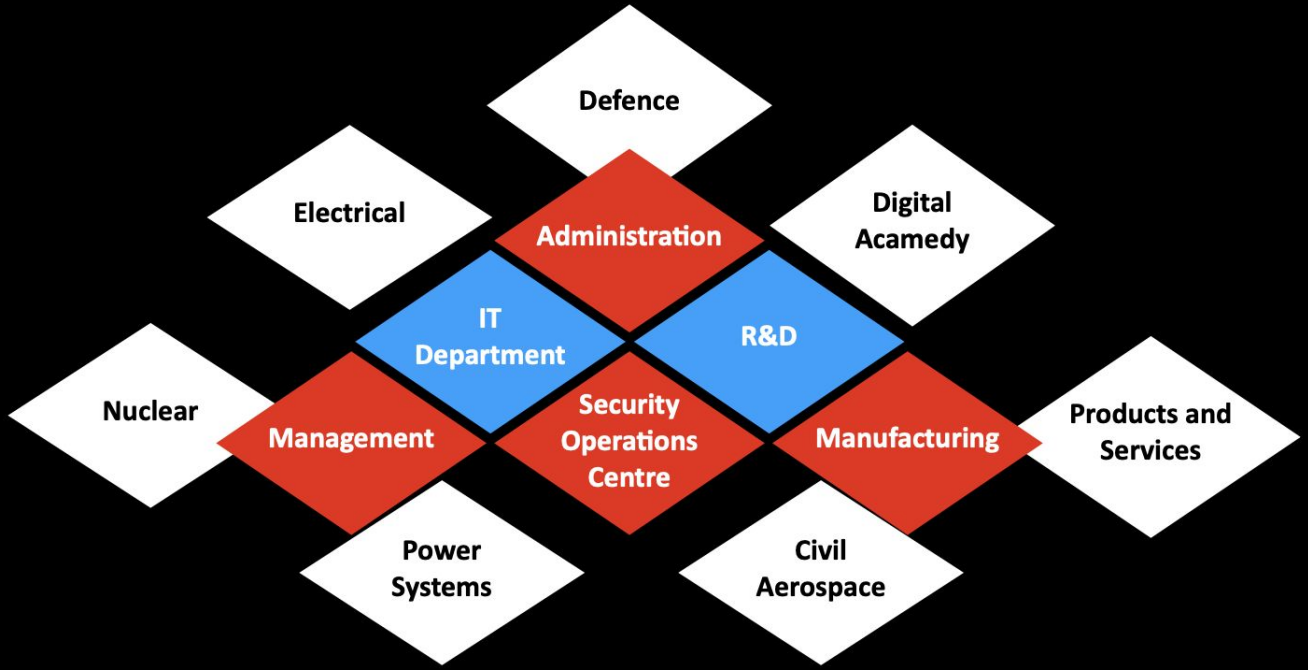
Stakeholders



Stakeholders - Grouping

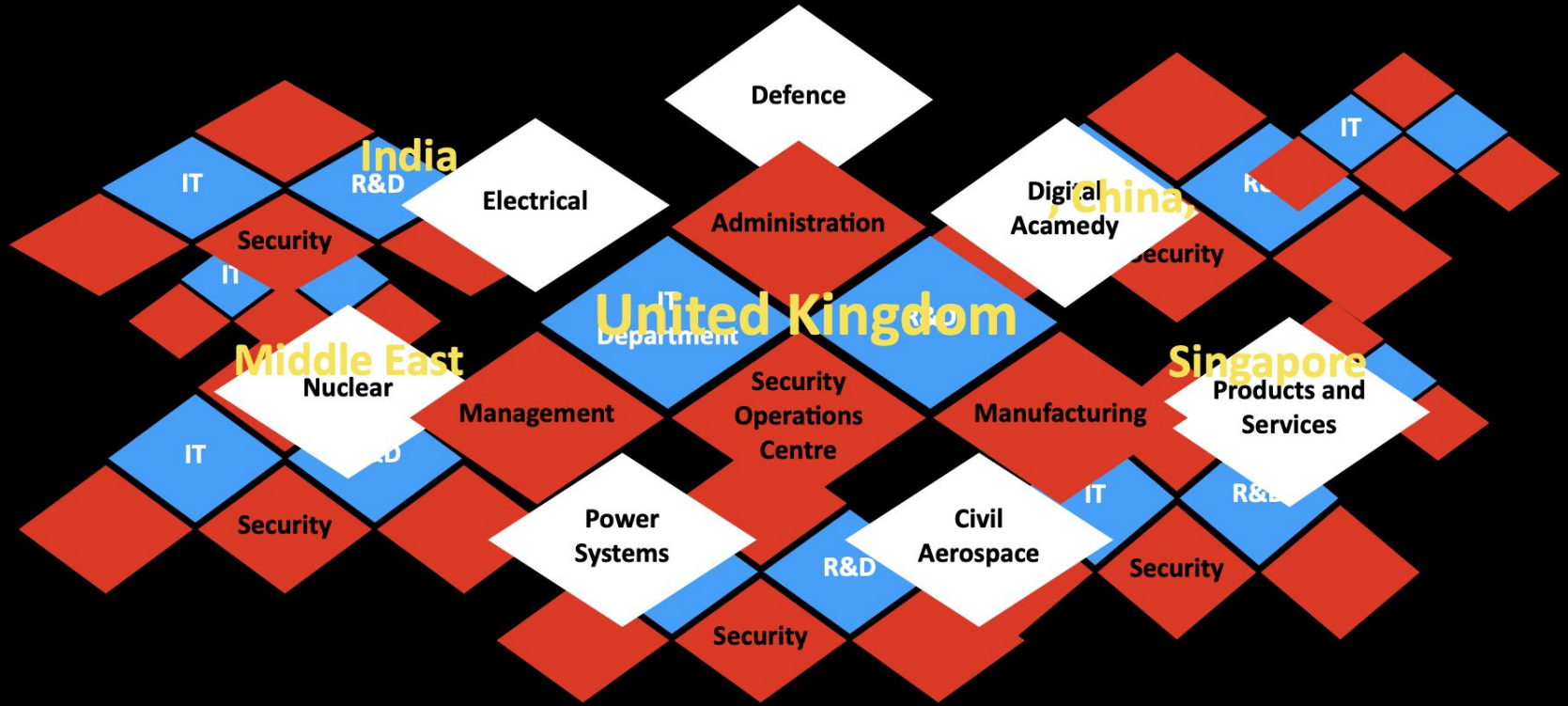
Stakeholders - Departments

Rolls Royce is organised into 6 distinct, but related divisions



Stakeholders - Geographical Locations

Singapore is one of Rolls Royce's 5 Global Hubs



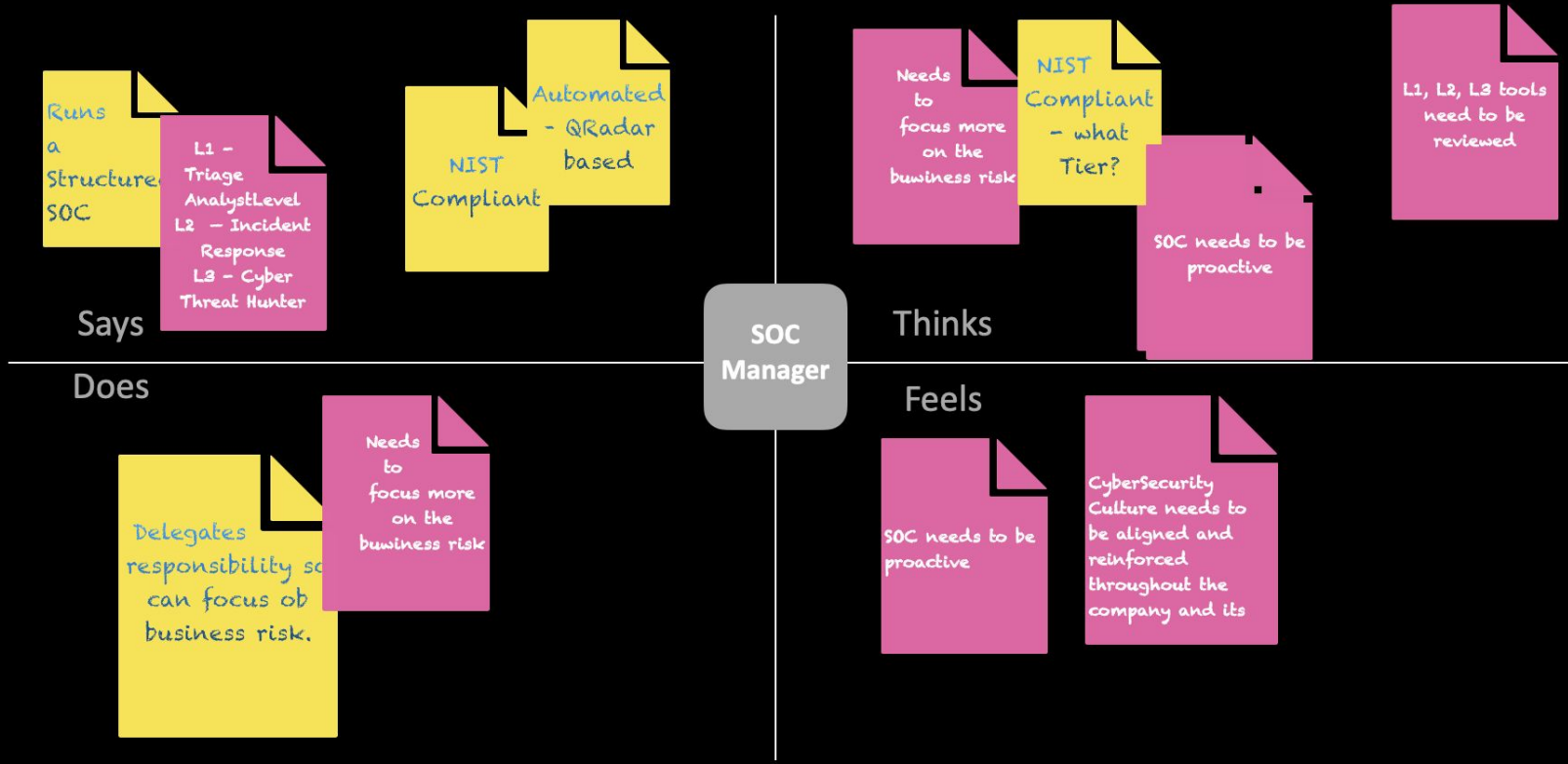
Stakeholders

So who are the actual stakeholders in Singapore?

- Security Operations Centre
  - SOC Manager - Primary Stakeholder, responsible for the Cybersecurity of the Singapore entity. Runs a well structured team comprising
  - Level 1 - Triage Analyst
  - Level 2 - Incident Response
  - Level 3 - Cyber Threat Hunter
- IT Department
  - Stakeholder, responsible for implementation of hardware and software.
- Management
  - Loss of reputation, need to set the standards for Singapore, and ensure they are propagated throughout the company and its dependency ecosystem.
  - Need to create an environment where there is an appetite for improvement
- All Departments and Employees
  - Sales personnel were targeted for the main offence.

x

Empathy Map


Runs a Structured SOC
L1 – Triage AnalystLevel L2 – Incident Response L3 – Cyber Threat Hunter
NIST Compliant
Automated - QRadar based
Says
Needs to focus more on the buwiness risk
NIST Compliant – what Tier?
SOC needs to be proactive
L1, L2, L3 tools need to be reviewed
Thinks
SOC Manager
Does
Delegates responsibility so can focus ob business risk.
Needs to focus more on the buwiness risk
Feels
SOC needs to be proactive
CyberSecurity Culture needs to be aligned and reinforced throughout the company and its

Security Operations - Centre Roles

Monitoring, Security incident response, Security Information and Event Management (SIEM), Threat intelligence, Information risk management, Information assurance (IA), Information security compliance, Security governance.

Security Operations Center (SOC) Manager

This role encompasses managing there entire SOC team. SOC Managers have an intimate understanding of all SOC tiers. In addition, communication with the CISO, other business leaders, partners and audit an compliance heads is mandatory. Strong People management and crisis management skills are also needed.

L1 - Incident responder / Security Analyst- Triage

As the SOC's first responder, the incident responder is responsible for configuring and monitoring security tools, as well as using these tools to identify threats. The job, which maps to the Tier 1 level in the SOC, involves looking into the hundreds of alerts received daily to triage, classify and prioritize them. Once this is done, the information is ultimately handed off to the security investigator.

L2- Incident Response Security Analyst - Investigation

Using sophisticated allies, such as threat intelligence, the security investigator's job is to identify affected hosts and devices and then evaluate running and terminated processes. This usually also involves deeper investigation to identify sources of attack, lateral movement analysis, methodologies used and duration of residence of the attack vector in the environment. Security investigators, which map to Tier 2, are also responsible for crafting and deploying mitigation and eradication strategies.

L3 Cyber Threat Hunter / Advanced security analyst

The advanced security analyst, who is in Tier 3, is the most experienced of the SOC crew. These analysts usually work in the background to identify unknown vulnerabilities, review past threats and mitigations, and assess vendor health and product vulnerabilities. They make recommendations to change products, processes and tools.

IT / Operations

Responsible for the Infrastructure data and software.
Blocks inbound attack traffic, disables users.
Implements and evaluates new software

https://searchsecurity.techtarget.com/tip/5-key-enterprise-SOC-roles-and-responsibilities x

Security Breaches

Phishing - Exfiltration Malware

End-Point -Salesman Targeted to gain credentials to access the Rolls Royce Network

Hacker able to perform reconnaissance and gain access to Research Data

The attack vector was comprised delivery of Fileless Metamorphic Malware installing a Reverse TCP process to exfiltrate data

Unusual port activity detected by SOC, offences found and closed.
SOC communicated breach details to Management, Stakeholders and Regulatory Authorities.

DDOS - Diversion

Initial hack allowed time for reconnaissance and identify ips and ports to attack

The attacker used several networks to launch the attack on the ports discovered by Phishing mail

SOC identified targets and implemented existing DDOS Defence Tools eg IP-based Access Control Lists (ACLs) . DDOS attack mitigated

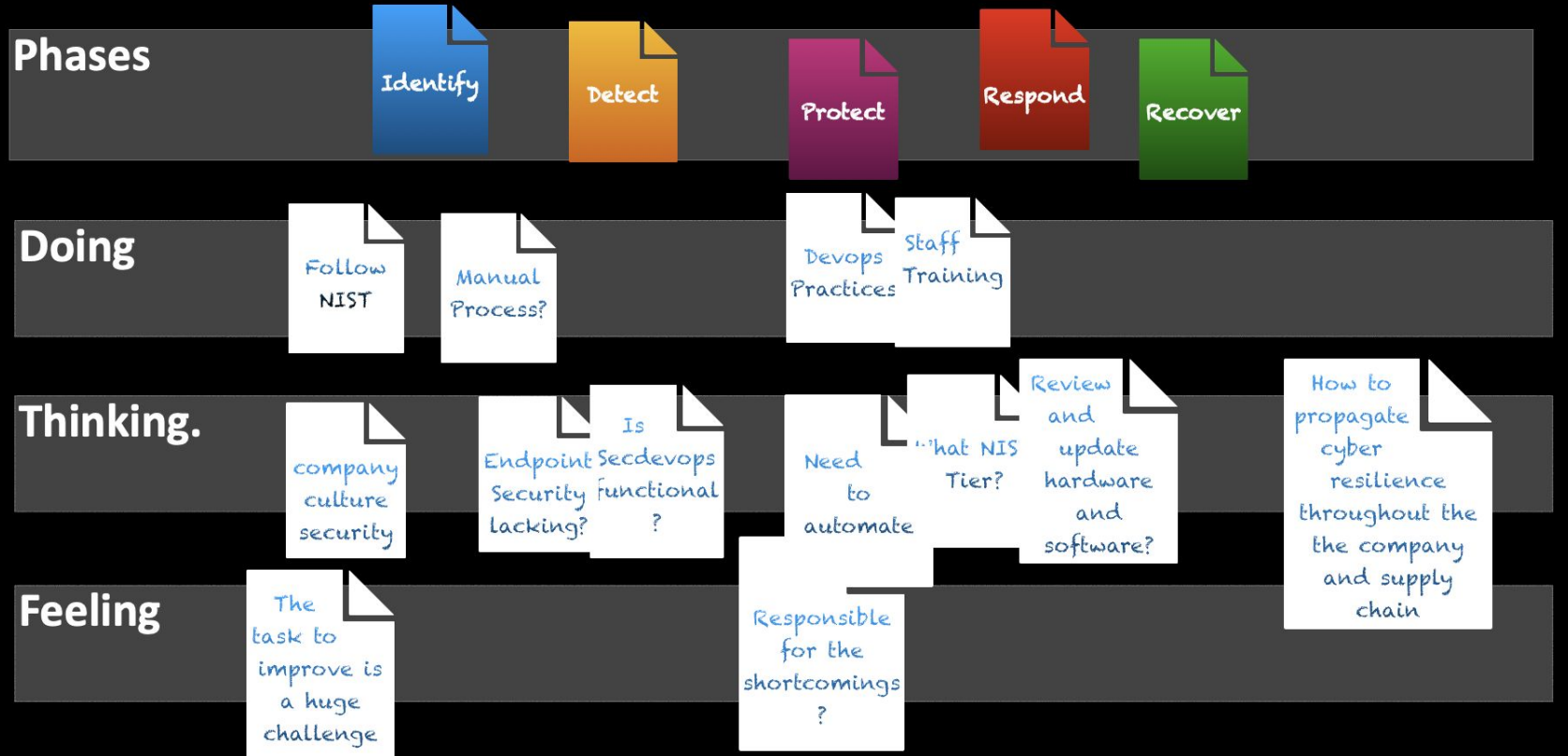
SOC communicated breach details to Management, Stakeholders and Regulatory Authorities.

x

Security Operations Centre - Pain Points

- Timeline from Identify through to Recovery too long
- Endpoint security exposed as a weakness.
- Threat detection inadequate
- Prevention inadequate
- Improve CyberSecurity culture throughout the organisation
- Streamline and simplify

As Is Scenario



Cybersecurity Framework?

- **Core**
  - Desired cybersecurity outcomes organized in a hierarchy and aligned to more detailed guidance and controls
- **Profiles**
  - Alignment of an organization's requirements and objectives, risk appetite and resources ***using*** the desired outcomes of the Framework Core
- **Implementation Tiers**
  - A qualitative measure of organizational cybersecurity risk management practices

x

NIST Cybersecurity Framework Components - What Level?

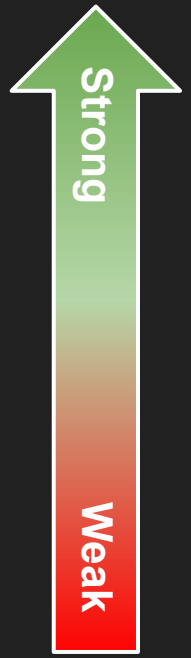
SIGURNOST CONSULTING

Framework Core

Functions	Categories	Subcategories
Identify	Asset Management (ID.AM) Business Environment (ID.BE) Governance (ID.GV) Risk Assessment (ID.RA) Risk Management Strategy (ID.RM) Supply Chain Risk Management (ID.SC)	ID.AM-1 to ID.AM-6 ID.BE-1 to ID.BE-5 ID.GV-1 to ID.GV-4 ID.RA-1 to ID.RA-6 ID.RM-1 to ID.RM-3 ID.SC-1 to ID.SC-5
Protect	Identity Management, Authentication and Access Control (PR.AC) Awareness and Training (PR.AT) Data Security (PR.DS) Information Protection Processes and Procedures (PR.IP) Maintenance (PR.MA) Protective Technology (PR.PT)	PR.AC-1 to PR.AC-7 PR.AT-1 to PR.AT-5 PR.DS-1 to PR.DS-8 PR.IP-1 to PR.IP-12 PR.MA-1 to PR.MA-2 PR.PT-1 to PR.PT-5
Detect	Anomalies and Events (DE.AE) Security Continuous Monitoring (DE.CM) Detection Processes (DE.DP)	DE.AE-1 to DE.AE-5 DE.CM-1 to DE.CM-8 DE.DP-1 to DE.DP-5
Respond	Response Planning (RS.RP) Communications (RS.CO) Analysis (RS.AN) Mitigation (RS.MI) Improvements (RS.IM)	RS.RP-1 RS.CO-1 to RS.CO-5 RS.AN-1 to RS.AN-5 RS.MI-1 to RS.MI-3 RS.IM-1 to RS.IM-2
Recover	Recovery Planning (RC.RP) Improvements (RC.IM) Communications (RC.CO)	RC.RP-1 RC.IM-1 to RC.IM-2 RC.CO-1 to RC.CO-3

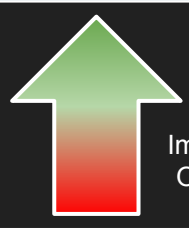
Framework Tiers

Tier#
Tier4: Adaptive • Adaptive risk management practice • Cultural, risk-informed program • Actively shares information
Tier3: Repeatable • Formalized risk management • Organization-wide program • Receives external partner information
Tier2: Risk Informed • Some risk management practices • Increased awareness, no program • Informal external participation
Tier1: Partial • Ad hoc risk management • Limited cybersecurity risk awareness • Low external participation



Framework Profile

Target Profile
Desired state of alignment between core elements and organizational requirements, risk tolerance, and resources
Where do I aspire to be relative to the Framework?



Improvement Opportunity

Current Profile
Current state of alignment between core elements and organizational requirements, risk tolerance, and resources
Where am I today relative to the Framework?

Source Reference:
https://www.youtube.com/watch?v=9BDev7sZUrI
https://www.itsmsolutions.com/

SIGURNOST CONSULTING

Tier 3 —> Tier 4

The progression from Tier 3 to Tier 4 can be summarised as a cultural change from being reactive to proactive.

Tier 3 Repeatable

Risk Management Process

- formally approved and expressed as policy
- cybersecurity practices are updated based on the application of risk management process to changes in business requirements and a changing threat/technology landscape.

Integrated Risk Management Program

- organization-wide approach to manage cybersecurity risk
- risk-informed policies
- process are defined, implemented, and reviewed
- cybersecurity and non-cybersecurity executives regularly communicate about cybersecurity risks

External Participation

- organization regularly collaborates and receives information from outside entities
- organization generates and shares information of their own with outside entities
- organization is aware of cyber risks in their supply chain and formally acts against those risks including written agreements communicating baseline requirements, governance structures, and policy implementation/monitoring

Tier 4 Adaptive

Risk Management Process

- continuous improvement incorporating advanced technology and best practices
- actively adapted based on past and present cybersecurity activities including lessons learned and predictive indicators
- responds to sophisticated changing threat landscape in a timely and effective way

Integrated Risk Management Program

- organization-wide approach to management of cybersecurity risks
- risk-informed policies
- processes and procedures in place to to address potential cybersecurity events
- senior executives treat cyber risk the same as financial risk
- cybersecurity risk management is part of organisational culture

External Participation

- organization receives, generates, and reviews, information for continuous analysis of its risks in an evolving technological and threat landscape
- organization shares this information internally and externally
- organization understands cyber risks in supply chain and uses real-time information to understand and consistently act against those risks
- proactively communicates formally and informally to create and maintain strong supply chain relationships

https://blog.twinstate.com/cybersecurity/nist/cybersecurity-framework-tiers

x

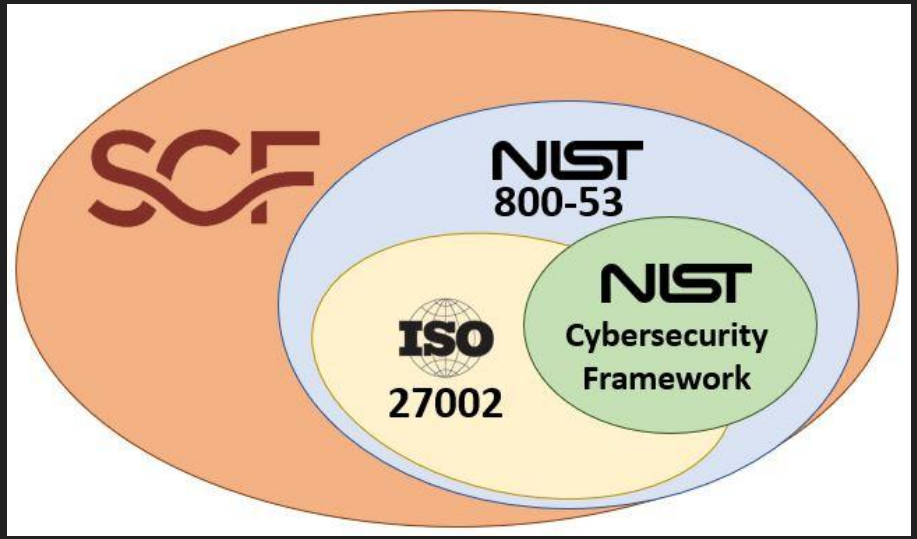
Conclusion

Opportunity for Improvement

- Rolls Royce Singapore complies with NIST, and is ISO-27001 certified.
- Despite this the SOC manager has determined that the organisation operates at a NIST Tier 3 level - Repeatable.
- This is inadequate for a leading global technology company.
- Rolls Royce Singapore needs to perform an holistic review and raise it's NIST operating level to Tier 4 - Adaptive.

Observe Reflect Make

NIST Cybersecurity Framework, IS0-27002, NIST 800-53



Our presentation will focus mainly on mapping our solutions to NIST CSF.

Rolls Royce is ISO-27001 certified, a subset of the larger ISO-27002. ISO 27002 is essentially a subset of NIST 800-53 where the fourteen (14) sections of ISO 27002 security controls fit within the twenty (20) families of NIST 800-53 rev5 security controls.

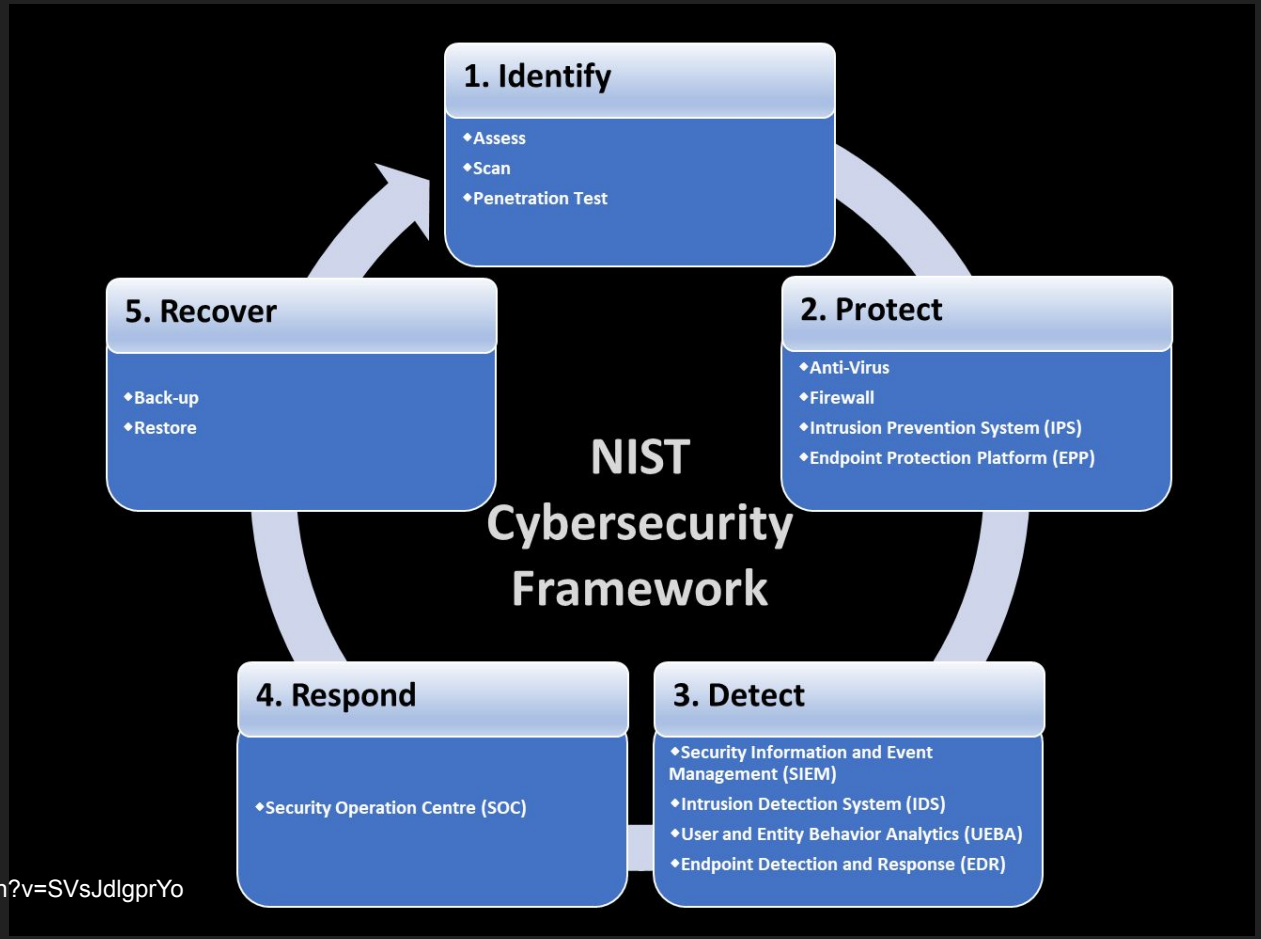
The NIST CSF is a subset of NIST 800-53 and also shares controls found in ISO 27002.

The NIST CSF takes parts of ISO 27002 and parts of NIST 800-53, but is not inclusive of both.

That makes the NIST CSF a decent choice for smaller companies that need a set of "best practices" to align with, where ISO 27002 and NIST 800-53 are the “heavy hitters” for larger companies or those that have unique compliance requirements.

The NIST CSF is often used as a reporting tool to report security to executive leadership, since the five high-level categories of Identify, Detect, Protect, Respond & Recover make it easier to report complex topics under this perspective.

NIST Cybersecurity Framework



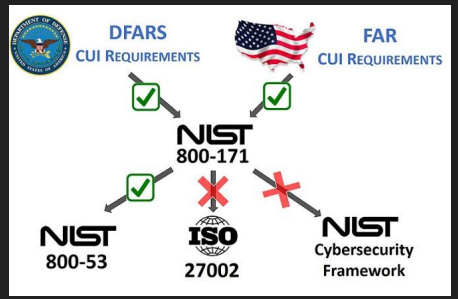
Source Reference:
https://www.youtube.com/watch?v=SVsJdlgprYo
https://www.netsurion.com/

PROPOSED SOLUTION FRAMEWORK

IDENTIFY *a cyber resilience plan*

TOOLS & TECHNOLOGY	Objectives
Below are some of the services that Sigurnost Consulting will be providing Rolls Royce in the near term, and as we achieve our milestones in the mid- and long-term,, more services will be offered : • Cyber Resilience Assessment (ID.BE, ID.BE-4, ID.BE-5, ID.AM-1, ID.AM-2, ID.AM-4, ID.AM-5, ID.AM-6, ID.SC) • Offensive security services - hacking anything to secure anything : - penetration testing, vulnerability management and adversary simulation which can help identify, prioritize and remediate security flaws covering the entire digital and physical ecosystem (ID.RA1, PR.IP-12) Zero Trust Security Assessment (ID.RM-1, ID,RM-2, ID.RM-3) DevSecOps Assessment (ID.AM-2, ID.AM-3, ID.BE-5, ID.RA-2, ID.RA-3, ID.SC-2) ** Identifiers indicate mapping to NIST CSF for activities in the near term.*	In light of the spearfishing/ data exfiltration occurrence, and for planning the future, assess the existing Zero Trust and Cyber Resilience strategies and architecture. Together with the other NIST Core functions, achieve complete NIST Tier 4 Adaptive maturity level • Risk Management Process • Integrated Risk Management Program • External Participation

IDENTIFY *a cyber resilience plan*

	TASKS & ACTIVITIES Related to Defense (referenced from NIST Special Publication 800-171 Revision 2 for entries that can be mapped to NIST CSF Framework)
Due to the sensitivity of some information in Rolls Royce pertaining to the Defense sector, this Identify section is also referencing NIST SP 800-171, a NIST Special Publication that provides recommended requirements for protecting the confidentiality of Controlled Unclassified Information (CUI). Defense contractors must implement the recommended requirements contained in NIST SP 800-171 to demonstrate their provision of adequate security to protect the covered defense information included in their defense contracts, as required by DFARS clause 252.204-7012. If a manufacturer is part of a Department Of Defense (DOD), General Services Administration (GSA), NASA or other federal or state agencies' supply chain, the implementation of the security requirements included in NIST SP 800-171 is a must. 	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. (ID.AM-1, ID.AM-2) Control the flow of CUI in accordance with approved authorizations. (ID-AM-3) Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems. (ID.AM-3) Verify and control/limit connections to and use of external systems. (ID.AM-4) Limit use of organizational portable storage devices on external systems. (ID.AM-4) Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI. (ID.RA-1, ID-RA-3, ID-RA4, ID-RA5) Periodically assess the security controls in organizational systems to determine if the controls are effective in their application. (ID.RA-1)

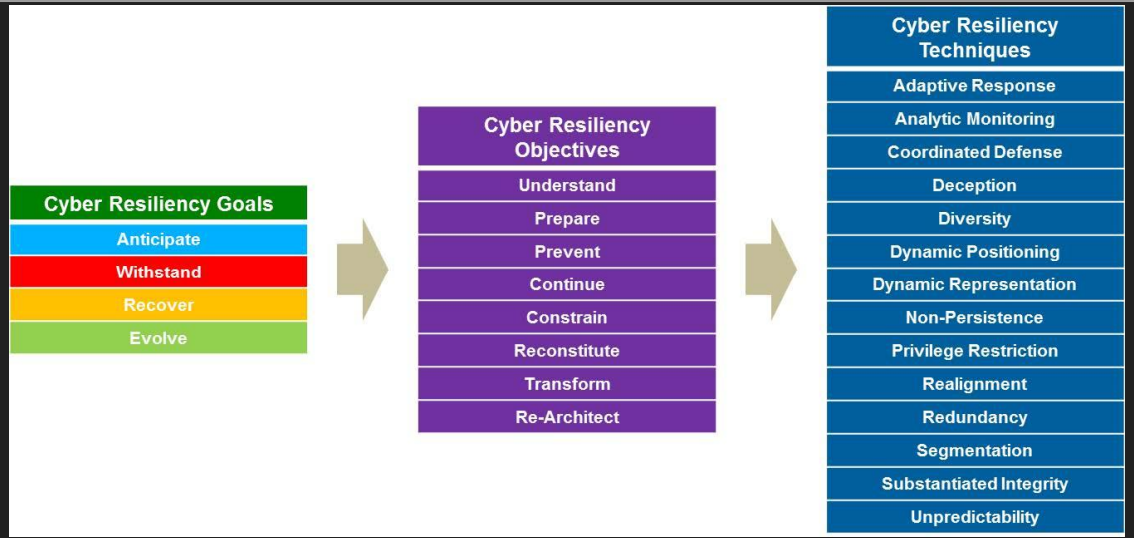
Mitre Cyber Resiliency Assessment Framework

(ID.BE, ID.BE-4, ID.BE-5, ID.AM-1, ID.AM-2, ID.AM-4, ID.AM-5, ID.AM-6, ID.SC)

The Mitre Cyber Resiliency Assessment Framework is one of the tools our consulting company can employ, as well as the Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Assessment tool. Once again, one objective is for Rolls Royce to achieve a complete NIST CSF Tier 4 level.

This framework will allow us to identify where, how, and when cyber resiliency techniques can be applied to improve architectural resiliency against advanced cyber threats.

Below is a high-level overview of the Mitre framework, broken down into Goals, Objectives, and Techniques. Within the framework are more detailed tables. For example, the objectives Understand and Continue are shown to be mapped to Adaptive Response, Privilege Restriction, and so on.

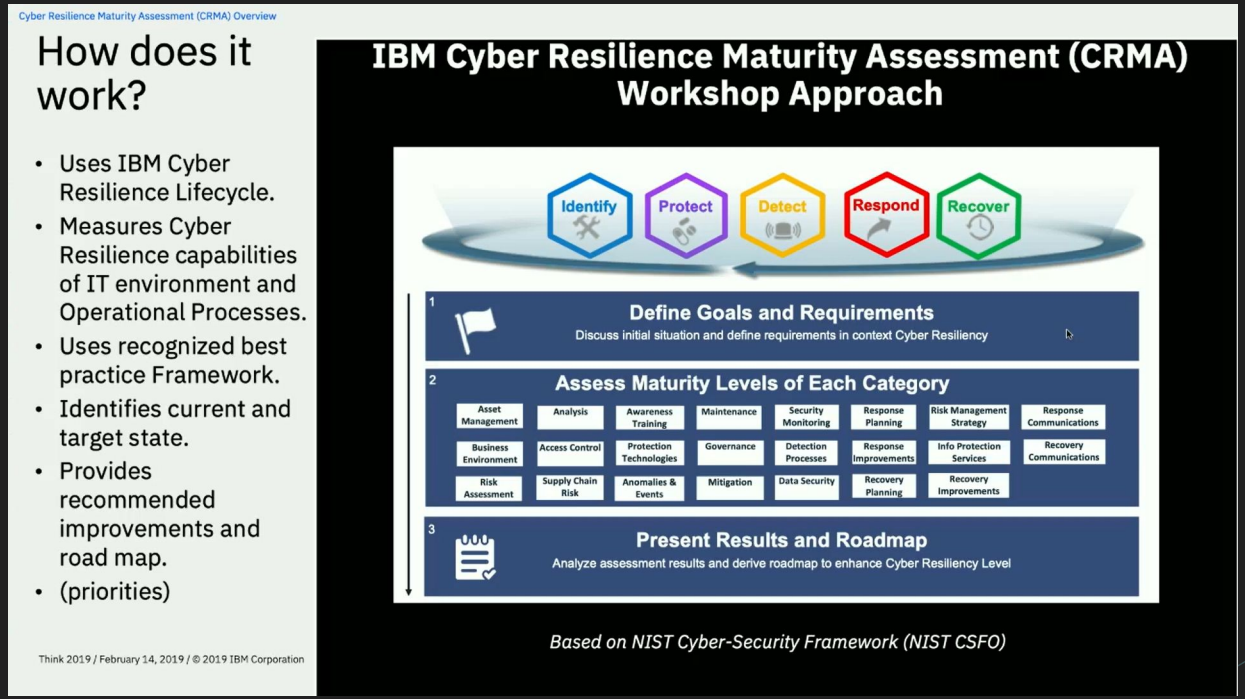


Representative Examples of Cyber Resiliency Mechanisms :

TECHNIQUE	Near-Term
Deception: Use obfuscation and misdirection (e.g., disinformation) to confuse an adversary (under objectives : Understand, Prevent)	• Encryption of mission data • Honeypots (low interaction, based on commonly used attacker requested services) • Encryption of security control information
Unpredictability: Make changes frequently and randomly, not just in response to actions by the adversary (under objectives : Prevent, Continue)	• Random change of crypto keys • Randomize communications patterns (e.g., frequency-hopping) • Randomization of session IDs • Centralized, automated frequent randomization of admin passwords

IBM Cyber Resilience Maturity Assessment (CRMA)

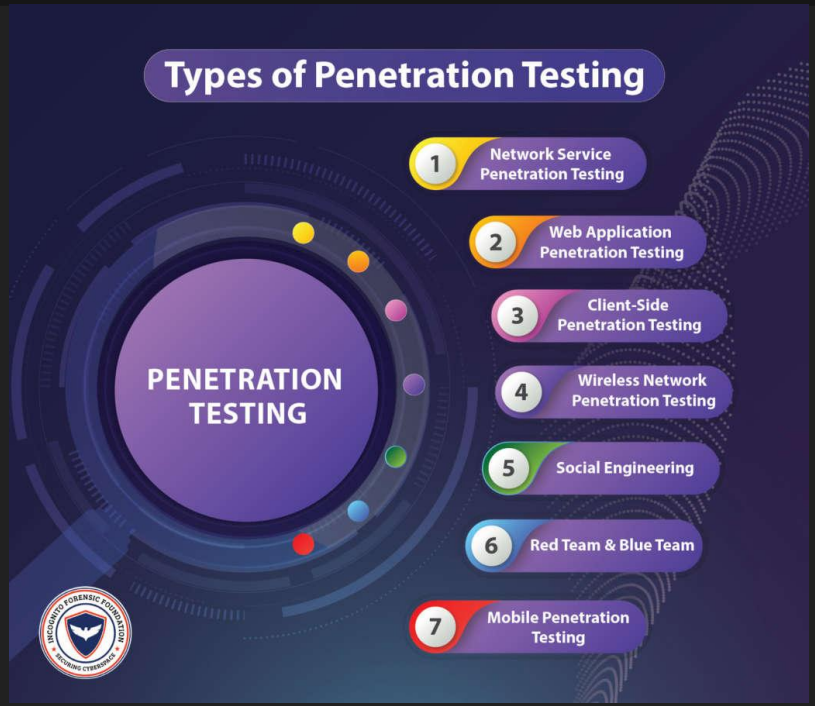
Just for illustration, IBM also offers a similar consulting service, the IBM Cyber Resilience Maturity Assessment (CRAM). If we look at the high-level diagram below, it is a familiar sight, providing recommended improvements and road map mapped to the NIST CSF core functions.



Penetration Testing

(ID.RA1, PR.IP-12)

No matter how ingenious or innovative security experts get, hackers have always been a step ahead. Along with the latest tools for protection, it is paramount that Rolls Royce conduct routine penetration testing to find and fix any weaknesses in their systems. This activity meets the Tier 4 NIST CSF criteria of proactively detecting threats and predicting issues based on current trends and their IT architecture.



Penetration Testing

(ID.RA1, PR.IP-12)

Network Service Penetration Testing

- **Firewall configuration testing**
- **Firewall bypass testing**
- **DNS attacks**
- **IPS deception**

Web Application Penetration Testing

Testing of all web applications like browsers, plugins in addition to downloads, and so on. In addition to exposing vulnerabilities, a web application penetration test also creates awareness about bad browsing habits and helps to establish protocols against jeopardizing practices.

Client-Side Penetration Testing

The object of this type of penetration test is to find out if there are any vulnerabilities in a particular employee's computer or that of a client.

Wireless Network Penetration Testing

Wireless network penetration testing extends to laptops, smartphones, tablets, etc. It highlights which devices pose security risks and enable hackers to gain entry into company servers. An important aspect of wireless network tests is to assess the protocols used to configure the wireless network at a client's location.

Social Engineering Tests

A major aspect of cybersecurity is the human aspect. While various penetration tests can fortify the digital infrastructure, dedicated hackers can obtain vital information such as login credentials from unsuspecting employees through other illegal means.

Here are a just a sample of tools Sigurnost Consulting can use for PenTests

Netsparker Build Your Resistance to Threats

NETSPARKER - identify vulnerabilities such as SQL Injection and Cross-site Scripting in web applications and web APIs.

Acunetix

ACUNETIX - detects and reports on over 4500 web application vulnerabilities including all variants of SQL Injection and XSS. It supports HTML5, JavaScript, and Single-page applications as well as CMS systems.

hackerone

HACKERONE - Find and fix critical vulnerabilities. Uses communication tools like Slack, integrates with GitHub and Jira. One will be able to achieve compliance standards like SOC2, ISO, PCI, HITRUST, etc. Partners of HackerOne include the U.S. Department of Defense, Google, CERT Coordination Center, etc. and found over 120,000 vulnerabilities and awarded over $80M in bug bounties.

Penetration Testing

(ID.RA1, PR.IP-12)

Red Team and Blue Team

As an organization grows, a single penetration tester cannot assess its cybersecurity measures. The most efficient way to test the effectiveness of existing security is to organize two teams consisting of testers and employees and simulate an actual cyberattack.

The Red Team emulates a group of hackers bent on breaching the systems and stealing sensitive data, while the Blue Team emulates a team of IT security professionals. The goal of the Red Team is to use any and every means necessary of exploiting vulnerabilities and that of the Blue Team is to defend against all sorts of attacks.

Such a type of penetration test is imperative for Rolls Royce to strengthen resiliency against cyberattacks and ensure effective security. It highlights all the methods used by hackers and creates awareness among security professionals about how to respond to real scenarios.

Mobile Penetration Testing

A wide array of tools can be used to try and hack into a client's smartphone. This not only exposes vulnerabilities, but also creates awareness for the user about pertinent issues in mobile security.

breachlock

RATA Web Application Vulnerability Scanner - first Artificial Intelligence, Cloud and Human Hacker powered automated web vulnerability scanner. Integrates into CI/CD tools like Jenkins, JIRA, Slack, and Trello.

metasploit

METASPLOIT - based on the concept of "exploit," which is a code that can surpass the security measures and enter a certain system. If entered, it runs a 'payload', a code that performs operations on a target machine, thus creating a perfect framework for penetration testing.

SOCIAL-ENGINEER TOOLKIT - attacks are targeted at the human element rather than on the system element. It has features that let you send emails, java applets, etc. containing the attack code. It goes without saying that this tool is to be used very carefully and only for white-hat reasons.

WIRESHARK

WIRESHARK - a network protocol analyzer –popular for providing the minutest details about your network protocols, packet information, decryption, etc. It can be used on Windows, Linux, OS X, Solaris, FreeBSD, NetBSD, and many other systems.

Zero Trust Security

(ID.RM-1, ID,RM-2, ID.RM-3, ID.GV-2)

The Zero Trust Network, or Zero Trust Architecture is a security strategy centered on the belief that organizations should not automatically trust anything *inside* or *outside* its perimeters and instead must verify anything and everything trying to connect to its systems before granting access.

Zero Trust draws on technologies such as :

- ❏ multifactor authentication, IAM, orchestration, analytics, encryption, scoring and file system permissions. Zero Trust also calls for governance policies such as giving users the least amount of access they need to accomplish a specific task.

Zero Trust Security is not something that organizations can implement by purchasing one solution, but rather something that is incrementally implemented with a combination of solutions and processes that are underpinned by Zero Trust principles.

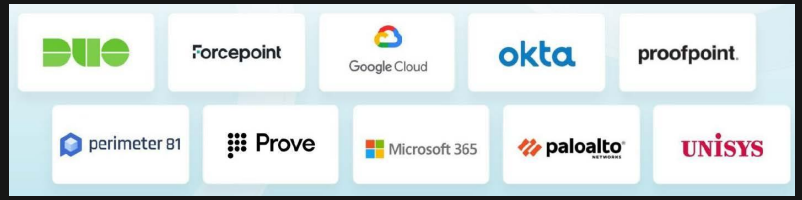
In practice, this means measures such as:

- Moving beyond the idea of inside versus outside and redesigning cyber defence in terms of secure micro-parameters, with multiple points of network defence
- Implementing the ability to control, inspect, and restrict network traffic traveling in any direction—north-south or east-west—within your organisation
- Subjecting users to checks and balances, each time they cross into a different area of the network or try to access a new set of resources, to verify their needs and privileges
- Preventing excess privileges from accumulating by periodically revoking and refreshing access and credentials
- Continuously monitoring who's accessing what and the level of risk these activities might present

Zero Trust implementation requires more than simply plugging in a new box. Rather, it represents a new way of thinking about cybersecurity, embodied in evolving approaches to management, automation, auditability, resiliency, and integration.

Below are some third-party solutions that Sigurnost Consulting can propose.

More detail on some solutions' features will be discussed in the Protect section - like Duo, Proofpoint, paloalto



PROTECT

PROPOSED SOLUTION FRAMEWORK

against attacks by discovering vulnerabilities before they are exploited

SIGUNNOST CONSULTING

TOOLS & TECHNOLOGY - Categories & Identifiers

- Identity Management, Authentication and Access Control (PR.AC)
- Awareness and Training (PR.AT)
- Data Security (PR.DS)
- Information Protection Processes and Procedures (PR.IP)
- Maintenance (PR.MA)
- Protective Technology (PR.PT)

SUMMARY OUTCOME RESULTS from TASKS & ACTIVITIES

Reference: U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency - CYBER RESILIENCE REVIEW (CRR) CRR: NIST Cybersecurity Framework Crosswalks (cisa.gov)

- DevSecOps Methodology for all In-House and Outsourced Software Applications Development Projects : **NIST Framework - Secure Software Development Framework (SSDF)**
- Next Gen Firewall & Zero Trust Network Platform plus Network Segmentation : **Palo Alto Networks®**
- Intrusion Protection System (IPS) : **Darktrace Antigena®**
- EndPoint Protection Platform: **CrowdStrike Falcon®**
- Enterprise Email Security Platform: **Proofpoint®**
- Enterprise DDoS Protection Platform : **Cloudflare®**
- Multi-Factor Authentication: **DUO® multi-factor authentication addon for Palo Alto Networks®**
- Enterprise Security Awareness Computer-Based Training Solution : **NINJIO®**
- Enterprise Data Loss Protection & Encryption: **McAfee Total Protection for DLP® & McAfee Drive Encryption®**
- Enterprise Knowledge Management: **IBM Watson Discovery®**

Product Walk-Through

1.Asset Management

The purpose of Asset Management is to identify, document, and manage assets during their life cycle to ensure sustained productivity to support critical services.

Goal - The relationship between assets and the services they support is established.

- Confidentiality, integrity, and availability requirements are established for each service related asset under facilities (PR.IP-5).

Goal - Access to assets is managed.

- Multi-factor 2FA authentication - Access (including identities and credentials) requests are reviewed and approved by the asset owner and granted based on their protection requirements (PR.AC-1, PR.AC-2, PR.AC-3, PR.AC-6, PR.AC-7).
- Access privileges are reviewed to identify excessive or inappropriate privileges and modified as a result of reviews (PR.AC-1).
- Access permissions are managed Incorporating the principle of least privilege and separation of duties (PR.AC-4).
- Identities (e.g. user accounts) are proofed before they are bound to credentials that are asserted in interactions (PR.AC-6).

Goal - Information assets are categorized and managed to ensure the sustainment and protection of the critical service.

- Information assets are categorized based on sensitivity and potential impact to the critical service (such as public, internal use only, secret) (PR.DS).
- The categorization of information assets are monitored and enforced (PR.DS).
- Policies and procedures are present for the proper labeling and handling of information assets (PR.DS).
- All staff members who handle information assets (including those who are external to the organization, such as contractors) are trained in the use of information categories (PR.AT-1).
- High-value information assets are backed-up and retained (PR.IP-4).
- Guidelines exist for properly disposing of information assets (PR.DS-3, PR.IP-6).
- Adherence to information asset disposal guidelines is monitored and enforced (PR.DS-3, PR.IP-6).

Goal - Facility assets supporting the critical service are prioritized and managed.

- Protection and sustainment requirements of the critical service are considered during the selection of facilities (PR.IP-5).

MIL4-Measured

- Asset management activities are periodically reviewed and measured to ensure they are effective and producing intended results (PR.IP-7).
- Asset management activities are periodically reviewed to ensure they are adhering to the plan (PR.IP-7).
- Higher-level management is aware of issues related to the performance of asset management (PR.IP-8).

MIL5-Defined

- The organization has adopted a standard definition of asset management activities from which operating units can derive practices that fit their unique operating circumstances (PR.IP).
- Improvements to asset management activities are documented and shared across the organization (PR.IP).

Next

PROTECT

PROPOSED SOLUTION FRAMEWORK

against attacks by discovering vulnerabilities before they are exploited

SIGURNOST CONSULTING

TOOLS & TECHNOLOGY - Categories & Identifiers

- Identity Management, Authentication and Access Control (PR.AC)
- Awareness and Training (PR.AT)
- Data Security (PR.DS)
- Information Protection Processes and Procedures (PR.IP)
- Maintenance (PR.MA)
- Protective Technology (PR.PT)

SUMMARY OUTCOME RESULTS from TASKS & ACTIVITIES

Reference: U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency - CYBER RESILIENCE REVIEW (CRR) CRR: NIST Cybersecurity Framework Crosswalks (cisa.gov)

2.Controls Management

The purpose of Controls Management is to identify, analyze, and manage controls in a critical service's operating environment.

Goal - Control objectives are established.

- Control objectives have been established for assets required for delivery of the critical service (PR.AC, PR.DS, PR.IP, PR.MA, PR.PT).
- Control objectives are prioritized according to their potential to affect the critical service (PR.AC, PR.DS, PR.IP, PR.MA, PR.PT).

Goal - Controls are implemented.

- Controls have been implemented to achieve the control objectives established for the critical service (PR.AC,PR.DS,PR.IP, PR.MA,PR.PT).
- Controls have been implemented, incorporating network segregation where appropriate, to protect network integrity (PR.AC-5).
- Controls have been implemented to protect data-at-rest (PR.DS-1).
- Controls have been implemented to protect data-in-transit (PR.DS-2).
- Controls have been implemented to protect against data leaks (PR.DS-5).
- Audit/log records have been determined, documented, implemented, and reviewed in accordance with policy (PR.PT-1).
- Controls have been implemented to protect and restrict the use of removable media in accordance with policy [PR.PT-2].
- Controls have been implemented to protect communication and control networks (PR.PT-4).
- Cybersecurity human resource practices have been implemented for the critical service (e.g., de-provisioning, personnel screening) (PR.IP-11).
- Access to systems and assets is controlled by incorporating the principle of least functionality (e.g., whitelisting, blacklisting, etc.) (PR.PT-3).

Goal - Control designs are analyzed to ensure they satisfy control objective.

- Control designs are analyzed to identify gaps where control objectives are not adequately satisfied (PR.IP-7).
- As a result of the controls analysis, new controls are introduced or existing controls modified to address gaps (PR.IP-7).

Goal - The internal control system is assessed to ensure control objectives are met.

- The performance of controls is assessed on a scheduled basis to verify they continue to meet control objectives (PR.IP-7).
- As a result of scheduled assessments, new controls are introduced or existing controls modified to address problem areas (PR.IP-7).

MIL4-Measured

- Controls management activities are periodically reviewed and measured to ensure they are effective and producing intended results(PR.IP-7).
- Controls management activities are periodically reviewed to ensure they are adhering to the plan (PR.IP-7).
- Higher-level management is aware of issues related to the performance of controls management (PR.IP-8).

MIL5-Defined

- The organization has adopted a standard definition of controls management activities from which operating units can derive practices that fit their unique operating circumstances (PR.IP).
- Improvements to controls management are documented and shared across the organization (PR.IP).

Next

PROTECT

PROPOSED SOLUTION FRAMEWORK

against attacks by discovering vulnerabilities before they are exploited

SIGURNOST CONSULTING

TOOLS & TECHNOLOGY - Categories & Identifiers

- Identity Management, Authentication and Access Control (PR.AC)
- Awareness and Training (PR.AT)
- Data Security (PR.DS)
- Information Protection Processes and Procedures (PR.IP)
- Maintenance (PR.MA)
- Protective Technology (PR.PT)

SUMMARY OUTCOME RESULTS from TASKS & ACTIVITIES

Reference: U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency - CYBER RESILIENCE REVIEW (CRR) CRR: NIST Cybersecurity Framework Crosswalks (cisa.gov)

3.Configuration and Change Management

The purpose of Configuration and Change Management is to establish processes to ensure the integrity of assets using change control and change control audits.

Goal -The life cycle of assets is managed.

- A change management process is used to manage modifications to assets (PR.IP-3).
- Resilience requirements are evaluated as a result of changes to assets [PR.IP-3).
- Capacity management and planning is performed for assets (PR.DS-4).
- Change requests are tracked to closure (PR.IP-3).
- Stakeholders are notified when they are affected by changes to assets (PR.IP-3).
- A System Development Life Cycle is implemented to manage systems supporting the critical service (PR.IP-2).

Goal - The integrity of technology and information assets is managed.

- Configuration management is performed for technology assets (PR.IP-1).
- Techniques are in use to detect changes to technology assets (PR.DS-6, PR.DS-8).
- Modifications to technology assets are reviewed (PR.IP-1, PR.IP-3).
- Integrity requirements are used to determine which staff members are authorized to modify information assets (PR.AC-4, PR.IP-3, PR.IP-11).
- The integrity of information assets is monitored (PR.DS-6).
- Unauthorized or unexplained modifications to technology assets are addressed (PR.IP-3).
- Modifications to technology assets are tested before being committed to production systems (PR.DS-7).
- A process for managing access to technology assets has been implemented (PR.AC).
- The maintenance and repair of assets is performed and logged in a timely manner (PR.MA-1).
- The maintenance and repair of assets is performed with approved and controlled tools and/or methods (PR.MA-1).
- The remote maintenance and repair of assets is approved, logged, and performed in a manner that prevents unauthorized access (PR.MA-2).

Goal - Asset configuration baselines are established.

- Determine Technology assets configuration baselines (PR.IP-1).
- Approval is obtained for proposed changes to baselines (PR.IP-1, PR.IP-3).

MIL4-Measured

- Change management activities are periodically reviewed and measured to ensure they are effective and producing intended results (PR.IP-7).
- Change management activities are periodically reviewed to ensure they are adhering to the plan (PR.IP-7).
- Higher-level management is aware of issues related to the performance of change management (PR.IP-8).

MIL5-Defined

- The organization has adopted a standard definition of change management activities from which operating units can derive practices that fit their unique operating circumstances (PR.IP).
- Improvements to change management are documented and shared across the organization (PR.IP).

Next

PROTECT

PROPOSED SOLUTION FRAMEWORK

against attacks by discovering vulnerabilities before they are exploited

SIGURNOST CONSULTING

TOOLS & TECHNOLOGY - Categories & Identifiers

- **Identity Management, Authentication and Access Control (PR.AC)**
- **Awareness and Training (PR.AT)**
- **Data Security (PR.DS)**
- **Information Protection Processes and Procedures (PR.IP)**
- **Maintenance (PR.MA)**
- **Protective Technology (PR.PT)**

SUMMARY OUTCOME RESULTS from TASKS & ACTIVITIES

Reference: U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency - CYBER RESILIENCE REVIEW (CRR) CRR: NIST Cybersecurity Framework Crosswalks (cisa.gov)

4.Vulnerability Management

The purpose of Vulnerability Management is to identify, analyze, and manage vulnerabilities in a critical service's operating environment.

Goal - Preparation for vulnerability analysis and resolution activities is conducted.

- A vulnerability analysis and resolution strategy has been developed (PR.IP-12).

Goal - A process for identifying and analyzing vulnerabilities is established and maintained.

- The information from these sources is kept current (PR.IP-7).

Goal - Exposure to identified vulnerabilities is managed.

- The effectiveness of vulnerability mitigation is reviewed (PR.IP-7).

Goal - The root causes of vulnerabilities are addressed

- Underlying causes for vulnerabilities are identified (through root-cause analysis or other means) and addressed (PR.IP-12).

MIL4-Measured

- Vulnerability management activities are periodically reviewed and measured to ensure they are effective and producing intended results (PR.IP-7).
- Vulnerability management activities are periodically reviewed to ensure they are adhering to the plan (PR.IP-7).
- Higher-level management is aware of issues related to the performance of vulnerability management (PR.IP-8).

MIL5-Defined

- The organization has adopted a standard definition of vulnerability management activities from which operating units can derive practices that fit their unique operating circumstances (PR.IP).
- Improvements to vulnerability management activities are documented and shared across the organization (PR.IP).

Next

PROTECT

PROPOSED SOLUTION FRAMEWORK

against attacks by discovering vulnerabilities before they are exploited

SIGURNOST CONSULTING

TOOLS & TECHNOLOGY - Categories & Identifiers	**SUMMARY OUTCOME RESULTS from TASKS & ACTIVITIES**
• Identity Management, Authentication and Access Control (PR.AC) • Awareness and Training (PR.AT) • Data Security (PR.DS) • Information Protection Processes and Procedures (PR.IP) • Maintenance (PR.MA) • Protective Technology (PR.PT)	**Reference: U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency - CYBER RESILIENCE REVIEW (CRR)** CRR: NIST Cybersecurity Framework Crosswalks (cisa.gov)
	5.Incident Management The purpose of Incident Management is to establish processes to identify and analyze events, detect incidents, and determine an organizational response. Goal - A process for identifying, analyzing, responding to, and learning from incidents is established. ● Determine the organization has a plan for managing incidents (PR.IP-9). ● The incident management plan is reviewed and updated (PR.IP-10). ● The roles and responsibilities are in the plan included in job descriptions (PR.IP-11). Goal - Post-incident lessons learned are translated into improvement strategies. ● Analysis is performed to determine the root causes of incidents (PR.IP-7). ● A link between the incident management process and other related processes (problem management, risk management, change management, etc.) is examined (PR.IP-7). ● Lessons learned from incident management are used to improve asset protection and service continuity strategies (PR.IP-7). MIL4-Measured ● Incident management activities are periodically reviewed and measured to ensure they are effective and producing intended results (PR.IP-7). ● Incident management activities are periodically reviewed to ensure they are adhering to the plan (PR.IP-7). ● Higher-level management is aware of issues related to the performance of incident management (PR.IP-8). MIL5-Defined ● The organization has adopted a standard definition of incident management activities from which operating units can derive practices that fit their unique operating circumstances (PR.IP). ● Improvements to incident management activities are documented and shared across the organization (PR.IP).

Next

PROTECT

PROPOSED SOLUTION FRAMEWORK

against attacks by discovering vulnerabilities before they are exploited

SIGURNOST CONSULTING

TOOLS & TECHNOLOGY - Categories & Identifiers

- Identity Management, Authentication and Access Control (PR.AC)
- Awareness and Training (PR.AT)
- Data Security (PR.DS)
- Information Protection Processes and Procedures (PR.IP)
- Maintenance (PR.MA)
- Protective Technology (PR.PT)

SUMMARY OUTCOME RESULTS from TASKS & ACTIVITIES

Reference: U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency - CYBER RESILIENCE REVIEW (CRR) CRR: NIST Cybersecurity Framework Crosswalks (cisa.gov)

6.Service Continuity Management

The purpose of Service Continuity Management is to ensure the continuity of essential operations of services and their associated assets if a disruption occurs as a result of an incident, disaster, or other disruptive event.

Goal - Service continuity plans for high-value services are developed.

- Service continuity plans are developed and documented for assets required for delivery of the critical service (PR.IP-9).
- Service continuity plans are developed using established standards, guidelines, and templates (PR.IP-9).
- Staff members are assigned to execute specific service continuity plans (PR.IP-9).
- Key contacts are identified in the service continuity plans (PR.IP-9).
- Service continuity plans are stored in a controlled manner and available to all those who need to know (PR.IP-9).
- Availability requirements such as recovery time objectives and recovery point objectives are established (PR.IP-9).
- Mechanisms (e.g., failsafe, load balancing, hot swap capabilities) are implemented to achieve resilience requirements in normal and adverse situations (PR.PT-5).

Goal - Service continuity plans are reviewed to resolve conflicts between plans.

- Plans are reviewed to identify and resolve conflicts (PR.IP-9)

Goal - Service continuity plans are tested to ensure they meet their stated objectives.

- Standards for testing service continuity plans been are implemented (PR.IP-10).
- A schedule for testing service continuity plans has been established (PR.IP-10).
- Service continuity plans are tested (PR.IP-10).
- Backup and storage procedures for high-value information assets are tested (PR.IP-4).
- Test results are compared with test objectives to identify needed improvements to service continuity plans (PR.IP-10).

Goal - Service continuity plans are executed and reviewed.

- Conditions have been identified that trigger the execution of the service continuity plan (PR.IP-9).
- Execution of service continuity plans is reviewed (PR.IP-9).
- Improvements are identified as a result of executing service continuity plans (PR.IP-7).

MIL4-Measured

- Service continuity activities are periodically reviewed and measured to ensure they are effective and producing intended results (PR.IP-7).
- Service continuity activities are periodically reviewed to ensure they are adhering to the plan (PR.IP-7).
- Higher-level management is aware of issues related to the performance of service continuity (PR.IP-8).

MIL5-Defined

- The organization has adopted a standard definition of service continuity activities from which operating units can derive practices that fit their unique operating circumstances (PR.IP).
- Improvements to service continuity are documented and shared across the organization (PR.IP).

Next

PROTECT

PROPOSED SOLUTION FRAMEWORK

against attacks by discovering vulnerabilities before they are exploited

SIGURNOST CONSULTING

TOOLS & TECHNOLOGY - Categories & Identifiers

- Identity Management, Authentication and Access Control (PR.AC)
- Awareness and Training (PR.AT)
- Data Security (PR.DS)
- Information Protection Processes and Procedures (PR.IP)
- Maintenance (PR.MA)
- Protective Technology (PR.PT)

SUMMARY OUTCOME RESULTS from TASKS & ACTIVITIES

Reference: U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency - CYBER RESILIENCE REVIEW (CRR) CRR: NIST Cybersecurity Framework Crosswalks (cisa.gov)

7.Risk Management

The purpose of Risk Management is to identify, analyze, and mitigate risks to critical service assets that could adversely affect the operation and delivery of services.

Goal - Risks to assets and services are mitigated and controlled.

MIL4-Measured

- Risk management activities are periodically reviewed and measured to ensure they are effective and producing intended results (PR.IP-7).
- Risk management activities are periodically reviewed to ensure they are adhering to the plan (PR.IP-7).
- Higher-level management is aware of issues related to the performance of risk management (PR.IP-8).

MIL5-Defined

- The organization has adopted a standard definition of risk management activities from which operating units can derive practices that fit their unique operating circumstances (PR.IP).
- Improvements to risk management are documented and shared across the organization (PR.IP).

8.External Dependencies Management

The purpose of External Dependencies Management is to establish processes to manage an appropriate level of controls to ensure the sustainment and protection of services and assets that are dependent on the actions of external entities.

Goal - Relationships with external entities formally established and maintained.

- Resilience requirements are included in formal agreements with external entities (PR.AT-3).

Goal - Dependencies on public services and infrastructure service providers are identified.

MIL4-Measured

- External dependency management activities are periodically reviewed and measured to ensure they are effective and producing intended results (PR.IP-7).
- External dependency management activities are periodically reviewed to ensure they are adhering to the plan (PR.IP-7).
- Higher-level management is aware of issues related to external dependency management (PR.IP-8).

MIL5-Defined

- The organization has adopted a standard definition of the external dependency management activities from which operating units can derive practices that fit their unique operating circumstances (PR.IP).
- Improvements to external dependency management are documented and shared across the organization (PR.IP).

Next

PROTECT

PROPOSED SOLUTION FRAMEWORK

against attacks by discovering vulnerabilities before they are exploited

SIGURNOST CONSULTING

TOOLS & TECHNOLOGY - Categories & Identifiers

- **Identity Management, Authentication and Access Control (PR.AC)**
- **Awareness and Training (PR.AT)**
- **Data Security (PR.DS)**
- **Information Protection Processes and Procedures (PR.IP)**
- **Maintenance (PR.MA)**
- **Protective Technology (PR.PT)**

SUMMARY OUTCOME RESULTS from TASKS & ACTIVITIES

Reference: U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency - CYBER RESILIENCE REVIEW (CRR) CRR: NIST Cybersecurity Framework Crosswalks (cisa.gov)

9.Training and Awareness

The purpose of Training and Awareness is to develop skills and promote awareness for people with roles that support the critical service.

Goal - Cyber security awareness and training programs are established.

- Cyber security awareness needs have been identified for the critical service (PR.AT-1).
- Required cyber security skills have been identified for specific roles (administrators, technicians, etc.) for the critical service (PR.AT-1).
- Skill gaps present in personnel responsible for cyber security are identified (PR.AT-1).
- Cyber security training needs have been identified (PR.AT-1).

Goal - Awareness and training activities are conducted.

- Cyber security awareness activities for the critical service are conducted (PR.AT-1).
- Cyber security training activities for the critical service are conducted (PR.AT-1).
- The effectiveness of the awareness and training programs is evaluated (PR.AT, PR.IP-7).
- Awareness and training activities are revised as needed (PR.AT, PR.IP-7).
- Privileged users have been trained in their specific roles and responsibilities in support of the critical service (PR.AT-2).
- Senior executives have been trained in their specific roles and responsibilities in support of the critical service (PR.AT-4).
- Physical and information security personnel have been trained in their specific roles and responsibilities in support of the critical service (PR.AT-5).

MIL4-Measured

- Training activities are periodically reviewed and measured to ensure they are effective and producing intended results (PR.IP-7).
- Training activities are periodically reviewed to ensure they are adhering to the plan (PR.IP-7).
- Higher-level management is aware of issues related to the performance of training (PR.IP-8).

MIL5-Defined

- The organization has adopted a standard definition of the training activities from which operating units can derive practices that fit their unique operating circumstances (PR.IP).
- Improvements to training are documented and shared across the organization (PR.IP).

Next

PROTECT

PROPOSED SOLUTION FRAMEWORK

against attacks by discovering vulnerabilities before they are exploited

SIGURNOST CONSULTING

TOOLS & TECHNOLOGY - Categories & Identifiers

- Identity Management, Authentication and Access Control (PR.AC)
- Awareness and Training (PR.AT)
- Data Security (PR.DS)
- Information Protection Processes and Procedures (PR.IP)
- Maintenance (PR.MA)
- Protective Technology (PR.PT)

SUMMARY OUTCOME RESULTS from TASKS & ACTIVITIES

Reference: U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency - CYBER RESILIENCE REVIEW (CRR) CRR: NIST Cybersecurity Framework Crosswalks (cisa.gov)

10.Situational Awareness

The purpose of Situational Awareness is to actively discover and analyze information related to immediate operational stability and security and to coordinate such information across the enterprise to ensure that all organizational units are performing under a common operating picture.

Goal - Threat monitoring is performed.

- Responsibility for monitoring sources of threat information has been assigned (PR.AT-5).
- Resources have been assigned and trained to perform threat monitoring (PR.AT-1, PR.AT-5).

Goal - The requirements for communicating threat information are established.

- Internal stakeholders (such as the critical service owner and incident management staff) have been identified to whom threat information must be communicated (PR.IP-8).
- External stakeholders (such as emergency management personnel, regulatory, and information sharing organizations) have been identified to whom threat information must be communicated (PR.IP-8).

Goal - Threat information is communicated.

- Threat information is communicated to stakeholders (PR.IP-8).
- Resources have been assigned authority and accountability for communicating threat information (PR.AT-5).
- Resources have been trained with respect to their specific role in communicating threat information (PR.AT-1, PR.AT-5).

MIL4-Measured

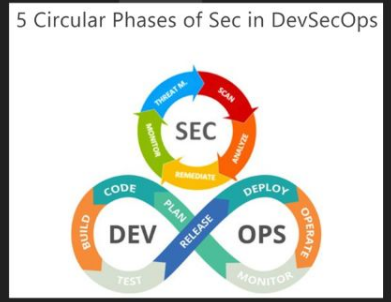
- Situational awareness activities are periodically reviewed and measured to ensure they are effective and producing intended results (PR.IP-7).
- Situational awareness activities are periodically reviewed to ensure they are adhering to the plan (PR.IP-7).
- Higher-level management is aware of issues related to situational awareness (PR.IP-8).

MIL5-Defined

- The organization has adopted a standard definition of the situational awareness activities from which operating units can derive practices that fit their unique operating circumstances (PR.IP).
- Improvements to situational awareness activities are documented and shared across the organization (PR.IP).

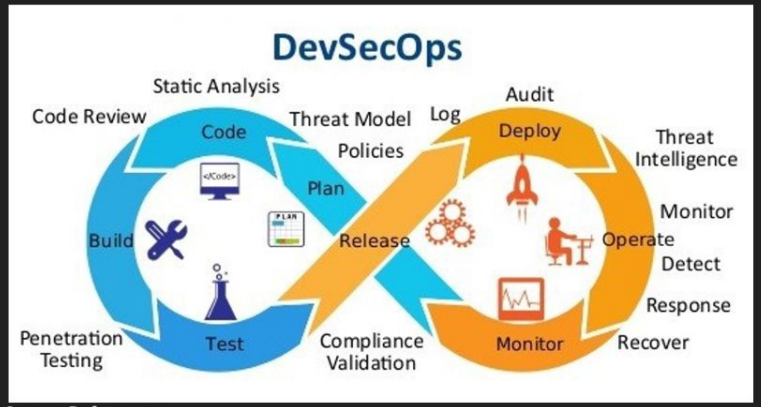
Back

NIST Computer Security Resource Center (CSRC) DevSecOps
Proposed Cybersecurity Measures to counter 'Exploit Aged Hardware/Software'
Adoption of NIST Framework: Secure Software Development Framework (SSDF)



Tools and people can change over time but the culture Enterprise creates through processes and metrics determines the sustainability of DevSecOps. From ground up integrate Security into entire DevOps through 5 continuous circular phases:

- Threat Modeling
- Scan
- Analyze
- Remediate
- Monitor



Source Reference:
https://www.devopsschool.com/blog/what-is-devsecops-benefits-of-adopting-devsecops/
https://kondukto.io/5-circular-phases-of-sec-in-devsecops/
https://csrc.nist.gov/Projects/devsecops/resources

Advantage of DevSecOps

- Reduces vulnerabilities present on application code.
- Reduces vulnerabilities present on IaC[1] technologies.
- Reduces the number of ways to exploit application
- Improves application stability, availability and security.
- Secure by Design and the ability to measure.
- Faster Speed of recovery in the case of a security incident.
- Focus on the application's security from the beginning.
- Leverage open-source with increased confidence
- Improving Overall Security by enabling Immutable infrastructure which further involves security automation.

Successful ways to adopt DevSecOps

- Automate the process as much as possible.
- Follow the DevOps methodology.
- Write to code securely.
- Evaluation of current security measures and concluding what to do to overcome problems.
- Integrate the security to DevSecOps.
- Helps to adopt DevSecOps right tools.
- Monitoring Continuous Integration and Continuous Delivery.
- Analyze code and do a vulnerability assessment.
- Mandatory security at every stage.

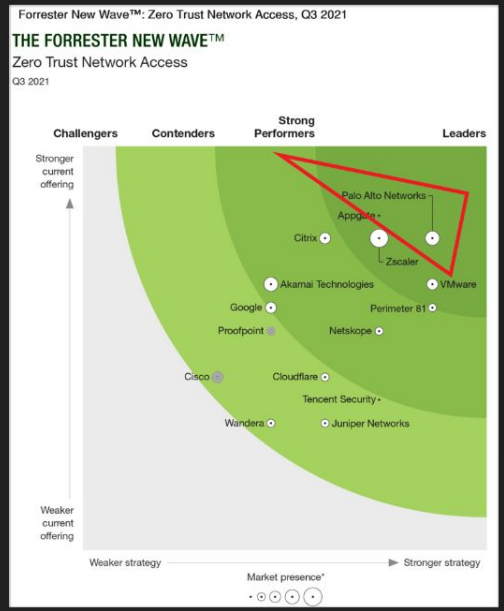
[1] : Infrastructure as Code (IaC) is the management of infrastructure (networks, virtual machines, load balancers, and connection topology) in a descriptive model, using the same versioning as DevOps team uses for source code. IaC is a key DevOps practice and is used in conjunction with continuous delivery.

NIST CSF Core Protect : Firewall (FW) & Zero Trust Network (ZTN) Access

Proposed Cybersecurity Measures to counter 'Known & Unknown Cybersecurity Threats'

Palo Alto Networks® ML-powered Next-Gen Firewall & Zero Trust Network Platform Overview

- Palo Alto Networks® Named a Leader in the 2020 Gartner Magic Quadrant for Network Firewalls Protection Platform positioned highest in execution and furthest in vision, in their 2020 report.
- Palo Alto Networks Prisma® Access is Named a Leader in Zero Trust Network Access (ZTNA) in the Forrester New Wave Q3 2021 Report. Built-in support for authenticating and authorizing third parties is superior to other ZTNA solutions. Built for securing the non-web applications that are so common in complex on-prem environments.
- Palo Alto Networks® produced world's first ML-powered Next-Gen Firewall to stay two steps ahead of new emerging threats, see and secure Enterprises faster with less manual errors including IoT.
- Palo Alto Networks® firewalls offer strong granular application controls for social media applications and an application-usage-based policy optimization feature. The firewall offers TLS usage monitoring for traffic across different versions of TLS.



Source Reference: https://start.paloaltonetworks.com/2020-gartner-mq-for-firewalls.html
https://reprints2.forrester.com/#/assets/2/174/RES176124/report?utm_source=marketo&utm_medium=email&utm_campaign=Global-DA-EN-21-08-20-7014u000001h9xoAAA-P3-Prisma_Access-ZTNA-New-Wave-Report

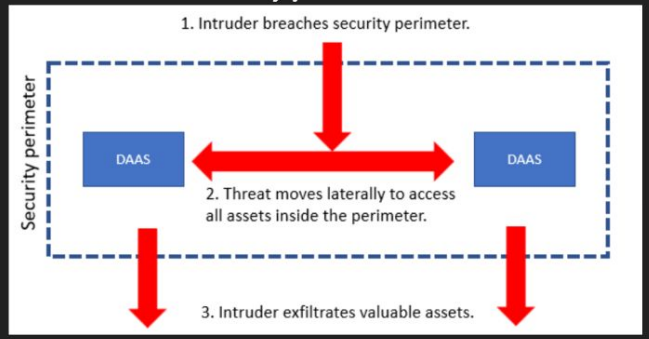
Source Reference:
https://start.paloaltonetworks.com/2020-gartner-mq-for-firewalls.html
https://start.paloaltonetworks.com/ztna-new-wave-report

NIST CSF Core Protect : Firewall (FW) & Zero Trust Network (ZTN) Access

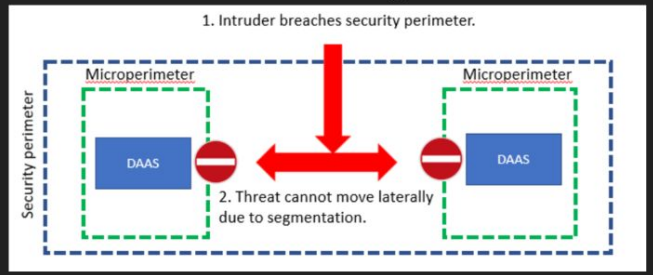
Proposed Cybersecurity Measures to counter 'Known & Unknown Cybersecurity Threats'

Palo Alto Networks® ML-powered Next-Gen Firewall & Zero Trust Network Platform Overview

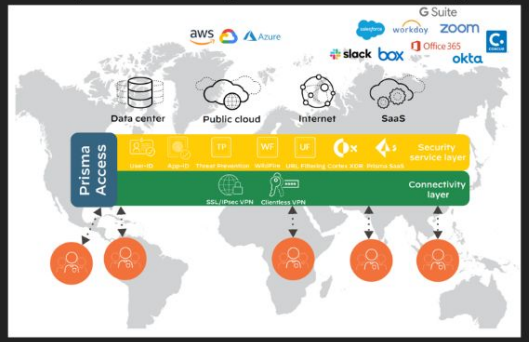
Lateral movement inside the perimeter by attacker once security perimeter breached



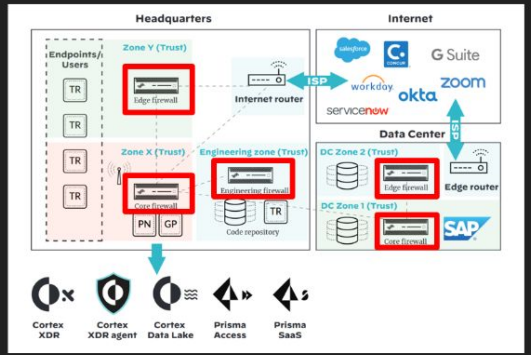
Limited movement inside the perimeter with Zero Trust and network segmentation



Global Security Service Layer & Connectivity Layer on Cloud



Network Segmenting HQ & Data Centre



Source Reference:
https://www.paloaltonetworks.com/cyberpedia/what-is-network-segmentation
https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/use-case/zero-trust-deployment-at-palo-alto-networks

NIST CSF Core Protect : Policy-based multi-factor authentication for Firewall

Proposed Cybersecurity Measures to counter 'Stolen Credentials or Compromised Endpoints'

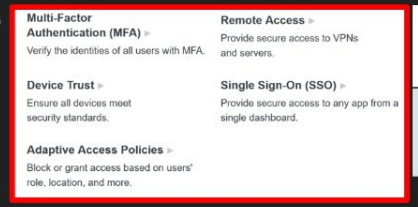
DUO® policy-based multi-factor authentication in Palo Alto Networks® Next-Gen Firewall Overview

DUO® Policy-based multi-factor authentication in Palo Alto Networks® Next-Gen Firewall

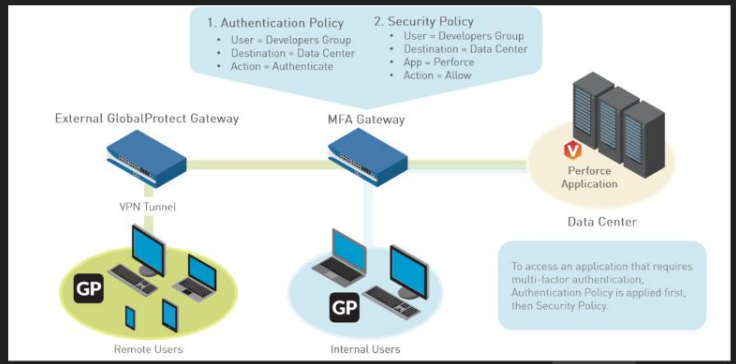
- Enforce multi-factor authentication from the firewall to stop malicious adversaries from moving laterally in a network and accessing sensitive resources with stolen credentials or compromised endpoints.
- DUO® and Palo Alto Networks® partnership enables Enterprises to implement a Zero-Trust security architecture by requiring 2FA two-factor authentication and device hygiene checks for local and VPN users.

DUO® and Palo Alto Networks® Integration Benefits

- **Securing VPN Access**: Palo Alto Networks® GlobalProtect (GP) Gateway is integrated with Duo® to verify users and check the security of their devices before granting them VPN access.
- **Securing Internal Applications**: Duo® integrates with the Palo Alto Networks® Captive Portal to verify the identity of users and the security of their devices, regardless of whether they are logging in locally or through a remote VPN connection, and whether they are accessing internal or cloud applications.
- **Securing Administrative Logins** : Duo® secures administrative logins to Palo Alto Networks® firewalls. Administrators are authenticated using Duo MFA and the security of their devices is verified before granting access to the admin interface. This integration is done using SAML[1].



Palo Alto Networks® GlobalProtect (GP) Gateway is integrated with DUO® to facilitate Multi-Factor Authentication



Source Reference: https://docs.paloaltonetworks.com/globalprotect/9-1/globalprotect-admin/authentication/configure-globalprotect-to-facilitate-multi-factor-authentication-notifications

Source Reference:
https://duo.com/partnerships/technology-partners/select-partners/palo-alto-networks
https://www.paloaltonetworks.com/company/press/2017/palo-alto-networks-delivers-industry-first-capabilities-to-prevent-credential-theft-and-abuse
https://duo.com/product

[1] : Security Assertion Markup Language (SAML) is an open standard that allows identity providers (IdP) to pass authorization credentials to service providers (SP)

NIST CSF Core Detect-Protect : Network Intrusion Detection + Intrusion Prevention

Proposed Cybersecurity Measures to counter 'unauthorized access'

Darktrace Enterprise Immune System® and Darktrace Antigena® Overview

SIGURNOST CONSULTING

Darktrace Enterprise Immune System®

- Darktrace Enterprise Immune System® learns normal 'patterns of life' to discover unpredictable cyber-threats, while delivering complete visibility across Enterprise's dynamic workforce — from cloud and collaboration tools to endpoints and the corporate network.
  - **Detects the unpredictable** - Leverages Self-Learning AI to spot novel attacks and insider threats
  - **Learns 'on the job'** - Understands the DNA of Enterprise business as it evolves, learning and adapting continuously
  - **Provides pervasive coverage** - Correlates insights across multiple silos via an open and extensible architecture

Darktrace Antigena®

- Darktrace Antigena® **brings unique Autonomous Response technology to the Enterprises, with a range of market-leading security products that deliver proactive cyber defense to all parts of the digital infrastructure.**
  - **Interrupts attacks by enforcing 'normal'** - Understands Enterprise business, stops novel cyber-threats
  - **Responds in seconds** - Machine-speed actions taken to interrupt fast-moving attacks
  - **Targeted and proportionate** - Contains the threat only, without disrupting the business

Source Reference:
https://www.darktrace.com/en/enterprise-immune-system/
https://www.darktrace.com/en/darktrace-antigena/

DARKTRACE

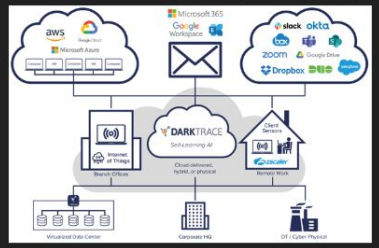
2021 Fortress Cyber Security Awards
Winner — Threat Detection (Darktrace Immune System)

CDM Global Infosec Awards 2021
Cyber Security Artificial Intelligence (Market Leader)
Artificial Intelligence and Machine Learning (Best Product)
Email Security and Management (Best Product)
Endpoint Security (Hot Company)
Security Company of the Year (Market Leader)

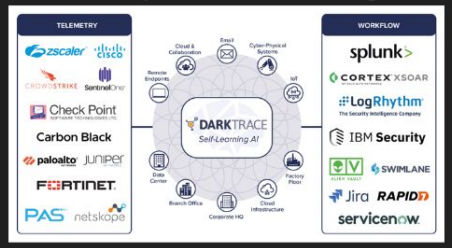
Cybersecurity Excellence Awards 2021
Gold — Best Cybersecurity Company, North America
Gold — Artificial Intelligence Security (Cyber AI Analyst)

Source Reference:
https://www.darktrace.com/en/awards/

Darktrace® Self-Learning AI Coverage



Darktrace® Open Architecture & Integrations



Darktrace® AI Cyber Security that adapts to the Unknown

Darktrace® Autonomous Response across Enterprise Entire Digital Estate

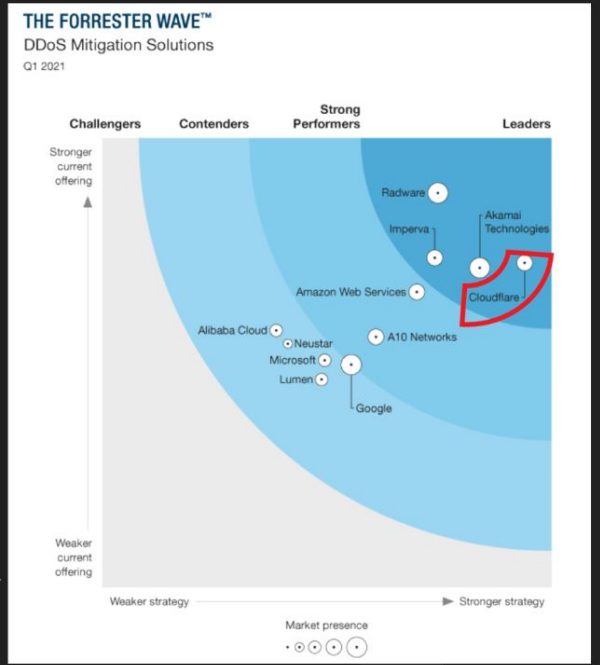
NIST CSF Core Protect: Business Network Protection
Proposed Cybersecurity Measures to counter 'DDoS Attacks'
Cloudflare® Enterprise DDoS Protection Solution Overview

Cloudflare® Enterprise DDoS Protection

- Cloudflare® Named a Leader in The Forrester Wave™ Report: DDoS Mitigation Solutions, Q1 2021.
- Forrester Research, Inc. evaluated 11 of the most significant providers in the market for DDoS Mitigation based on 28-criteria across current offering, strategy, and market presence. In the report, "The Forrester Wave™: DDoS Mitigation Solutions, Q1 2021" Cloudflare® was named a 'Leader'.
- According to Forrester, 'Cloudflare® protects against DDoS from the edge, and fast,' and that 'customer references view Cloudflare®'s edge network as a compelling way to protect and deliver applications.' .
- Cloudflare® also received the highest possible scores in 15 criteria, including 1. Security operations centers, 2. Response automation, 3. Speed of implementation, 4. Product vision, 5. Performance
- Cloudflare® also received the highest score over all assessed vendors in the strategy category.

Detecting & Mitigating DDoS Attacks

- Once traffic arrives at our edge, it encounters Cloudflare®'s 3 software-defined DDoS protection systems:
  - Gatebot - Cloudflare's centralized DDoS protection systems for detecting and mitigating globally distributed volumetric DDoS attacks.
  - dosd (denial of service daemon) - Cloudflare's decentralized DDoS protection systems.
  - flowtrackd (flow tracking daemon) - Cloudflare's TCP state tracking machine for detecting and mitigating the most randomized and sophisticated TCP-based DDoS attacks in unidirectional routing topologies (such as the case for Magic Transit).



Source Reference: https://www.cloudflare.com/forrester-wave-ddos-mitigation-2021/

Source Reference:
https://blog.cloudflare.com/moobot-vs-gatebot-cloudflare-automatically-blocks-botnet-ddos-attack-topping-at-654-gbps/#ddos-detect-mitigate
https://www.cloudflare.com/forrester-wave-ddos-mitigation-2021/

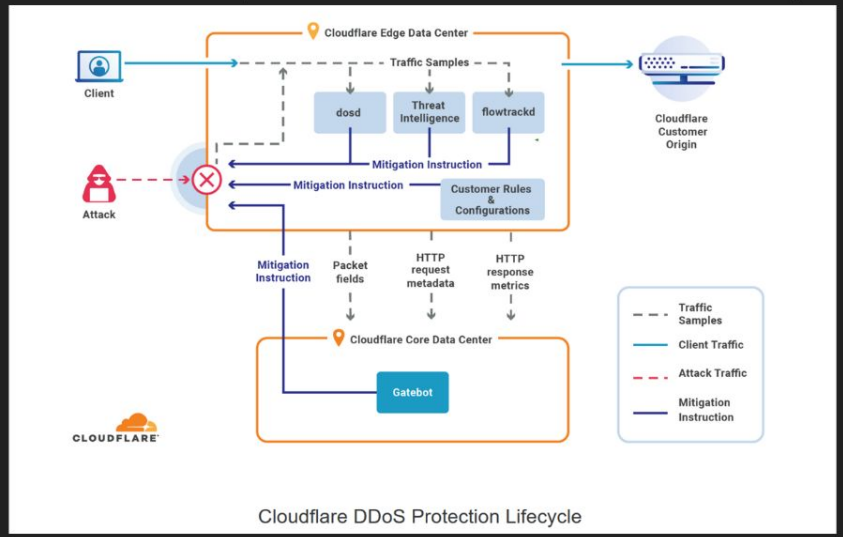
NIST CSF Core Protect: Business Network Protection

Proposed Cybersecurity Measures to counter 'DDoS Attacks'

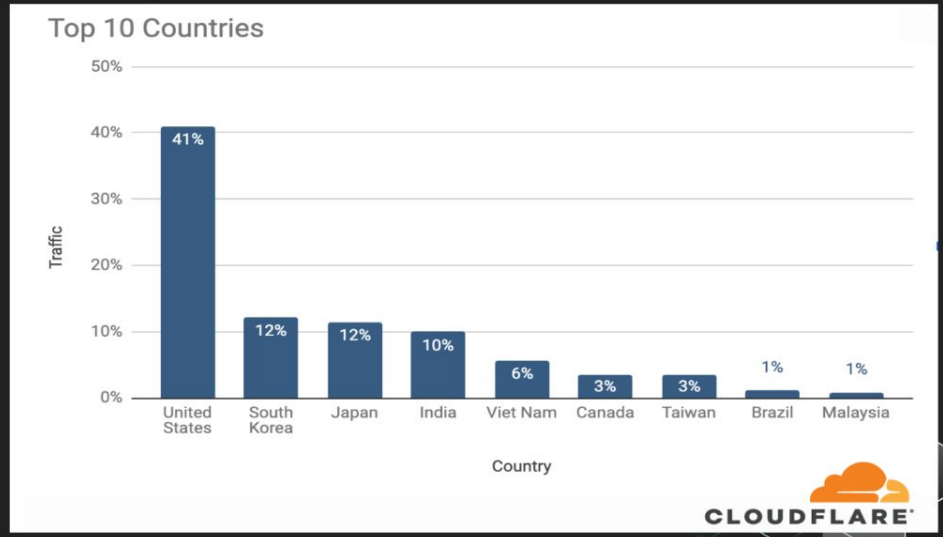
Cloudflare® Enterprise DDoS Protection Solution Overview

Detecting & Mitigating DDoS Attacks

- Cloudflare® 's 3 software-defined DDoS protection systems collect traffic samples in order to detect DDoS attacks. The types of traffic data that they sample include:
  - Packet fields such as the source IP, source port, destination IP, destination port, protocol, TCP flags, sequence number, options, and packet rate.
  - HTTP request metadata such as HTTP headers, user agent, query-string, path, host, HTTP method, HTTP version, TLS cipher version, and request rate.
  - HTTP response metrics such as error codes returned by customers' origin servers and their rates.



Cloudflare DDoS Protection Lifecycle



Source Reference:
https://blog.cloudflare.com/moobot-vs-gatebot-cloudflare-automatically-blocks-botnet-ddos-attack-topping-at-654-gbps/#ddos-detect-mitigate
https://www.cloudflare.com/forrester-wave-ddos-mitigation-2021/

NIST CSF Core Detect-Protect: Security Awareness Computer-Based Training
Proposed Cybersecurity Measures to counter 'DDoS', 'Malware', 'Phishing', 'EPP Do's /Don'ts'
NINJIO® Enterprise Security Awareness Computer-Based Training Solution Overview

- NINJIO® is the Only Vendor recognized as a Gartner Peer Insights Customers' Choice 2021 for Security Awareness Computer-Based Training (SACBT).
- NINJIO®, a cybersecurity awareness training company, currently serving some of the largest organizations in the world.
- Over the last five years, NINJIO® has built an award-winning library of engaging, micro-learning content based on "ripped from the headlines" security breaches. In addition to all episodes being developed by Hollywood television professionals and Writer's Guild members, NINJIO® has added a list of celebrity voice actors to the roster including well-known media celebrities, e.g. Jon Lovtiz, Laticia Rolle, Alex Thomas, and Robert Davi.
- NINJIO® empowers individuals and Enterprise Organizations transforming Corporate Cyber Culture to become defenders against cyber threats.
- NINJIO® custom creates 3- to 4-minute Hollywood style micro-learning videos that teach organizations, employees, and families how not to get hacked.
- Target periodic (daily/weekly/fortnightly/monthly/quarterly) Computer Based Training & Pop Quizzes, & Exams for targeted individual employees at large from Functional Teams, SOC Team, NOC IT Team, IT Support Team, R&D Team, QA Team, Manufacturing & Supply Chain Teams, Sales Team, Marketing Team, Business Development Team, Business Operations & Support Teams, Business Management etc.

Gartner peerinsights customers' choice 2020

NINJIO

NINJIO NAMED THE ONLY CUSTOMERS' CHOICE IN GARTNER PEER INSIGHTS

Never before has only one provider been named as Gartner Peer Insights "Voice of the Customer" in the Security Awareness Computer-Based Training category.

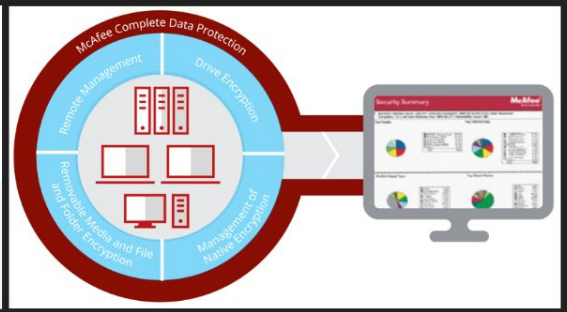
"Vendors placed in the upper-right quadrant of the "Voice of the Customer" quadrants are recognized with the Gartner Peer Insights Customers' Choice distinction. A maximum of 7 vendors can qualify." – Gartner 2020 'Voice of the Consumer': Security Awareness Computer-Based Training Report.

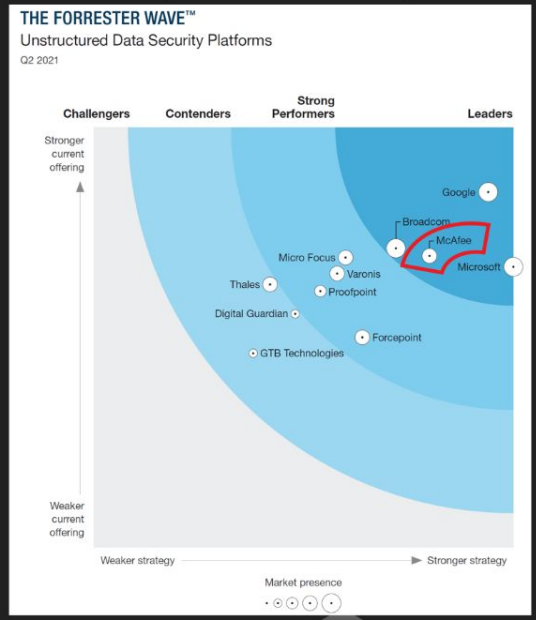
Source Reference: https://ninjio.com/gartner-voice-of-the-customer/

Source Reference:
https://www.cybersecuritydive.com/press-release/20210202-ninjio-is-the-only-vendor-recognized-as-a-gartner-peer-insights-customers/

NIST CSF Core Protect: Data Loss Prevention (DLP) & Encryption
Proposed Cybersecurity Measures to counter 'Known & Unknown top & advanced threats'
McAfee Total Protection for DLP ® & McAfee Drive Encryption® Overview

- McAfee® Named a Leader in The Forrester Wave™: Unstructured Data Security Platforms, Q2 2021.
- Total Protection for Data Loss Prevention (DLP)
- Protect intellectual property and business critical information on the network, in the cloud, and at the endpoints.
- Enable data protection with drive, file, folder, removable media encryption, and data protection for cloud storage.
- Data encryption integrated with centralized management and encryption for Apple FileVault and Microsoft BitLocker to prevent unauthorized access and loss or theft of sensitive data.
- McAfee Total Protection for DLP includes the following components.
  - *McAfee DLP Discover — Finds sensitive data
  - *McAfee DLP Prevent — Enforces DLP policies
  - *McAfee DLP Monitor — Scans network traffic in real time
  - *McAfee DLP Endpoint — Monitors and prevents confidential data loss
  - *McAfee Device Control — Protects removable devices and media
  - *McAfee MVISION Cloud Integration — Extends DLP policies to the cloud





Source Reference: https://www.mcafee.com/enterprise/en-us/solutions/lp/the-forrester-wave-unstructured-data-security-platforms.html?eid=S31X00LZ&smcid=TWO&utm_source=blog&utm_medium=organic#form-download

Source Reference:
https://www.mcafee.com/enterprise/en-sg/products/total-protection-for-data-loss-prevention.html
https://www.mcafee.com/enterprise/en-sg/products/complete-data-protection.html

NIST CSF Core Protect: Enterprise Knowledge Management
Proposed Cybersecurity Measures to counter 'User Behavior and Organizational Cultural Norms'

IBM Watson Discovery® Overview

- IBM Watson Discovery® Named a Leader in the 2021 Gartner Magic Quadrant for Insight Engines
- IBM Watson Discovery® is AI-powered intelligent search that specializes in understanding business-specific natural language, semantics and document structure in order to serve up insights and concise answers from complex business documents.
- Reduces research time by more than 75 percent.
- Watson Discovery® uses Natural Language Processing (NLP) to comprehend human language, allowing users to quickly and easily mine their business's data for answers, and identify patterns and trends that they might not otherwise notice.

Source: Gartner (March 2021)

Source Reference: https://www.gartner.com/doc/reprints?id=1-25I1KOVV&ct=210322&st=sb

Source Reference:
https://www.ibm.com/blogs/watson/2021/03/ibm-gartner-leader-2021-magic-quadrant-insight-engines/

DETECT

PROPOSED SOLUTION FRAMEWORK

Unknown threats with advanced analytics

SIGURNOST CONSULTING

TOOLS & TECHNOLOGY - Categories & Identifiers

- **Anomalies and Events (DE.AE)**
- **Security Continuous Monitoring (DE.CM)**
- **Detection Processes (DE.DP)**

- Security Information & Event Management (SIEM): **IBM Security QRadar® SIEM.**
- Security Orchestration, Automation & Response (SOAR): **IBM Security SOAR®.**
- Threat intelligence on adversary tactics, techniques, and procedures (TTPs) & the attack surface: **IBM X-Force Exchange® Commercial API, IBM Advanced Threat Protection Feed® & IBM Early Warning Feed®.**
- 3rd Party Threat Intelligence Software : **Recorded Future Intelligence Platform® addon for IBM Security QRadar® SIEM.**
- Threat Hunting Platform **: IBM Security i2®**
- User & Entity Behaviour Analytics (UEBA): **Securonix® UEBA addon for IBM Security QRadar® SIEM**
- Intrusion Detection System (IDS): **Darktrace Enterprise Immune System®**
- EndPoint Detection and Response (EDR): **CrowdStrike Falcon® & Proofpoint®**

Product Walk-Through

SUMMARY OUTCOME RESULTS from TASKS & ACTIVITIES

Reference: U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency - CYBER RESILIENCE REVIEW (CRR) CRR: NIST Cybersecurity Framework Crosswalks (cisa.gov)

3.Configuration and Change Management

The purpose of Configuration and Change Management is to establish processes to ensure the integrity of assets using change control and change control audits

Goal - Asset configuration baselines are established.

- Network Operations established & managed (DE.AE-1).
- Expected data flows (users & systems) established & manage (DE.AE-1).

4.Vulnerability Management

The purpose of Vulnerability Management is to identify, analyze, and manage vulnerabilities in a critical service's operating environment

Goal - Preparation for vulnerability analysis and resolution activities is conducted.

- Standard set of tools, methods to identify vulnerabilities, detect malicious code, detect unauthorized mobile code, monitor unauthorized personnel, connections, devices, and software in assets (DE.CM, DE.CM-4, DE.CM-5, DE.CM-7).

Goal - A process for identifying and analyzing vulnerabilities is established and maintained.

- Vulnerability information from identified sources is kept current & Vulnerabilities are actively discovered (DE.DP-5, DE.CM-8).

Goal - Exposure to identified vulnerabilities is managed.

- The effectiveness of vulnerability mitigation is reviewed (DE.DP-5).

Next

DETECT

PROPOSED SOLUTION FRAMEWORK
Unknown threats with advanced analytics

SIGURNOST CONSULTING

TOOLS & TECHNOLOGY - Categories & Identifiers
- **Anomalies and Events (DE.AE)**
- **Security Continuous Monitoring (DE.CM)**
- **Detection Processes (DE.DP)**

Back

SUMMARY OUTCOME RESULTS from TASKS & ACTIVITIES
Reference: U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency - CYBER RESILIENCE REVIEW (CRR) CRR: NIST Cybersecurity Framework Crosswalks (cisa.gov)

5.Incident Management

The purpose of Incident Management is to establish processes to identify and analyze events, detect incidents, and determine an organizational response

Goal -A process for identifying, analyzing, responding to, and learning from incidents is established.
- Has an organizational plan for managing incidents (reviewed & updated). (DE.DP-1, DE.DP-5).
- Staff's roles and responsibilities in Job Descriptions and reflected in incident management plan (DE.DP-1).

Goal - A process for detecting, reporting, triaging, and analyzing events is established.
- Events are detected, reported, data logged in incident knowledge base, analyzed for correlation, tagged for prioritization, status tracked, managed until resolution (DE.CM-1, DE.CM-2, DE.CM-3, DE.DP-4, DE.AE-2, DE.AE-3, DE.AE-4).
- Security forensic requirements for identification of Events evidence identified (DE.DP-2).

Goal - Incidents are declared and analyzed.
- Establish criteria for incident declaration (DE.AE-5).

Goal - Post-incident lessons learned are translated into improvement strategies.
- Root cause analysis of incidents, examine existing link between incident management process and problem management, risk management, change management etc (DE.DP-5).
- Improve asset protection and service continuity strategies by utilizing lessons learned from incident management (DE.DP-5).

MIL4-Measured
- Incident management activities are periodically reviewed and measured to ensure they are effective and producing intended results (DE.DP-3).

8.External Dependencies Management

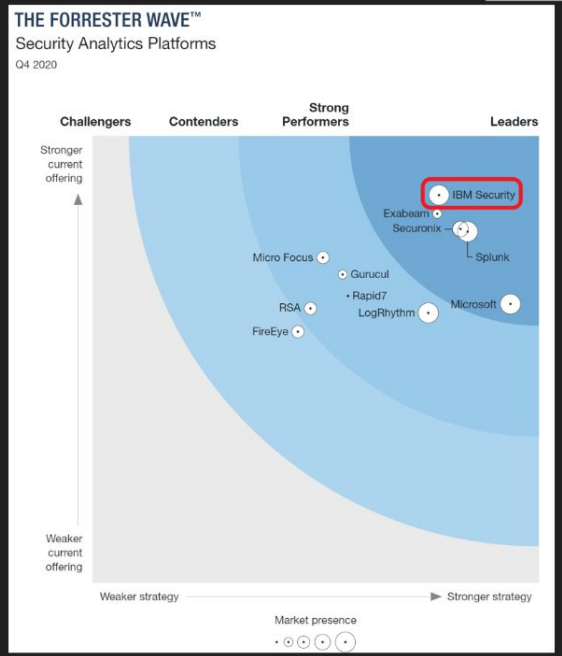
The purpose of External Dependencies Management is to establish processes to manage an appropriate level of controls to ensure the sustainment and protection of services and assets that are dependent on the actions of external entities

Goal - Performance of external entities is managed
- The performance of external entities is monitored against resilience requirements (DE.CM-6).

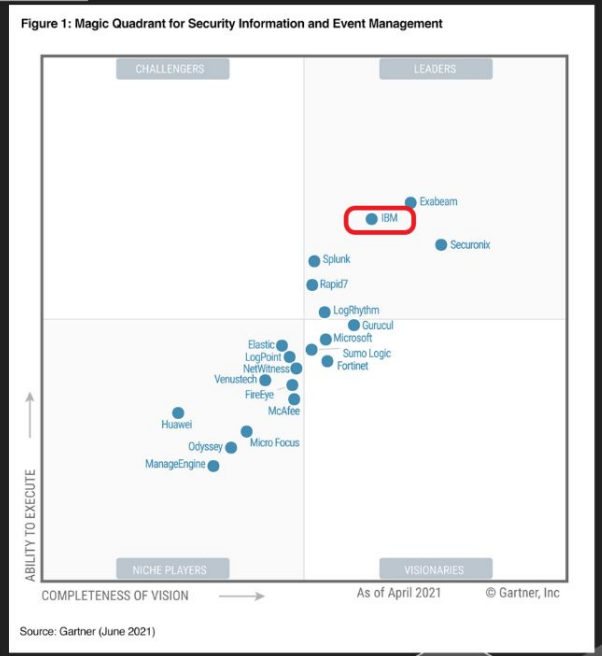
NIST CSF Core Detect: Security Info & Event Mgmt (SIEM) & Sec, Orchestrate, Auto, Resp (SOAR) Proposed Cybersecurity Measures to counter 'Known & Unknown top & advanced threats'

IBM Security QRadar® SIEM + IBM Security SOAR® Platform Overview

- IBM Security QRadar® Named a Leader in the 2021 Gartner Magic Quadrant for Security Information & Event Management (SIEM)
  - **Centralized visibility to detect, investigate and respond** to the most critical organization-wide cybersecurity threats.
  - **Intelligent security analytics** for actionable insight into the most critical threats
  - **Benefits**
1. Identify insider threats
2. Detect advanced threats
3. Secure the cloud
4. Uncover data exfiltration
5. Manage compliance
6. Monitor OT and IOT security
- IBM Security QRadar® SIEM + IBM Security SOAR® Named a Leader in Security Analytics Platforms in the Forrester New Wave Q4 2020 Report.
- IBM Security SOAR® **Benefits**
  - Respond faster and more efficiently
  - Orchestrate and automate response
  - Make SOC's response dynamic



Source Reference: https://reprints2.forrester.com/#/assets/2/73/RES157496/report



Source Reference: https://www.ibm.com/account/reg/us-en/signup?formid=urx-50511

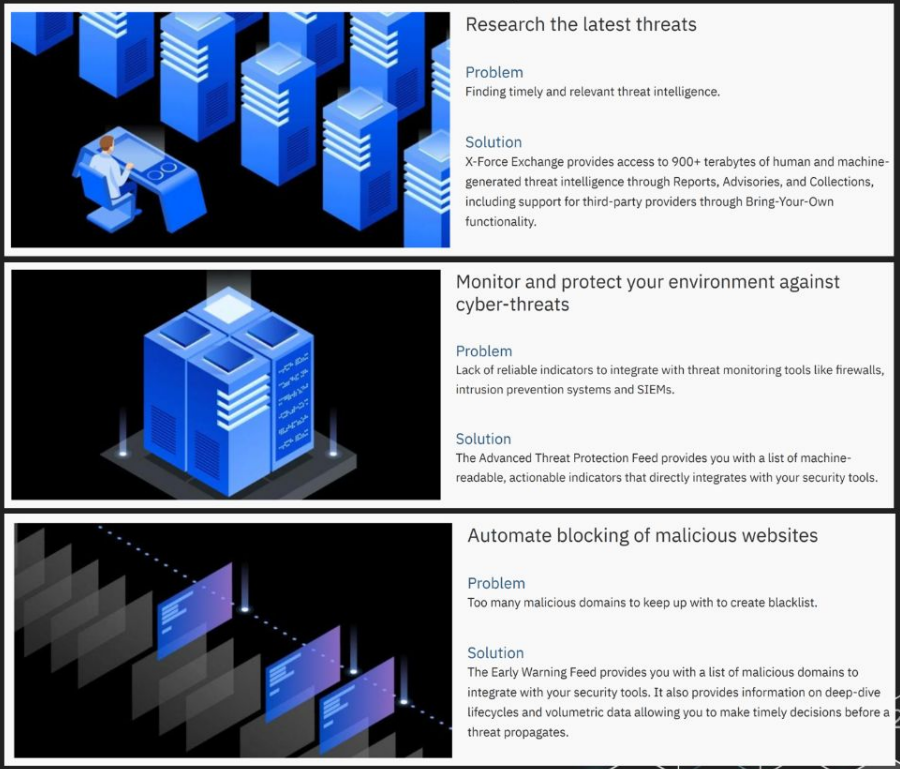
Source Reference:
https://www.ibm.com/sg-en/security/security-intelligence?p1=Search&p4=43700056979249224&p5=b&gclid=CjwKCAjw95vJBhAgEiwAmRrutFiJD7bBBTDi0onvqZ4iuDfR70S8Wv_SVm8r2foVa4sxZs--nXqXghoCmWYQAvD_BwE&gclsrc=aw.ds
https://www.ibm.com/sg-en/products/soar-platform

NIST CSF Core Detect: Threat intelligence - adversary tactics, techniques, procedures (TTPs) & attack surface

Proposed Cybersecurity Measures to counter ‘Known & Unknown top & advanced threats’

IBM X-Force Exchange® Commercial API, IBM Advanced Threat Protection Feed® & IBM Early Warning Feed® Overview

- The IBM X-Force Exchange® enables rapid research on latest global security threats, aggregate actionable intelligence, consult with experts, and collaborate with peers.
- IBM X-Force Exchange® Commercial API provides access to IBM X-Force Exchange® collaborative platform’s contextualized external threat intelligence.
- IBM Advanced Threat Protection Feed® monitors and protects Enterprise efficiently by providing machine-readable, actionable indicators that directly integrate with firewalls, IPS and SIEM.
- IBM Early Warning Feed provides early warning on hundreds of new malicious domains daily through IBM's collaboration with Quad9.



Source Reference:
https://www.ibm.com/products/xforce-exchange/detailshttps://www.ibm.com/sg-en/products/soar-platform

NIST CSF Core Detect: Cyber Threat Hunting

Proposed Cybersecurity Measures to counter 'Known & Unknown top & advanced threats'

IBM Security i2® Overview

- IBM Security i2® provides the means to proactively hunt for cyber threats.
- Significantly improve detection rates and accelerate time to detect, investigate and remediate threats.
- IBM Security i2® helps cyber analysts conduct cyber threat hunting by turning disparate data sets into comprehensive and actionable intelligence in near real-time.
- A cost-effective solution that reduces training, maintenance and deployment costs.

Source Reference:
https://www.ibm.com/security/cyber-threat-hunting
https://www.aitrends.com/security/ai-in-cybersecurity-helping-with-threat-hunting-reducing-attack-vectors/

NIST CSF Core Detect: Threat intelligence - adversary tactics, techniques, procedures (TTPs) & attack surface

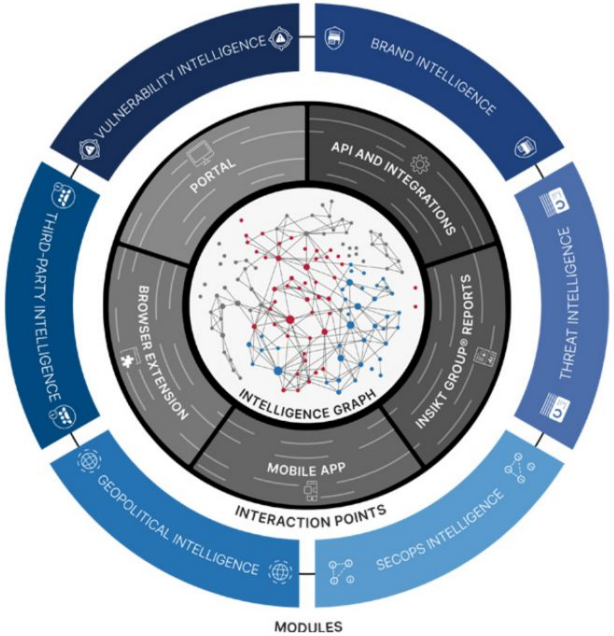
Proposed Cybersecurity Measures to counter ‘Known & Unknown top & advanced threats’

Recorded Future® Intelligence Platform addon for IBM Security QRadar® SIEM Overview

- Recorded Future® delivers the world’s most technically advanced security intelligence to disrupt adversaries, empower defenders, and protect organizations.
- Recorded Future® provides elite, context-rich, actionable intelligence in real time that’s intuitive and immediately accessible via a web portal, mobile application, and browser extension for seamless integration with IBM Security QRadar® SIEM.
- Recorded Future® Intelligence Platform combines automated analytics with human expertise to unite an unrivaled variety of open source, dark web, technical sources, and original research.
- Dynamically categorizing, linking, and analyzing intelligence in real time, the platform delivers easy-to-consume insights for proactive and persistent risk mitigation, via role-based modules that are tailored.
- Results feedback from Customers
  1. Resolve Security Threats 63% Faster
  2. Identify 22% More Security Threats Before Impact
  3. Improve Security Team Efficiency By 32%

Recorded Future®

The World’s Most Advanced Intelligence Platform



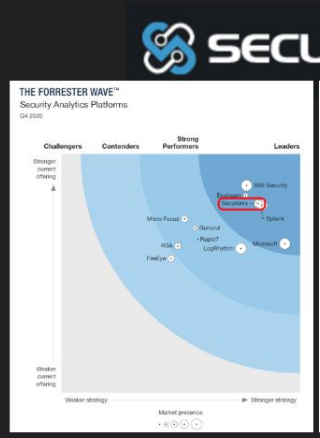
Source Reference:
https://www.recordedfuture.com/platform/
https://www.brighttalk.com/webcast/13713/287507/applying-recorded-future-threat-intelligence-to-the-ibm-security-stack
https://go.recordedfuture.com/hubfs/data-sheets/qradar-1.pdf

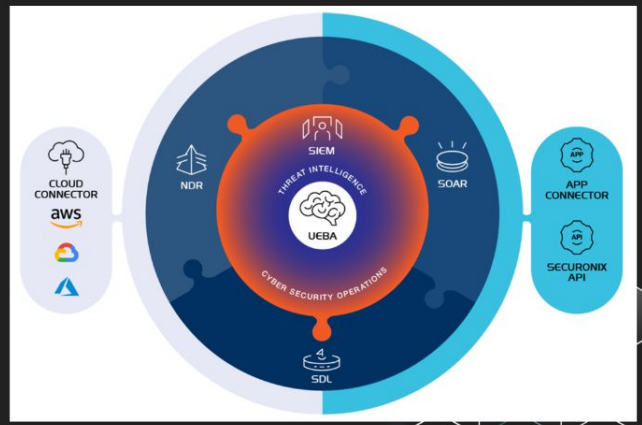
NIST CSF Core Detect: User and Event Behavior Analytics (UEBA)

Proposed Cybersecurity Measures to counter 'Known & Unknown top & advanced threats'

Securonix® UEBA integration with IBM Security QRadar® SIEM Overview

- Securonix® User and Entity Behavior Analytics (UEBA), trusted by 5 of the Fortune 10 companies, transform Enterprise Security Operations
  - Detect unknown, zero day, and advanced persistent threats.
  - Automate routine response actions for common scenarios.
- Leverages sophisticated ML and behavior analytics to analyze and correlate interactions between users, systems, applications, IP addresses, and data.
- Detects advanced insider threats, cyber threats, fraud, cloud data compromise, and non-compliance.
- Built-in automated response playbooks and customizable case management workflows allow fast & accurate response to threats efficiently.
- Securonix® UEBA Benefits and Capabilities
  - Accurately Detect Advanced Threats
  - Quick Time To Value and Rapid Deployment
  - Shorten Time To Respond With Automated Security
  - Protection in the Cloud, for the Cloud
- **Securonix® UEBA add-on for IBM Security QRadar® allows security analysts and response SOC teams to leverage the industry's leading behavior-based insider and cyber threat detection solution to investigate the highest risk users, accounts, and systems in the organization within the IBM QRadar® Console.**





Source Reference:
https://www.securonix.com/https://www.ibm.com/sg-en/products/soar-platform
https://www.securonix.com/
https://reprints2.forrester.com/#/assets/2/73/RES157496/report

NIST CSF Core Detect-Protect : Network Intrusion Detection + Intrusion Prevention

Proposed Cybersecurity Measures to counter 'unauthorized access'

Darktrace Enterprise Immune System® and Darktrace Antigena® Overview

Darktrace Enterprise Immune System®

- Darktrace Enterprise Immune System® learns normal 'patterns of life' to discover unpredictable cyber-threats, while delivering complete visibility across Enterprise's dynamic workforce — from cloud and collaboration tools to endpoints and the corporate network.
  - **Detects the unpredictable** - Leverages Self-Learning AI to spot novel attacks and insider threats
  - **Learns 'on the job'** - Understands the DNA of Enterprise business as it evolves, learning and adapting continuously
  - **Provides pervasive coverage** - Correlates insights across multiple silos via an open and extensible architecture

Darktrace Antigena®

- Darktrace Antigena® **brings unique Autonomous Response technology to the Enterprises, with a range of market-leading security products that deliver proactive cyber defense to all parts of the digital infrastructure.**
  - **Interrupts attacks by enforcing 'normal'** - Understands Enterprise business, stops novel cyber-threats
  - **Responds in seconds** - Machine-speed actions taken to interrupt fast-moving attacks
  - **Targeted and proportionate** - Contains the threat only, without disrupting the business

Source Reference:
https://www.darktrace.com/en/enterprise-immune-system/
https://www.darktrace.com/en/darktrace-antigena/

DARKTRACE

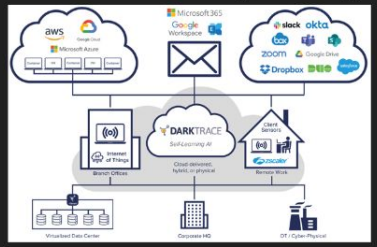
2021 Fortress Cyber Security Awards
Winner — Threat Detection (Darktrace Immune System)

CDM Global Infosec Awards 2021
Cyber Security Artificial Intelligence (Market Leader)
Artificial Intelligence and Machine Learning (Best Product)
Email Security and Management (Best Product)
Endpoint Security (Hot Company)
Security Company of the Year (Market Leader)

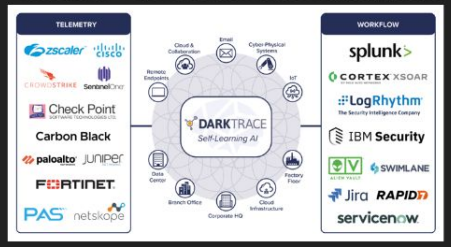
Cybersecurity Excellence Awards 2021
Gold — Best Cybersecurity Company, North America
Gold — Artificial Intelligence Security (Cyber AI Analyst)

Source Reference:
https://www.darktrace.com/en/awards/

Darktrace® Self-Learning AI Coverage



Darktrace® Open Architecture & Integrations



Darktrace® AI Cyber Security that adapts to the Unknown

Darktrace® Autonomous Response across Enterprise Entire Digital Estate

NIST CSF Core Detect-Protect: EndPoint Detection & Response (EDR) & EndPoint Protection (EPP) Proposed Cybersecurity Measures to counter 'BYOD & Corporate End Point Device variants'

CrowdStrike Falcon® EndPoint Security Platform Overview

- CrowdStrike® Named a Leader in the 2021 Gartner Magic Quadrant for Endpoint Protection Platforms
- Protecting Customers in 176 Countries Around the World
- Get peace of mind, and join the world's most secure businesses using CrowdStrike® to stop breaches.
- CrowdStrike® is recognized as a Leader and the security vendor placed furthest for Completeness of Vision in the 2021 Magic Quadrant for Endpoint Protection Platforms (EPP). CrowdStrike® is the only company to not only maintain its Leader position but obtain the furthest position in Completeness of Vision in the EPP Magic Quadrant.
- CrowdStrike Falcon® platform's single, lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network.
- Powered by the proprietary CrowdStrike Threat Graph® database, the Falcon® platform correlates over 5 trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.
- With CrowdStrike®, Enterprise customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon® platform.

Source Reference: Magic Quadrant for End Point Protection Platforms - Gartner May 2021

Source Reference:
https://www.crowdstrike.com/resources/reports/gartner-magic-quadrant-endpoint-protection-platforms-2021/
https://go.crowdstrike.com/2021-Gartner-Magic-Quadrant-Epp-Report.html?utm_campaign=brand&utm_content=sea&utm_medium=sem&utm_source=goog&utm_term=crowdstrike%20gartner%202020&gclid=Cj0KCQiwjo2JBhCRARIsAFG667VbgWCuC7uc3bjFTGbqO9ZGNsg939U3iNt-2ZXqf9t0KEvj-JHfXh0aAjRMEALw_wcB
https://www.crowdstrike.com/resources/reports/gartner-magic-quadrant-endpoint-protection-platforms-2021/

NIST CSF Core Detect-Protect: EndPoint Detection & Response (EDR) & EndPoint Protection (EPP) Proposed Cybersecurity Measures to counter 'BYOD & Corporate End Point Device variants' CrowdStrike Falcon® EndPoint Security Platform Compliance & Certification

SIGURNOST CONSULTING

- Unified cloud-native framework that powers the next generation of enterprise security and IT operations to solve real-world customer problems.
- CrowdStrike®'s Security Cloud is a pioneer in the next-generation enterprise endpoint protection platform, spanning across endpoints, workloads, identities and applications, from the network edge to the cloud. Leverage the power and speed of the cloud, artificial intelligence (AI) and an intelligent, lightweight agent to defend against modern cyberattacks.

CROWDSTRIKE

CrowdStrike recognizes that compliance and certification frameworks are critical to your organization. CrowdStrike can help you meet these requirements, providing you with confidence regarding the safe, smooth and compliant operation of your business. External validation and accreditation is critically important to organizations that rely on CrowdStrike's capabilities and technology to secure their data and comply with regulatory requirements.

PCI DSS v3.2 | CMMC | FedRAMP | EU-U.S. and Swiss-U.S. Privacy Shield Frameworks | HIPAA | NIST | FFIEC | NSA-CIRA | CREST | SOC 2 | AV Comparatives | CSA-STAR | AMTSO | VPAT | GDPR |

ANTI-MALWARE TESTING STANDARDS ORGANIZATION (AMTSO)

CrowdStrike is a registered Vendor Member of the Anti-Malware Testing Standards Organization. AMTSO's mission is to help improve business conditions related to the development, use, testing and rating of anti-malware products and solutions.

- As a vendor member, CrowdStrike contributes to the development of standards for testing anti-malware products.
- CrowdStrike participates in tests that adhere to the anti-malware testing standards created by AMTSO. For example, the CrowdStrike Machine Learning Engine was certified by AMTSO Testing Member SE Labs.

NIST SP 800-53 REV. 4

This report, produced by leading compliance assessor Coalfire, outlines how CrowdStrike Falcon can assist organizations in their compliance efforts with respect to National Institute of Standards and Technology (NIST). NIST Special Publication 800-53 Revision 4 is a security control standard that provides guidelines for selecting technical, physical, and operational security controls for components of an information system that processes, stores, or transmits federal information. In summary, the report shows:

- CrowdStrike Falcon is a suitable solution for addressing the system protection and monitoring controls identified in NIST SP 800-53 Rev. 4.
- CrowdStrike Falcon helps implementing organizations with eight separate NIST control families, covering 23 separate controls.

AV COMPARATIVES TESTING

AV-Comparatives, a leading vendor-independent organization offering systematic testing that checks whether security software live up to their promises and claims. AV Comparatives asked CrowdStrike to participate in their first-ever public comparative test report of next generation security products. In summary, the test report shows:

- CrowdStrike Falcon received the first ever 'Approved NextGen Security' award.
- CrowdStrike Falcon was the only tested endpoint solution to achieve 100% detection efficacy on all exploits used in the testing.
- CrowdStrike Falcon scored a range of 98 to 99.2% detection efficacy with zero false positives on three separate malware tests performed by AV-Comparatives.

Source Reference:
https://www.crowdstrike.com/endpoint-security-products/falcon-platform/
https://www.crowdstrike.com/why-crowdstrike/crowdstrike-compliance-certification/

NIST CSF Core Detect-Protect: EndPoint Detection & Response (EDR) & EndPoint Protection (EPP) Proposed Cybersecurity Measures to counter 'BYOD & Corporate End Point Device variants' Proofpoint® Enterprise Email Security & Protection Solution Overview

SIGURNOST CONSULTING

proofpoint.

- Proofpoint® Named a Leader in The Forrester Wave™ Report: Enterprise Email Security, Q2 2021.
- Email remains the most common channel for opportunistic and targeted cyber attacks—and a major source of data loss. As organizations migrate to the cloud and quickly shift to a remote-work model, organizations are exposed to new classes of advanced email threats and attack vectors. Ransomware to credential phishing to business email compromise (BEC) to supply chain attacks, email continues to be the number one threat vector. The published Forrester Wave™ Report: Enterprise Email Security, Q2 2021 evaluates enterprise email security providers to help security teams select the right solution for their needs.
- Forrester has recognized Proofpoint® as a leader in Enterprise Email Security Domain and its evaluation also gave Proofpoint® the highest score in the current offering category, which includes criteria such as email filtering, threat intelligence, data leak prevention, integrations, incident response, customer support and customer success.
- Email is a central mainstay of modern business. Email is also the source of more than 90% of malware attacks and a deluge of other threats such as phishing, business email compromise (BEC), and more.
- Proofpoint® delivers the most effective solutions to protect Enterprise Businesses from the threats that target them, the data they work with, their digital activity, and the digital channels they rely on. Proofpoint® people-centric approach can help fill all Enterprises' cybersecurity gap.

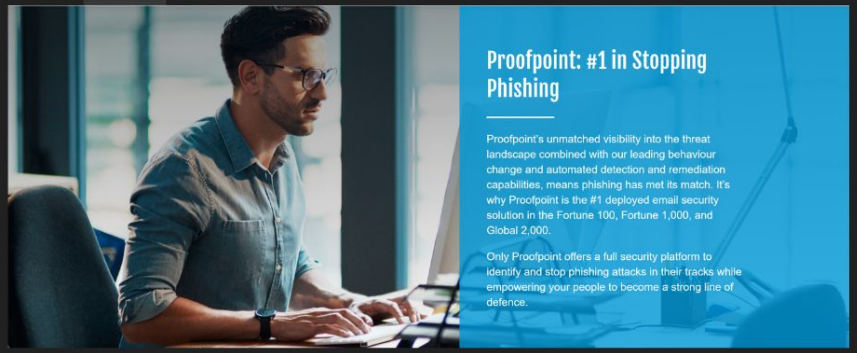
Source Reference:
https://reprints2.forrester.com/#/assets/2/444/RES157497/report

Source Reference:
https://www.proofpoint.com/au/resources/analyst-reports/forrester-wave-report-enterprise-email-security
https://www.proofpoint.com/au/resources/analyst-reports/gartner-market-guide-email-security
https://www.proofpoint.com/us/resources/solution-briefs/protected-with-proofpoint

NIST CSF Core Detect-Protect: EndPoint Detection & Response (EDR) & EndPoint Protection (EPP) Proposed Cybersecurity Measures to counter 'BYOD & Corporate End Point Device variants' Proofpoint® Stop Phishing with a Fully Integrated Solution Overview

SIGURNOST CONSULTING

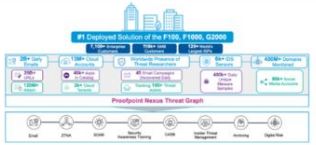
proofpoint.



- Proofpoint® provides a layered approach to stop threats targeting Enterprises' employees. Proofpoint®'s fully integrated approach provides cutting-edge threat intelligence and technology combined with educated users to keep Enterprises safe from phishing
- Accurately detect phishing with Proofpoint® unique Impostor Classifier that dynamically classifies email threats
- Proofpoint® URL defense helps effectively detect, catch, and analyze billions of URLS every day
- Cut phishing risk by up to 90% with Proofpoint® security awareness training
- Remove risk without increasing manual overhead by automating incident response including phishing remediation
- Provide adaptive security control to risky users with email isolation.

Increased Visibility into Threats

Proofpoint has over 100,000 customers with visibility across multiple vectors such as email, cloud, network and social. This gives us unique insight into the threat landscape by correlating threats from various vectors to increase the effectiveness of our advanced email security. We use this visibility to constantly monitor and block more threats from ever getting to your people in the first place.

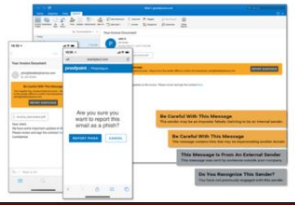


Increased Visibility into User Risk

Sending simulated phish to gauge user risk is great, but it's only one side of the coin. Being able to see which users are being targeted by real attacks offers additional insight. It's not just who is vulnerable to an attack, it's who is being targeted that you need to focus on. Our unmatched visibility into threats targeting your people provides targeted training to the users who need it most – helping you reduce risk faster and run a more targeted, time-efficient program.

Increased Behaviour Change

We don't view education as a checkbox, but as a critical tool. Our hundreds of diverse, multinational, and customizable training modules and awareness materials are designed to drive impactful behaviour change while ensuring compliance and minimizing user downtime. Our investment in continuing to develop our content library is always growing as demonstrated by our acquisition of The Defence Works and partnership with TeachPrivacy.

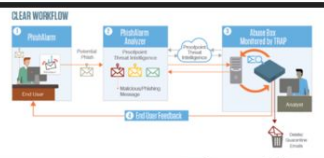


Increase in User Emails Reported

When you educate your users to spot phishing emails, they become part of your line of defence. And email warning tags allow them to report on suspicious emails more easily by responding directly from the tag. They can receive nudges if the message is from an external sender, potentially an impostor, or impersonating a domain. This makes it easier for users to rethink engaging with potentially suspicious messages.

Increase Automated Abuse Mailbox Remediation

Abuse mailboxes can drain time for already over-burdened incident response teams. Proofpoint's Closed-Loop Email Analysis and Response (CLEAR) solution automates the entire process, from users reporting emails to malicious messages being removed automatically. No YARA rules to configure, no sandbox or threat intelligence to purchase. Everything's included with CLEAR.



Source Reference:
https://www.proofpoint.com/au/solutions/protect-against-phishing

NIST CSF Core Detect-Protect: EndPoint Detection & Response (EDR) & EndPoint Protection (EPP) Proposed Cybersecurity Measures to counter 'BYOD & Corporate End Point Device variants' Technology & Alliance Partners : Proofpoint® and Crowdstrike® Overview

Unparalleled protection for end users and their endpoints

- Nearly 100% of threats are human activated. Transform Enterprises' security program by deploying automated remediation for attacks targeting Employees and their devices.

Get automated end-to-end protection against threats across email and devices.

- Proofpoint® and CrowdStrike® have partnered to transform Enterprises' security program and protect all Enterprise organizations from the ever-changing threat landscape. Together, Proofpoint® and CrowdStrike® improve Enterprise security efficacy and enhance Enterprise visibility and context around threats. Proofpoint® and CrowdStrike® orchestration and response capabilities make SOC security team more productive which help to reduce the overall risk against the No. 1 threat vector.

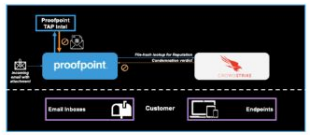
Integrations and Benefits

Pre-Delivery Protection

Proofpoint leverages CrowdStrike intelligence to block malicious email attachments at the gateway. Our combined visibility and threat detection capabilities protect your inbox and endpoint.

- Proofpoint sandboxes incoming files and queries the CrowdStrike Intelligence API for file reputation
- You get improved protection through our threat intelligence sharing, since we block ransomware, polymorphic malware, keyloggers and zero-day threats from getting to your inbox

Pre-delivery Email Protection



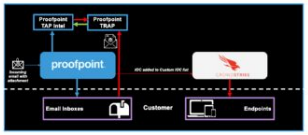
1. Email with attachement detected at email gateway (PPS).
2. Attachement sent to Proofpoint TAP (Sandbox) for analysis, file-hash reputation lookup with CrowdStrike Falcon X.
3. CrowdStrike condemns attachment, email is blocked at gateway.
4. If CrowdStrike does not respond with verdict but Proofpoint sandbox condemns attachment, email is blocked at gateway.

Post-Delivery Automated Remediation

Proofpoint automatically detects and quarantines email that turns malicious post-delivery. And we share intelligence about unknown threats with CrowdStrike. This helps to limit future attacks on your endpoints.

- Proofpoint quarantines any messages that have been delivered or forwarded
- If unknown to CrowdStrike, the malicious hash is added to the CrowdStrike list of custom indicators of compromise (IOCs)
- An alert is created if the malicious content tries to execute on the device

Post-delivery Protection



1. If an attachment delivered is later found to be malicious (weaponized URL etc.), Proofpoint TAP alerts TRAP (Threat Response Auto-Pull).
2. IOC created and added to CrowdStrike Customer IOC list for joint customers.
3. TRAP then pulls out the email from all customer inboxes (original plus forwards).
4. CrowdStrike Falcon platform generates alerts that can be followed up on by security team (also block any future attack directly on the endpoint).

Enhanced Zero Trust Security

As companies work to achieve zero trust security within their organizations, making sure the endpoint is within security compliance before allowing it to connect is critical. Proofpoint Meta and Crowdstrike Falcon integrate with posture checking to ensure endpoints are in compliance.

- Ensure secure access to confidential systems by using the Proofpoint Meta agent to detect if Crowdstrike Falcon is deployed on the endpoint. If not then several actions, such as disconnecting the endpoint, can take place.
- Proofpoint Meta administrators have flexibility to create a posture checking message for the end user letting them know why they have failed posture checking and provide potential remediation options such a clicking a URL to deploy the Crowdstrike Falcon agent.

Address Your Security Program Challenges

- Security Efficacy
- Solution Complexity
- Attacker Sophistication
- SOC Productivity
- Threat Visibility
- Time to Deploy
- Talent Shortage
- Manual Workflows

proofpoint.

CROWDSTRIKE

As companies continue struggling with advanced threats targeting their organizations, new approaches are needed to help mitigate the risk of these threats. Proofpoint® and CrowdStrike® know that over 90% of threats originate via the email vector. Proofpoint® and CrowdStrike® have partnered to give shared customers an enhanced security posture—from email to the device itself.

Source Reference:
https://www.proofpoint.com/eu/technology-partners/crowdstrike

PROPOSED SOLUTION FRAMEWORK

SIGURNOST CONSULTING

RESPOND *to cyber outbreaks*

TOOLS & TECHNOLOGY	TASKS & ACTIVITIES
• RESPONSE PLANNING (RP) • COMMUNICATIONS (CO) • ANALYSIS (AN) • MITIGATION (MI) • IMPROVEMENTS (IM) • Security Information & Event Management (SIEM): IBM Security QRadar® SIEM • Security Orchestration, Automation & Response (SOAR): IBM Security SOAR® • User & entity Behaviour Analytics (UEBA): Securonix® UEBA addon for IBM Security QRadar® SIEM • Intrusion Detection System (IDS): Darktrace Enterprise Immune System® • EndPoint Detection and Response (EDR): CrowdStrike Falcon® & Proofpoint®	1. RS.CO-1: Ensure personnel understand objectives, restoration priorities, task sequences and assignment responsibilities for event response. ○ Everyone must do their due diligence. ○ Change in culture needed to achieve Tier 4. 2. RS.CO-2: Incidents are reported consistent with established criteria ○ ALL alerts must be investigated and reported in completeness ○ Implement automated mechanisms to assist in the reporting of cybersecurity events. 3. RS.AN-1: Implement automated mechanisms to assist in the investigation and analysis of cybersecurity-related notifications. ○ IBM Security QRadar® SIEM with SOAR® (formerly Resilient) 4. RS.AN-2: Implement automated mechanisms to support incident impact analysis. ○ Test incident response capability 5. RS.AN-3: Provide on-demand audit review, analysis, and reporting for after-the-fact investigations of cybersecurity incidents. ○ All incidents regardless of severity or impact should be included in such reports. This is to help with investigations by providing all possible clues/reasons for the incidents. 6. RS.AN-4: Categorize cybersecurity incidents according to level of severity and impact consistent with the response plan. ○ Helps to prioritise threat treatment

PROPOSED SOLUTION FRAMEWORK

SIGURNOST CONSULTING

RESPOND *to cyber outbreaks*

TOOLS & TECHNOLOGY	TASKS & ACTIVITIES
• RESPONSE PLANNING (RP) • COMMUNICATIONS (CO) • ANALYSIS (AN) • MITIGATION (MI) • IMPROVEMENTS (IM) • Security Information & Event Management (SIEM): IBM Security QRadar® SIEM • Security Orchestration, Automation & Response (SOAR): IBM Security SOAR® • User & entity Behaviour Analytics (UEBA): Securonix® UEBA addon for IBM Security QRadar® SIEM • Intrusion Detection System (IDS): Darktrace Enterprise Immune System® • EndPoint Detection and Response (EDR): CrowdStrike Falcon® & Proofpoint®	13. RS.AN-5: Implement automated mechanisms to disseminate and track remediation efforts for vulnerability information captured from internal and external sources to key stakeholders. ○ This information MUST be kept current. ○ Vulnerabilities MUST be actively discovered. ○ Vulnerabilities MUST be categorised and prioritised. ○ Vulnerabilities MUST be analysed to determine relevance to the organisation. 14. RS.MI-2: Implement automated mechanisms to support the cybersecurity incident mitigation process. ○ Darktrace Enterprise Immune System® ○ World's first proven Autonomous Response technology for the enterprise which operates as an AI decision-making framework that neutralizes fast-moving and unpredictable attacks in seconds, while sustaining normal operations by design. 15. RS.IM-2: Update the response plans to address changes to the organization, manufacturing system, attack vectors, or environment of operation and problems encountered during plan implementation, execution, or testing. ○ Updates may include, for example, responses to disruptions or failures, and predetermined procedures. ○ Enable a process for the response plan to evolve to reflect new threats, improved technology, and lessons learned.

PROPOSED SOLUTION FRAMEWORK

RECOVER Access to critical data and applications

TOOLS & TECHNOLOGY

- IBM X-Force IRIS Vision Retainer
- Backup as a Service (BaaS)
- Recovery as a Service (RaaS) Rating
- Network as a Service (NaaS)
- Resilience Orchestration
- Multi-Network WAN

TASKS & ACTIVITIES

- Establish and improve effective RPO - Recovery Point Objectives and RTO - Recovery Time Objective.
- Expedite problem identification and reduce downtime
- Scalable to large and small system components
- Ease of testing and repeatable process
- Simplify regulatory reporting
- Education and Training

National Institute of Standards and Technology

Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	**RC.RP-1:** Recovery plan is executed during or after a cybersecurity incident
Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	**RC.IM-1:** Recovery plans incorporate lessons learned **RC.IM-2:** Recovery strategies are updated
Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	**RC.CO-1:** Public relations are managed **RC.CO-2:** Reputation is repaired after an incident **RC.CO-3:** Recovery activities are communicated to internal and external stakeholders as well as executive and management teams

Run Book Components

Pre-Conditions Required for Effective Recovery

- Formal Recovery Procedures in place, Critical people, facilities, technical components, and external services, Functional and security dependency maps ,Metrics - eg Labour costs, Legal Cost, Authorized resources and tested tools, Comprehensive recovery communications plan, Periodic training and exercises

Tactical Recovery Phase

Initiation

- Identify and Isolate. motivation, assets, techniques and tools, footprint, adapt the run book, prioritisation, harden the processes, metrics.

Execution

- Execute recovery run book, re-instantiate trust, reinforce vulnerabilities, track downtime, communications, restore services.

Termination

- Determine data has been restored, restoration complete, return to normal. Record details for improvement.

Strategic Recovery Phase

- Planning and Execution - consolidation, complete communications, determine long term goals for future incidents.
- Metrics - Review metrics to assess effectiveness of plan
- Recovery Plan Improvement - Review, Practice and improve

https://www.ibm.com/common/ssi/ShowDoc.wss?docURL=/common/ssi/rep_sm/x/649/ENUS5900-AAX/index.html&lang=en&request_locale=en

https://www.gartner.com/reviews/market/disaster-recovery-as-a-service

x

IBM Recovery Services

- **IBM DRaaS** - reliably helps recover critical IT business processes and data to support business resiliency. It also provides comprehensive disaster recovery services, including health monitoring as well as continuous replication of applications, infrastructure, data and cloud systems. Gartner 4* Star Rating

- **IBM BUaaS -** Backup as a service (BUaaS) helps protect and retrieve critical business data, monitor the health of your data protection environment and comply with government and industry regulations. It manages your data backup with robust on-site, off-site and hybrid cloud–based security.

- **IBM Resiliency orchestration services** - IBM Cloud Resiliency Orchestration provides disaster recovery monitoring, reporting, testing and workflow automation capabilities of complex hybrid environments in a scalable, easier-to-use solution built on industry standards. This service combines automation and analytics for faster, more cost-effective DR that helps keep daily business operations running and proactively avoids disruptions that lead to lost revenue, brand damage and dissatisfied customers.

https://www.ibm.com/services/business-continuity/resiliency-backup-service

x

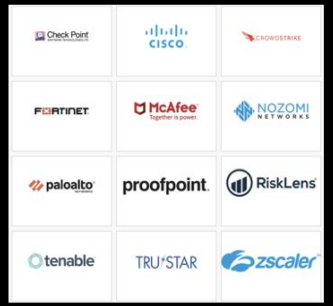
IBM **Managed Network Services**

- Solutions designed to help reduce unplanned downtime, improve global agility, simplify management and provide higher network capacity at a lower cost.
- SD-WAN Managed Services
- Analytics and automation

IBM X-Force IRIS Vision Retainer

- Two proactive services units (PSU) to use towards services that include:
- IR program assessment
- IR plan development
- IR playbook customization
- Tabletop Exercise
- Security Incident First Responder Training
- Strategic threat assessment
- Dark web search services

Partners



Next Steps and Challenges

- The biggest challenge is transforming the culture of the entire organisation to a Proactive - Adaptive tier of cyber security.
- Rolls Royce resides in a complex ecosystem of different technologies, business , supply chain and dependencies. An adaptive cyber Security culture must be propagated to all components.
- Whilst daunting, Tier 4 instills a culture of continuous improvement and change. This is unavoidable where Black Hats are always one step ahead.
- The proliferation of Cyber Security Software and Hardware Service Providers can help the transition, but can also add unwanted and unnecessary complexity to the functions performed by the SOC.
- We hope Sigurnost can help simplify and facilitate the move to Tier 4.

x

Thank You for Your Time

Thank You for Your Data

x