CyberProof®
A UST Company

THE INNER WORKINGS OF CYBER DEFENDERS

REAL EXAMPLES OF HOW SECURITY OPERATIONS TEAMS CAN COLLABORATE TO MITIGATE CYBER THREATS

TABLE OF CONTENTS

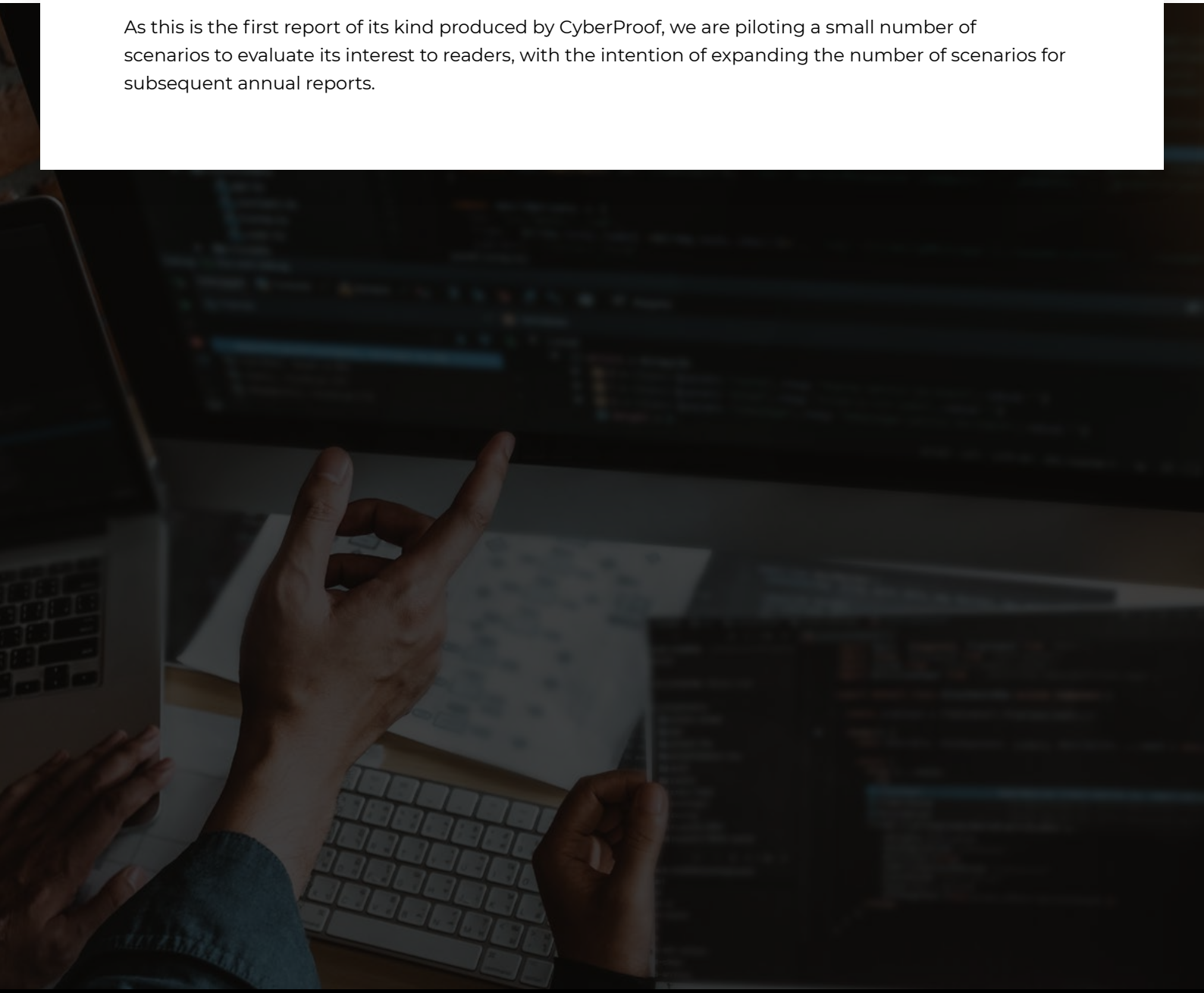
WHY READ THIS REPORT

You've probably encountered another wave of threat intelligence reports outlining top attack campaigns in 2020. These reports are helpful in that they provide insight into common attacker behaviors and methods, however many of them don't help you to apply this insight with examples of the mitigation steps taken by defenders.

The aim of this report is to go that extra step.

To do this, we illustrate three scenarios of how individual teams within CyberProof and our customers worked together – including L1 analysts, L2 analysts, SIEM specialists, DFIR specialists, Threat Hunters, and Cyber Threat Intelligence (CTI) analysts – to detect and respond to some of the most persistent attacks. We also highlight the techniques used to demonstrate how different teams can work together effectively to mitigate threats, and how use cases can be applied practically.

As this is the first report of its kind produced by CyberProof, we are piloting a small number of scenarios to evaluate its interest to readers, with the intention of expanding the number of scenarios for subsequent annual reports.



SCENARIO 1 – TARGETED MALSPAM CAMPAIGN EXPLOITING DATA LEAKAGE

CyberProof's CTI team was asked by a client to monitor the web for signs of leaked data that could be used in cyber attack campaigns. The CTI team subsequently discovered email addresses in a public server that were being used in a large malspam campaign, which enabled the attackers to mitigate security tools and compromise critical data.

Use Case Involved - By Team:

CTI team

- Data Leakage Monitoring
- Threat Intelligence Investigations and Response
- Root Cause Analysis
- Dark Web Monitoring
- Threat Actor Tracking

L1 + L2 analysts

- Incident Investigation
- Incident Response
- Detection Rule Implementation

SIEM engineers

- Detection Rule Creation

HERE ARE THE STEPS WE TOOK:

1 **Following lead –** While monitoring customers' assets, the CTI team discovered a public server that contained multiple business email addresses belonging to several of our customers. (See: https://attack.mitre.org/techniques/T1589/002/) The team collected all relevant information including leaked email addresses, IP addresses, domains, and reputation of the indicators.

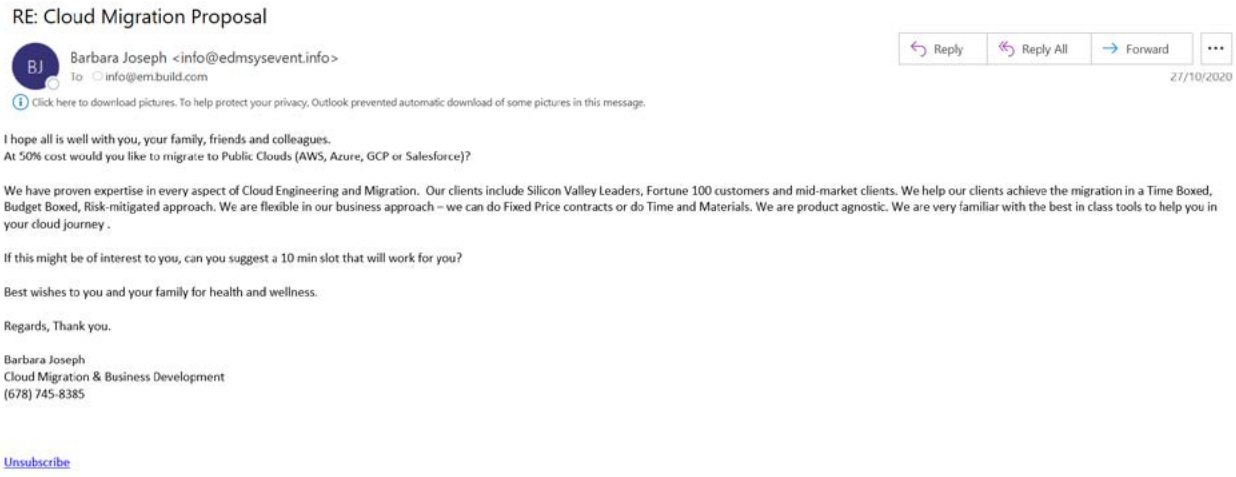

Index of /mlogd

Name	Last modified	Size	Description
Parent Directory		-	
fail-2020-09-18-17:2..>	2020-09-18 17:25	11M	
fail-2020-09-19-19:0..>	2020-09-19 19:03	4.1M	
fail-2020-09-22-04:2..>	2020-09-22 04:29	8.4M	
fail-2020-09-24-10:0..>	2020-09-24 10:02	1.1M	
fail-2020-09-26-08:3..>	2020-09-26 08:33	2.2M	
fail-2020-09-28-05:4..>	2020-09-28 05:49	1.0M	
fail-2020-10-02-13:3..>	2020-10-02 13:36	10M	
fail-2020-10-05-18:4..>	2020-10-05 18:49	8.7M	
fail-2020-10-06-12:1..>	2020-10-06 12:10	0	
fail-2020-10-07-03:5..>	2020-10-07 03:50	0	
fail-2020-10-07-03:5..>	2020-10-07 03:51	0	

Figure 1: Public server contains multiple business email addresses of customers

2 **Escalation to cyber analyst –** The CTI team created an incident in the CyberProof Defense Center (CDC) platform and gave it a severity assignment. The team added to the CDC all of the IOCs they'd collected and other relevant data. They then assigned the incident to the customer's L2 team.

3 **Investigation –** The L2 team began its investigation, following the directives in our playbook for email campaigns. The team studied and analyzed the IOCs provided by the CTI team. They concluded that the server identified by the CTI team was being used in a massive malspam campaign against one of our customers. (See: https://attack.mitre.org/techniques/T1566/)



RE: Cloud Migration Proposal

BJ Barbara Joseph <info@edmsysevent.info>
To info@em.build.com

Reply | Reply All | Forward
27/10/2020

Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

I hope all is well with you, your family, friends and colleagues.
At 50% cost would you like to migrate to Public Clouds (AWS, Azure, GCP or Salesforce)?

We have proven expertise in every aspect of Cloud Engineering and Migration. Our clients include Silicon Valley Leaders, Fortune 100 customers and mid-market clients. We help our clients achieve the migration in a Time Boxed, Budget Boxed, Risk-mitigated approach. We are flexible in our business approach – we can do Fixed Price contracts or do Time and Materials. We are product agnostic. We are very familiar with the best in class tools to help you in your cloud journey .

If this might be of interest to you, can you suggest a 10 min slot that will work for you?

Best wishes to you and your family for health and wellness.

Regards, Thank you.

Barbara Joseph
Cloud Migration & Business Development
(678) 745-8385

Unsubscribe

Figure 2: Phishing email found

4 **Response –** The L2 team initiated containment actions, following the directives in the playbook, including blocking the source, checking for users that were lured, etc. The team recommended that the customer inform members of its team and train them to be on the lookout for potential phishing attacks. All new data and actions that were taken were recorded in the CDC. The L2 team needed additional information about the spamming email addresses and tagged a CTI analyst in the CDC with this request.

5 **Root cause analysis –** The CTI team searched for the root cause of the data leakage and assigned the customer's Operations team actions aimed at remediating the source of the leakage. For example, the team opened a ticket to remove a GitHub account that publicly exposed multiple business email addresses of the customer.

6 **Monitor –** After the incident was completed, our SIEM team was assigned to create, test, and tune detection rules based on the IOCs. Following the CyberProof's predefined process, the rules were deployed in the SIEM and continue to be monitored our cyber analysts, providing protection against potential future incidents.

7 **Closure –** Once the detection rules were deployed successfully, the incident was assigned back to the cyber analyst, who gave it the relevant status and closed the incident. The CTI team then analyzed the incident IOCs in order to detect potential threats to other customers. This was done by investigating the server, searching for other customers' email addresses, and by looking for additional spam servers within the same network. The investigation was focused on (but not limited to) customers from the same sector or geolocation. When such a threat was detected, the CTI team investigated it and opened a new incident for that customer.

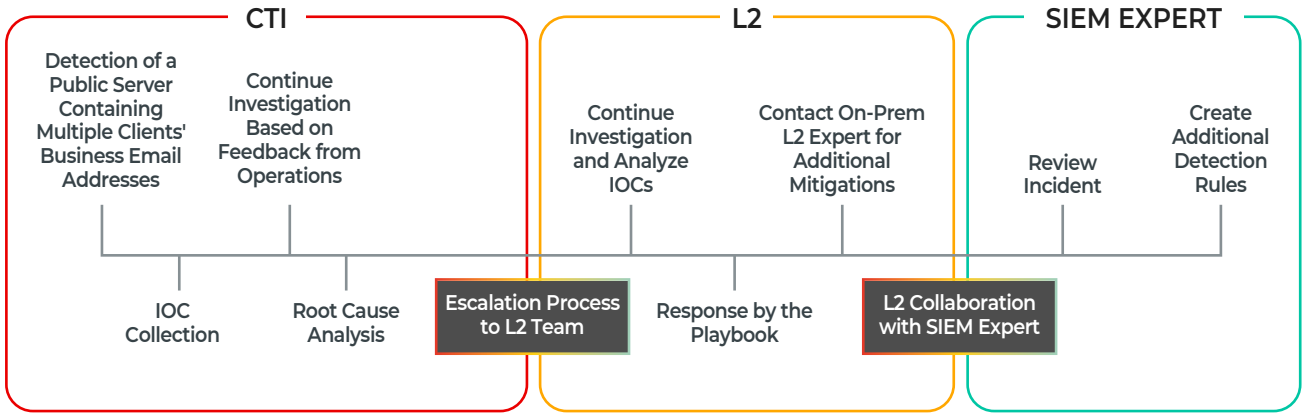
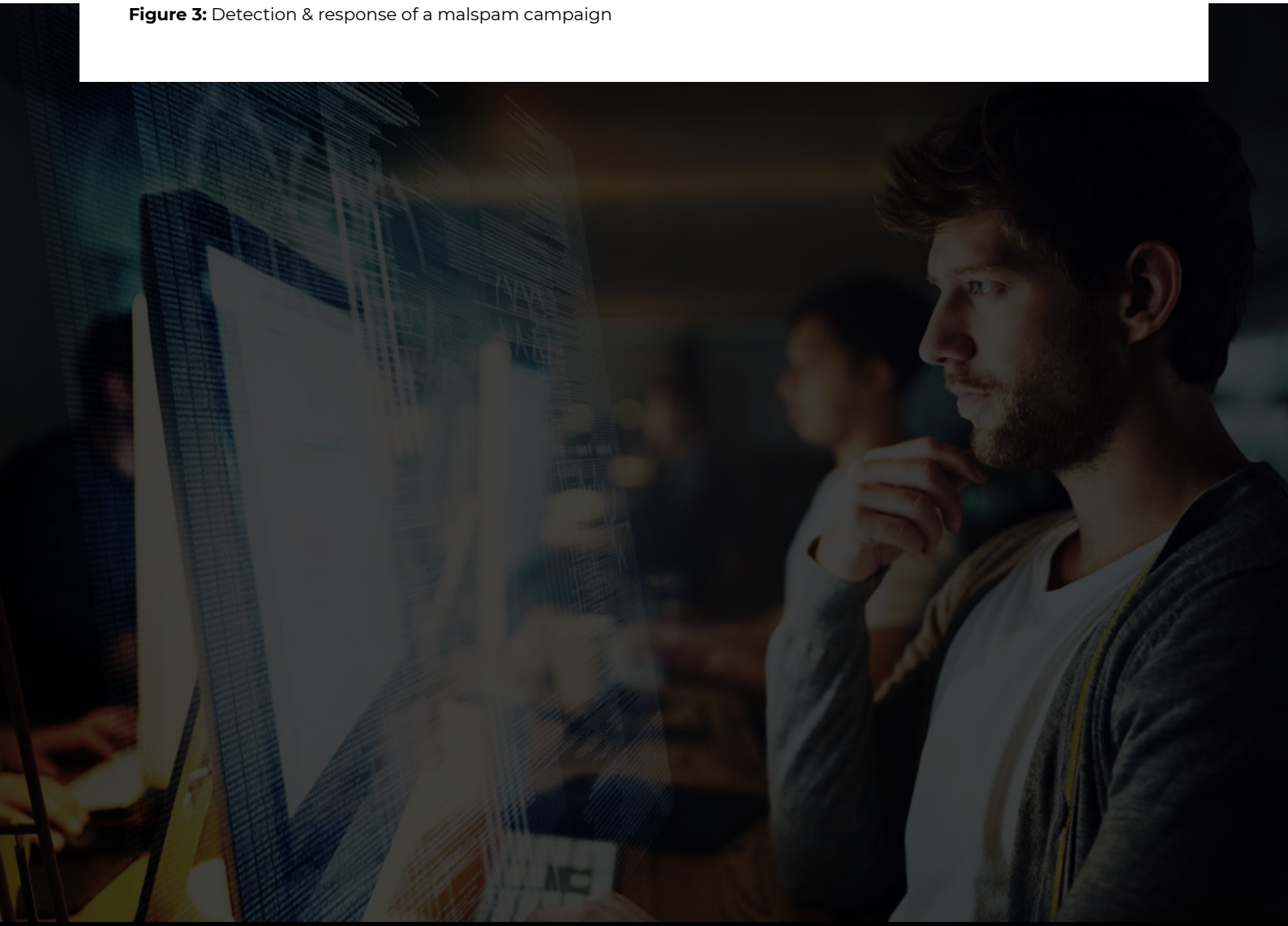


Figure 3: Detection & response of a malspam campaign



SCENARIO 2 – BLACK MARKETPLACE USING AZORULT MALWARE TO SELL EMPLOYEE CREDENTIALS

While proactively monitoring the dark web on behalf of one of our clients, our CTI team identified a potential threat within the client's environment. The CTI team collaborated with our L2 team and the client-side team to identify the threat and mitigate the damage.

Use Case Involved - By Team:

CTI team

- Data Leakage Monitoring
- Threat Intelligence Investigations and Response
- Root Cause Analysis
- Dark Web Monitoring
- Validation of Infection

L1 + L2 analysts

- Incident Investigation
- Incident Response
- Detection Rule Creation + Implementation

Threat Hunting team

- Compromise Assessment

HERE ARE THE STEPS WE TOOK:

1 **Following lead –** By monitoring a range of hacking forums on the dark web, the CTI team learned that a threat actor was offering for sale the stolen credentials of high-profile employees from multiple organizations. They suspected that one of our customers may have been compromised by this. There were also reasons to believe the credential theft had been accomplished using AZORult malware, a family of malicious software used for stealing user data.

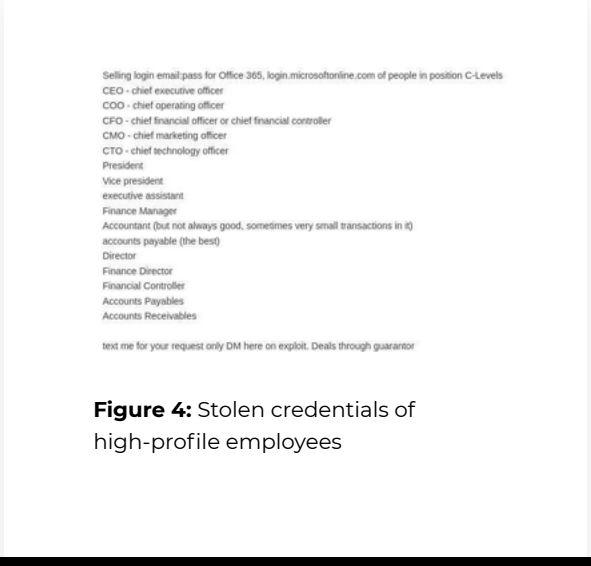


Figure 4: Stolen credentials of high-profile employees

2 **CTI investigation –** The CTI team checked several different black markets that sell credentials harvested by AZORult botnet and looked for indications that the customer's assets were compromised. The team then concluded that the best way of assessing if the customer was affected by the credential leak was to verify whether the customer's network was infected by AZORult. They created an incident in the CDC platform, and gave it a severity and SLA assignment. The research conducted by the CTI team led them to the following MITRE ATT&CK Tactics and Techniques, which taught them about the initial common vector of attack, and additional AZORult capabilities:

- **Resource Development -** T1586.002 Compromise Accounts: Email Accounts
- **Initial Access -** T1566 - Phishing
- **Execution -** T1204 - User Execution
- **Defense Evasion, Privilege Escalation -** T1134.002 Access Token Manipulation: Create Process with Token
- **Defense Evasion -** T1070.004 Indicator Removal on Host: File Deletion
- **Credential Access -** T1555.003 Credentials from Password Stores: Credentials from Web Browsers
- **Credential Access -** T1552.001 Unsecured Credentials: Credentials In Files
- **Discovery -** T1012 Query Registry
- **Discovery -** T1082 System Information Discovery
- **Discovery -** T1016 System Network Configuration Discovery
- **Discovery -** T1033 System Owner/User Discovery
- **Discovery -** T1124 System Time Discovery
- **Command And Control -** T1573.001 Encrypted Channel: Symmetric Cryptography
- **Command And Control -** T1105 Ingress Tool Transfer

3 **CTI response + L1 scanning –** The CTI team gathered IOCs associated with the AZORult malware – including IPs, domains, and hashes – as well as YARA rules. The collected domain IOCs were shared with the L1 analysts who, using SEG and firewalls, scanned the customers' networks for any hits.

4 **L2 analyst response –** The incident was assigned to an L2 analyst, who ensured that hashes were uploaded into the EDR for detection and that appropriate detection rules were implemented.

5 **Forensic analysis –** Recent samples of AZORult which had been collected by the CTI were delivered to the DFIR team to conduct research, static and dynamic analysis in order to understand the file's behavior, abilities and capabilities, and allow the extraction of additional IOCs, signatures, and the baseline for detection rules. The DFIR specialist's MITRE Tactics and Techniques research included:

- **Privilege Escalation, Persistence -** T1546 Event Triggered Execution, T1543 Create or Modify System Process
- **Defense Evasion -** T1140 Deobfuscate/Decode Files or Information, T1211 Exploitation for Defense Evasion, T1112 Modify Registry
- **Defense Evasion, Privilege Escalation -** T1055.012 Process Injection: Process Hollowing
- **Discovery -** T1083 File and Directory Discovery
- **Discovery -** T1057 Process Discovery
- **Collection -** T1005 Data from Local System, T1113 Screen Capture
- **Command and Control -** T1071 Application Layer Protocol
- **Exfiltration -** T1041 Exfiltration Over C2 Channel

6 **Threat Hunting –** The assigned Threat Hunter used the YARA rules to check whether malware had penetrated the customer's network. The Threat Hunter then recommended that the customer reset the passwords of executives, and enforce MFA for all accounts. The new data and actions that were taken were recorded in the CDC platform.

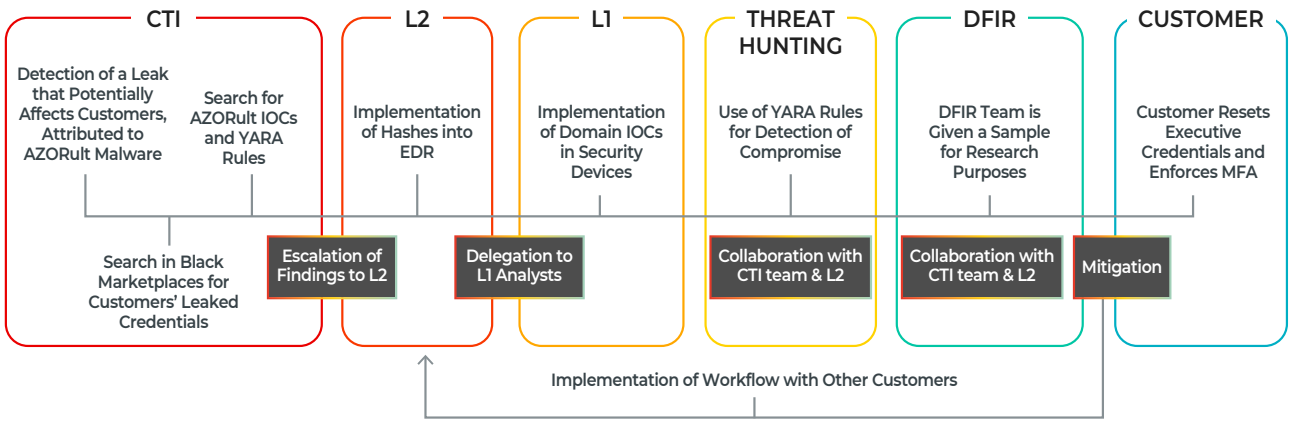


Figure 5: Tracking a potential credential theft that used AZORult malware

SCENARIO 3 – ICEDID TROJAN INFECTION ON ENDPOINT

L1 and L2 cyber analysts, Threat Hunters, the DFIR team and the CTI team collaborated using the CDC platform to uncover a malware infection on a customer's network that targeted companies within the Banking, Financial Services and Insurance (BFSI) sector.

Use Case Involved - By Team:

CTI team

- Threat Intelligence Investigations and Response
- Root Cause Analysis

Threat Hunting team

- Data Collection

L1 + L2 analysts

- Incident Investigation
- Incident Response
- Detection Rule Implementation

DFIR team

- Analysis of Malware on the Endpoint

HERE ARE THE STEPS WE TOOK:

1 **Following lead –** One of our L1 analysts received a notification regarding an Endpoint Detection and Response (EDR) alert: a suspected process injection described as a Cobalt Strike payload injected into a masqueraded process with legitimate looking metadata. It was also seen as ageNose.exe and Winnit.exe.

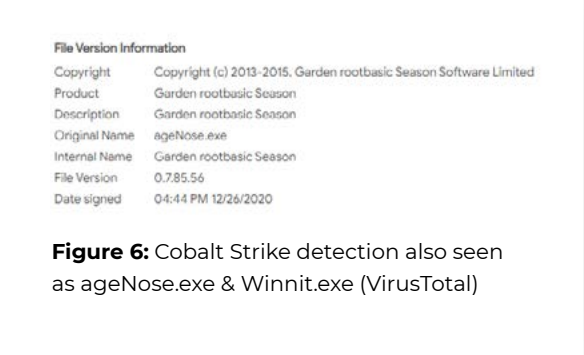


Figure 6: Cobalt Strike detection also seen as ageNose.exe & Winnit.exe (VirusTotal)

2 **L1 investigation –** The analyst began to collect evidence about related endpoint and user activity to clarify whether this was a false or true positive. The analyst identified a suspicious C&C communication with a Ukrainian IP which has a good reputation but communicates with suspicious executables. The analyst also found evidence of defense evasion techniques used. The L1 analyst escalated the incident to L2.

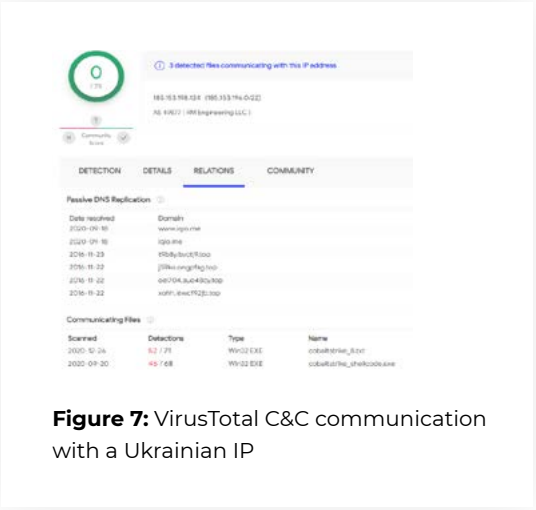


Figure 7: VirusTotal C&C communication with a Ukrainian IP

3 **L2 investigation –** The L2 analyst discovered that the executable carried out the following techniques:

- Used several .NET commands via cmd in order to query for domain admins
- Used several nltest commands via cmd in order to query for domain admins
- System info was initiated as a result of systeminfo.exe execution
- A sub-process executed the C&C commands before a PowerShell connection requested 3 scripts that contained obfuscated commands – one of which was an obfuscated command to download and execute an NSIS Agent backdoor

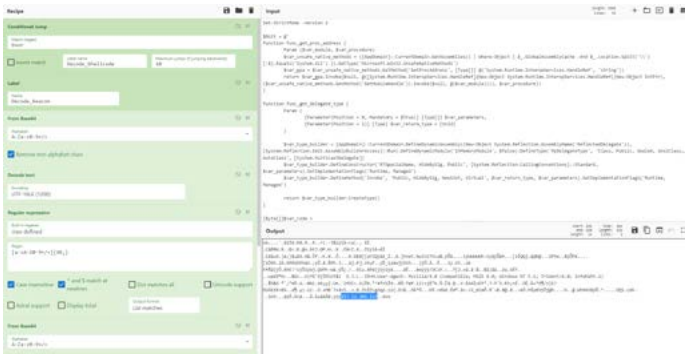
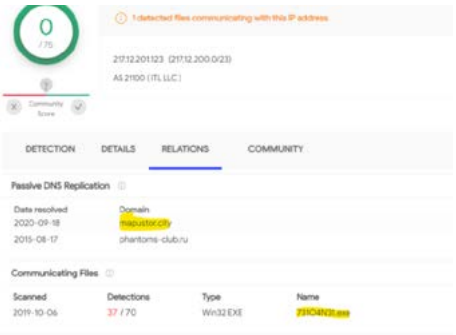


Figure 8: The Cyber Chef tool used to de-obfuscate the payload

Here is the IP that was mentioned:



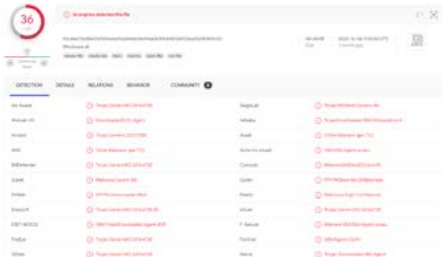


Figure 9: VirusTotal Detection of the Ukrainian IP

The main malware executable contained a few malicious modules inside after the unpacking including CobaltStrike, Meterpreter and Turla:

Figure 10: Intezer Malicious modules

4 **L2 response –** The L2 analyst took the necessary steps for containment and investigation, including password reset, PC isolation (physical), and validating with the user. The sender was investigated, and other users who received the email from the sender domain were investigated in order to validate that no infection was found.

5 **L2 root cause analysis –** The L2 analyst discovered a spear phishing email that delivered a ZIP attachment named "requests.zip" containing a macro enabled DOC file. The user opened the document, enabling the macro. The macro was executed – since it has a startup hook. Regsvr32 created a middle executable, with masqueraded metadata, and this generated a process armed with Cobalt Strike that was detected by the EDR system.

```
Attribute VB_Name = "ThisDocument"
Attribute VB_Base = "1Normal.ThisDocument"
Attribute VB_GlobalNameSpace = False
Attribute VB_Creatable = False
Attribute VB_PredeclaredId = True
Attribute VB_Exposed = True
Attribute VB_TemplateDerived = True
Attribute VB_Customizable = True
Attribute VB_Name = "UpQZP"
Sub wcXT3(KbCdK, ZJBHp)
' Aquatic duomo sociologists
' Batchec huchec mascing
' Indigestible anal paused
' Pennant greets scouting
' Pin upholstered
' Custard remixes engorged auroral
' Regales sonora paragraphing respectability rocked
' Chews tendentious
Set mgkch = CreateObject(ZJBHp + "cript.shell")
```

Figure 11: Malicious macro functions in the relevant .doc file (Inquest)

6 **CTI analysis –** To gain a more in-depth understanding of the attack, all of the observables identified by the L2 analyst were synchronized with the CTI team. The CTI team identified that similar campaigns were found for the IcedID banking trojan. (See: https://isc.sans.edu/diary/rss/26674.) Using threat graphs, we were able to associate the file hash with other indicators such as IP, domain and additional files, which are all associated with IcedID.


File Version Information

Copyright	®South stationdoor Sea Salt dar
Product	Sound bearjoy Whether
Description	Sound bearjoy Whether
Original Name	deser.exe
Internal Name	Sound bearjoy Whether
File Version	15.6.68.90

Figure 12: Dropped file metadata (VirusTotal)

7 **CTI response –** The indicators identified by the CTI team were reviewed by the L2 analyst, providing verification that it was an IcedID infection. The CTI team ensured that the IOCs were ingested into the relevant systems, and an alert that included these IOCs was shared with the customer.

8 **Digital Forensics and Incident Response (DFIR) endpoint forensics –** The DFIR team conducted remote analysis on the infected endpoint to extract additional artifacts and to learn more about the attack infrastructure and the validation of Data Loss Prevention (DLP) including:

- **Persistence ->** Registry Run Keys/ Startup Folder [T1547]
- **Persistence ->** Scheduled Task [T1053]
- **Credential Access ->** Credentials in Files [T1552]
- **Credential Access ->** Credential Dumping [T1003]
- **Discovery ->** Network Share Discovery [T1135]
- **Discovery ->** Query Registry [T1012]
- **Discovery ->** Remote System Discovery [T1018]
- **Discovery ->** System Information Discovery [T1082]
- **Discovery ->** System Network Configuration Discovery [T1016]

The client was notified and advised to reimage the machine. The DFIR team then analyzed the malware in a controlled environment for static analysis, dynamic behavior including partial reversing, and generated additional IOCs:

- **Execution ->** Command-Line Interface [T1059]
- **Execution ->** Execution through Module Load [T1129]
- **Execution ->** Scheduled Task [T1053]
- **Execution ->** Scripting [T1064]
- **Execution ->** Windows Management Instrumentation [T1047]
- **Defense Evasion ->** Scripting [T1202]
- **Command and Control ->** Remote File Copy [T1544]

9 **Threat Hunting team data collection –** Our Threat Hunting team found a legitimate sqllite3.dll that was dropped in a TEMP folder, and was used by the IcedID to perform queries to browser's databases with saved cookies, in order to steal them. (See: https://blog.malwarebytes.com/threat-analysis/2019/12/new-version-of-icedid-trojan-uses-steganographic-payloads/)

```
14  GetTempPathA(260, &sql_path);
15  lstrcatA(&sql_path, aSqlite32Dll);
16  if ( load_sql_functions((int)&sql_path) )
17  {
18    add_to_logger(1, 4, (int)&sqlite_use_internal);// "[INFO] bot.dg.sqlite > use internal"
19    return 1;
20  }
21  if ( !to_get_item_from_url((int)aSqlite32Dll_0, &v11, ArgList) )
22  {
23    add_to_logger(4, 4, (int)&unk_1001842C, aSqlite32Dll_0);// "[ERROR] bot.dg.sqlite > download url=%s"
24    return 0;
25  }
26  v2 = write_file((int)&sql_path, v11, *(int *)ArgList);
```

Figure 13: Legitimate sqllite3.dll dropped in a TEMP folder

10 **SIEM Expert lessons learned/tuning –** The L2 team delivered an overview of the incident to the SIEM expert, together with a description of the possibility of establishing new detections based on the incident findings. In light of these findings, the SIEM expert created additional detection rules and fine-tuned existing rules to improve future detections.

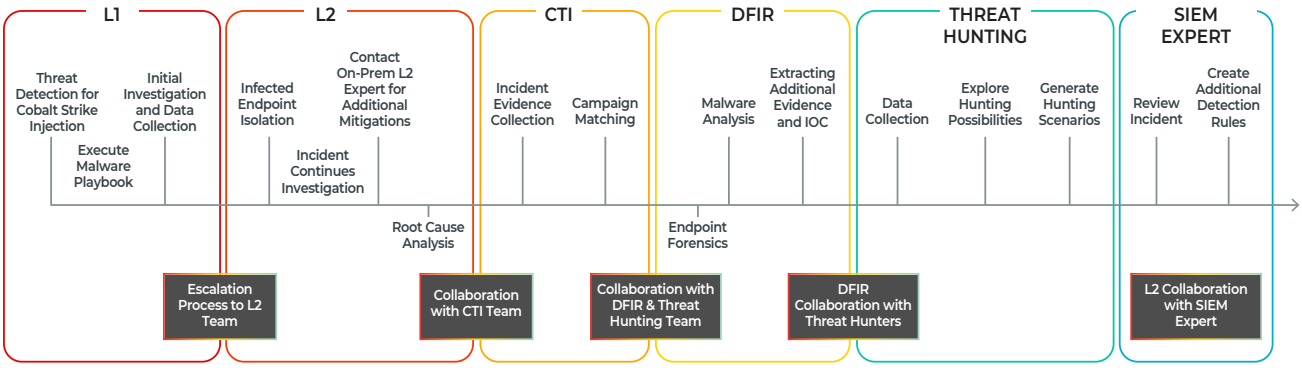


Figure 14: Detection & response of an IcedID infection

A DEEPER LOOK – MAPPING THREATS TO THE MITRE ATT&CK FRAMEWORK TO REDUCE RISK

Mapping incident handling to MITRE's Attacker Tactics, Techniques, and Common Knowledge (ATT&CK) framework is key to understanding what steps are needed at each stage of the attack life cycle.

Many security teams struggle to map their own processes to the ATT&CK matrix – but doing so effectively is an important step in successfully detecting and responding to the threats that emerge. As an example of what this mapping process can achieve, the below "overlay" of the diagram shown in Scenario 3 matches up various aspects of the attack with ATT&CK tactics and techniques (T&Ts).

The illustration demonstrates the type of process that an organization can undergo to fully leverage the ATT&CK framework in analyzing threats, determining appropriate response measures, and reducing risk to the organization.

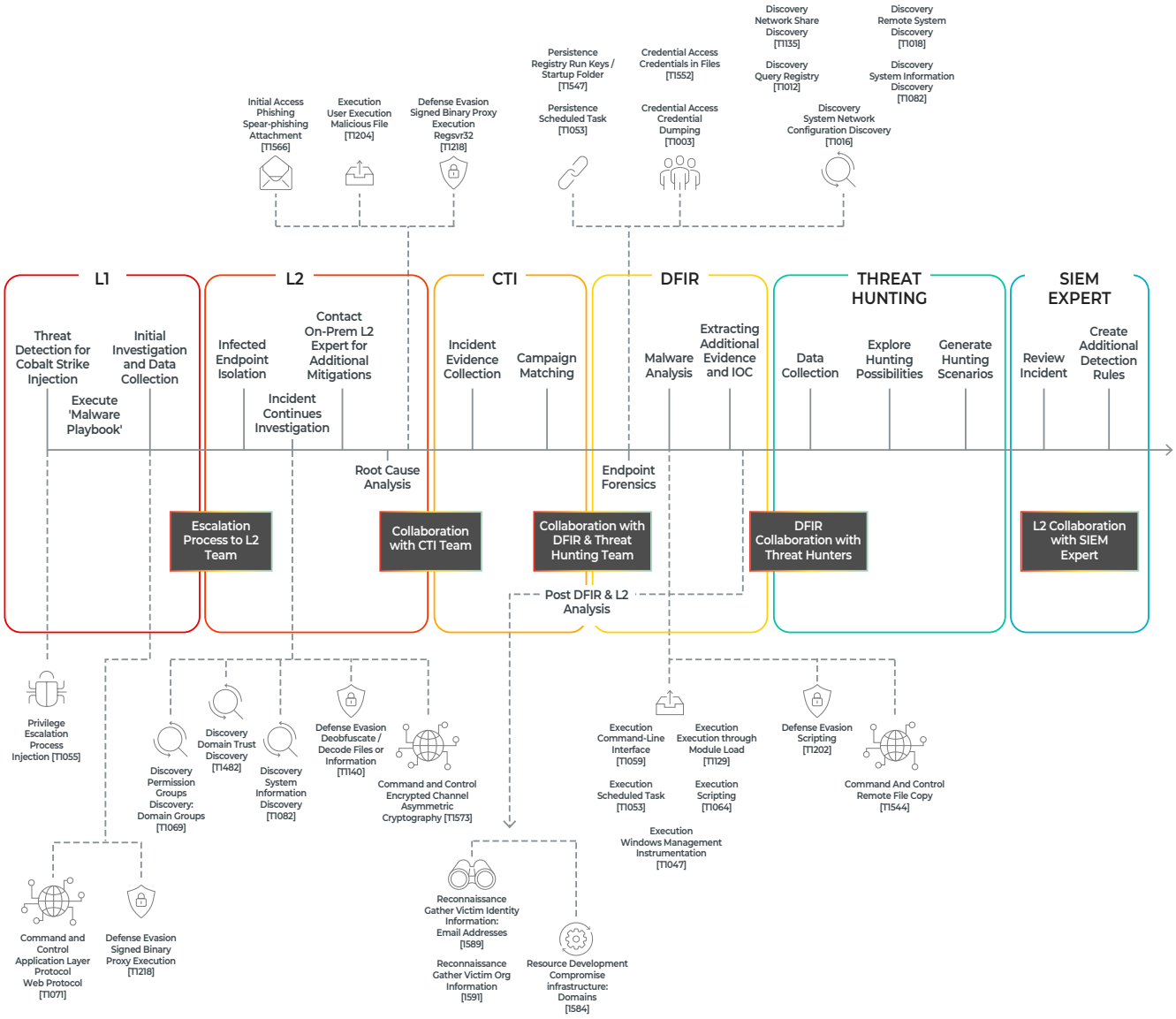
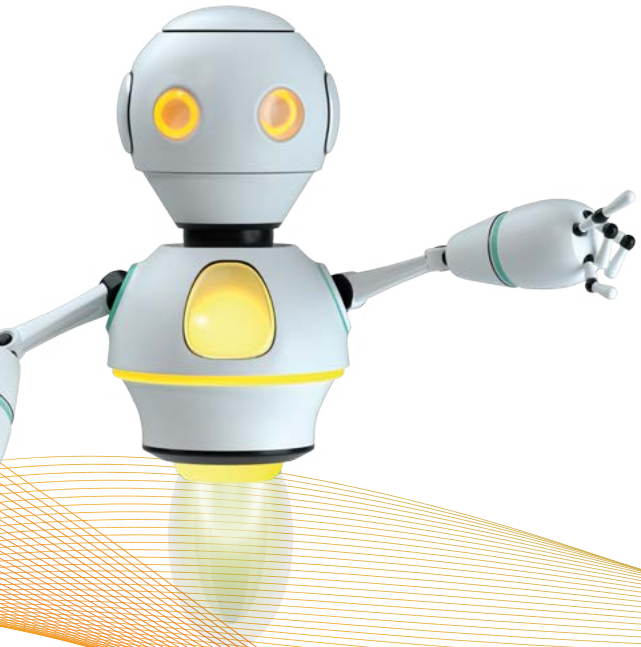


Figure 15: Mapping ATT&CK T&Ts – "Overlay" of Scenario 3

KEY TAKEAWAYS: FACILITATING COLLABORATIVE RESPONSE

These scenarios highlight how to work effectively with other teams to detect and respond more quickly and mitigate damage to the business. Based on these scenarios, we can extract common approaches that can be applied by other security teams in their day-to-day operations:



- **Use a centralized platform for collaborating between teams –** A platform that allows all teams to collaborate, view and access the same data in real time such as the CDC platform increases visibility and allows quick and support interaction between groups with different types of expertise.
- **Capture relevant data for future improvement –** To improve detection capabilities and streamline collaborative efforts at mitigating risks, teams should invest time in gathering feedback about each procedure. New detection rules should be developed, tested, and tuned to ensure they are working optimally.
- **Prioritize your time, effort and resources based on validated insight –** Map your attack surface and identify high-risk vulnerabilities by correlating both external threat data and internal infrastructure data into an integrated single pane of glass view.
- **Adopt a hybrid engagement model to access specialized skills –** Working in a hybrid engagement model enables an organisation's internal security team to extend their capacity by accessing the skills and capabilities of a Managed Security Services Provider (MSSP) that are hard to come by, and only when needed, such as endpoint detection & response, threat hunting, digital forensics, and incident response.

ABOUT CYBERPROOF

CyberProof is a security services company that intelligently manages your incident detection and response. Our solution provides complete transparency and dramatically reduces the cost and time needed to respond to security threats and minimize business impact.

SeeMo, our virtual analyst, automates and accelerates cyber operations by learning and adapting from endless sources of data and responds to requests by providing context and actionable information. This allows our nation-state cyber experts and your team to prioritize the most urgent incidents and proactively identify and respond to potential threats. We collaborate with our global clients, academia and the technology ecosystem to continuously advance the art of cyber defense.

CyberProof is part of the UST family. Some of the world's largest enterprises trust us to create and maintain secure digital ecosystems using our comprehensive cybersecurity platform and mitigation services.

For more information, see: www.cyberproof.com

LOCATIONS

Barcelona | California | London | Paris | Singapore | Tel Aviv | Trivandrum